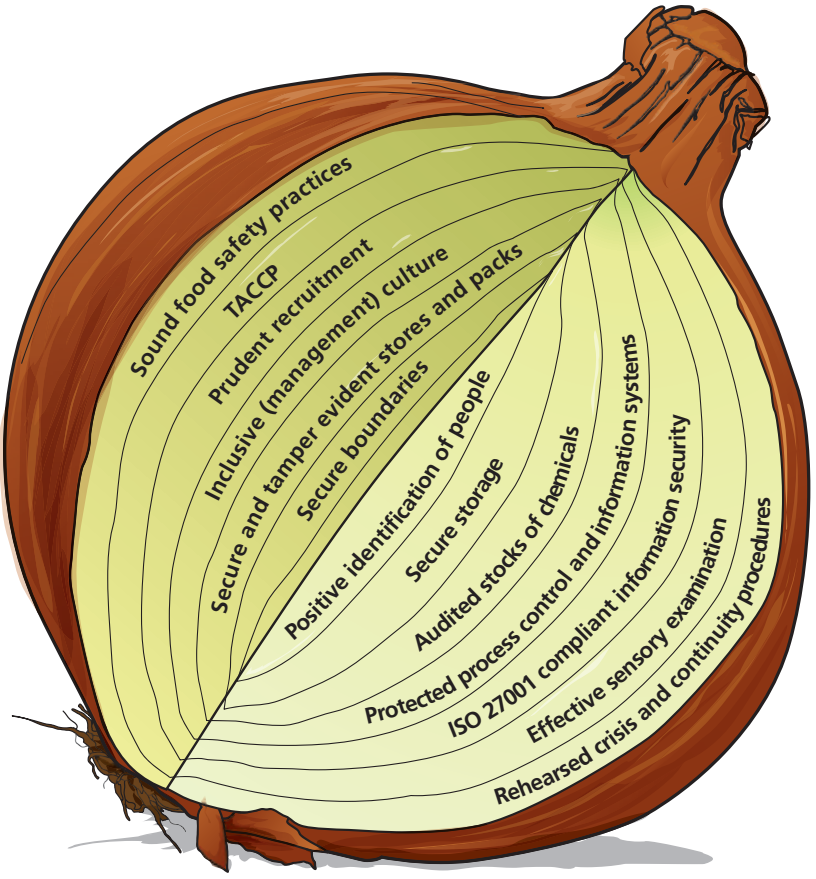
PAS 96:2010

Defending food and drink

Guidance for the deterrence, detection and defeat of ideologically motivated and other forms of malicious attack on food and drink and their supply arrangements

Reviewed and updated in 2010



CPNI
Centre for the Protection of National Infrastructure

BSI

Publishing and copyright information

ISBN 978 0 580 70039 2

ICS 67.020

Publication history
First published in March 2008
First (present) edition published in March 2010
This Publicly Available Specification comes into effect on 31st March 2010

Amendments issued since publication

Date	Text affected

Contents

Foreword

This Publicly Available Specification (PAS) was developed by the Centre for the Protection of National Infrastructure (CPNI) in collaboration with The British Standards Institution (BSI) in 2008. The original edition made use of preventative strategies within the World Health Organisation guidance on the Terrorist Threat to Food [1] which was revised in May 2008. This new 2010 edition of PAS 96 has been reviewed by relevant stakeholders and amendments made to ensure its continued relevance and accuracy.

Acknowledgement is given to the following organizations that were consulted in the development of this specification:

- Agrico UK
- Arla Foods
- Associated British Foods
- Baxters Food Group
- Cranfield University
- Dairy UK
- Defra
- Food and Drink Federation
- Food Standards Agency
- Gate Gourmet
- Health Protection Agency
- HJ Heinz
- J Sainsbury
- The Kellogg Company
- Kraft Foods
- London South Bank University
- Marks and Spencer
- Muller Dairy
- National Farmers Union
- Scottish Food and Drink Federation
- Tesco
- Waitrose

Wider comments from other parties were invited by BSI. The expert contributions made from organizations and individuals consulted in the development of this PAS are gratefully acknowledged.

Rationale and purpose

This section sets the context for PAS 96 *Defending Food and Drink*. It describes and explains the structure of the PAS and indicates the way in which it should, and should not, be used. As such it is an important part of the PAS and should be fully considered before the detailed provisions.

The food and drink industry in the UK – the food sector of the national infrastructure – could be under threat from ideologically motivated groups. The threat extends that from criminals who use extortion and from individuals with a grudge. It is different in nature from the (natural) hazards which the industry is well versed in handling. The threat is unlikely to decline in the foreseeable future. PAS 96 provides broad guidelines to industry operators which should help them assess (see Clauses **6** and **7**) and reduce (see Clauses **8** to **13** and Annex B) the risk to their businesses and to mitigate (see Clause **14**) the consequences of an attack.

Broad guidelines should be interpreted as precisely that. They are broad because managers will have specific knowledge of the specialist detail of their businesses which would not be appropriate for a document such as this, and because specific information may be of help to an intending criminal. They are guidelines and not requirements because a key feature of PAS 96 is 'proportionality'. The risk is different for different businesses, for different operations, and for different products. It is therefore implicit that different risk assessments will result in different action plans proportionate to an individual situation, and indeed in some cases to a legitimate decision to take no specific action.

To make the guidelines as sensible and as accessible as possible, PAS 96 is deliberately written to integrate the reasoning behind a provision with the provision itself. It tries to use language familiar to the industry without continual definition, and it tries to balance conciseness and comprehensiveness by making sensible references to other sources of information. Some repetition has been accepted where emphasis has been needed or to improve readability.

It assumes that managers are aware of Hazard Analysis Critical Control Point (HACCP) or similar risk management procedures, crisis management and business continuity management principles and have effective procedures in place. It is expected that most executives will build the provisions of PAS 96 into these existing protocols. PAS 96 recommends a team approach, as that is typically the best way of bringing relevant expertise together; however it is recognized that for many, particularly small enterprises, this may have to be a team of one person.

In contrast to many standards, PAS 96 is not seen as an external audit tool. The principle of proportionality means that different operations within even a single business may come to very different assessments of its implications. It may be reasonable for a customer to ask its supplier if it is familiar with the guidelines of PAS 96, and to ask if it has implemented the (proportionate) steps which it judges necessary, but not to require specific action on each individual paragraph.

PAS 96 is written in a UK context and invites operators to view the guidelines in the context of the legislative requirements of the UK. It does not consider application internationally, but operations may find some of the approaches helpful and are welcome to make whatever use they feel appropriate.

In summary, PAS 96 provides some approaches to the developing problem of malicious attack on the food and drink industry. Its provisions should be both practical and proportionate, and should help businesses deter potential attackers. BSI and CPNI welcome feedback on the structure, format and provisions of PAS 96, and especially of omissions which readers perceive or revisions which they feel necessary.

Introduction

Businesses within the food and drink industry are well versed in the processes needed to make safe, wholesome, nutritious and palatable food available to customers. Removal of contamination from raw food sources, processing to make them consumable, and managing distribution to avoid recontamination and spoilage are at the heart of the modern food industry. Hazard Analysis Critical Control Point (HACCP) methodology has proved invaluable in controlling adventitious hazards which are based on the environmental and biological nature of food and which are essentially random in character.

The public and businesses within the food and drink sector now face a different threat – that of malicious attack, especially by ideologically motivated individuals and groups. This threat will manifest in a way which reflects the motivation and capability of these people. It will not follow the statistically random, and therefore predictable patterns of familiar 'hazards' so the established HACCP approach might not work without modification.

This document seeks to inform all those involved in the food and drink industry of the nature of this threat, to suggest ways of deterring attack and to recommend approaches that will mitigate the effect of an attack should it happen. The interpretation of the guidance depends on the individual judgement of business managers. Action taken by any business should be proportionate to the threat faced by that business and the document points to approaches to assess this threat. The provisions of this PAS are not designed to be used as an audit tool as different organizations will make different assessments of threat, vulnerability and impact, and will implement different practices to defend the food they handle and the supply arrangements which they use.

Core to the defence of food is a systematic evaluation of vulnerable elements of the supply chain carried out by an experienced and trusted team. In this document, this is called 'Threat Assessment Critical Control Point (TACCP)' and is described in Clause **6**. The evaluation reflects established procedures for risk management and it is likely that organizations will incorporate it into crisis and/or business continuity management frameworks.

Many other publications, including British Standards and CPNI guides, are of direct relevance to the defence of food and drink. These include good practice guidance and standards for business continuity management and traceability. In the interests of conciseness, their content is outlined in this PAS and references are given for further reading in the bibliography. Food and drink supply requires appropriate energy and water services and an effective telecommunications and transport infrastructure, therefore reference is given to authoritative guidance to protective security in these areas. In addition, Annex A provides a short directory of organizations with relevance to aspects of food defence.

Food safety legislation plays a key part in protecting consumers from unsafe or unfit food. Food businesses are responsible for ensuring that the food meets food safety requirements. Full adoption of the guidance given in this PAS cannot prevent a malicious attack; but it should make such an attack less likely and the impact less traumatic.

1 Scope

This PAS provides guidance to food businesses of all sizes and at all points in the food supply chain – from farm to fork (see Figure 1 in **4.3**). It provides guidance on approaches to the protection of their business from all forms of malicious attack including ideologically motivated attack and to procedures to mitigate and minimize the impact of such an attack. It is intended to be of particular use to managers of small and medium sized food enterprises who may not have easy access to specialist advice.

Food businesses will be able to use the guidance in the context of an effective food safety management regime such as Hazard Analysis Critical Control Point (HACCP) or the Red Tractor [2]. This PAS assumes and builds on effective operation of such protocols.

Tamper-evident closure

2 Terms and definitions

For the purpose of this PAS, the following terms and definitions apply:

2.1 electronic security

procedures used to protect electronic systems from sources of threat, such as malware and hackers, intent on misusing them, corrupting them or putting them out of use

2.2 food defence

security of food and drink and their supply chains from all forms of malicious attack including ideologically motivated attack leading to contamination or supply failure

2.3 food supply

any and all elements of what is commonly called the food supply chain, net or web with the inclusion of drink and supporting and allied services (see **4.3**)

2.4 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 *Not to be confused with 'personal security'.*

2.5 product security

techniques used to make food products resistant to contamination or misuse including tamper-evident closures and lot marking

2.6 protective security

all the measures related to physical, electronic and personnel security which any organization takes to minimize the threat of malicious attack

2.7 Threat Assessment Critical Control Point (TACCP)

systematic management of risks through the process of assessment of threats, identification of vulnerabilities, and implementation of controls to raw materials, packaging, finished products, processes, premises, distribution networks and business systems by a knowledgeable and trusted team with the authority to implement changes to procedures

3 Malicious, ideologically motivated threats to food and food supply

Case Study A:

In September and October 1984, 751 residents of The Dalles in Oregon, USA suffered from food poisoning caused by Salmonellae enteritidis, of whom 45 were hospitalized. Fortunately no one died from the outbreak. It subsequently transpired that local members of the Rajneeshee religious cult had contaminated 10 salad bars with the intention of preventing individuals from voting and thereby influencing the result of local elections in Wasco County at which they hoped to gain political control. Two cult officials were eventually convicted and served 29 months in prison for a variety of offences. It is believed that they obtained the bacterial culture from commercial sources. Nine of the salad bars affected went out of business.

The attack identified the relative ease with which the wholesomeness of ready to consume food could be undermined and pinpointed a particularly vulnerable part of the food supply chain.

Foods sold 'open' for customers to select may be particularly vulnerable

Case Study B:

In Summer 2007, a major UK producer of baked, chilled pastry goods lost five days of production, at a cost of 5% of its annual turnover, when the factory was shut down following a malicious attack using peanuts.

The factory was designated as a nut free site and allergen information on product packaging reflected this status. The discovery of peanuts, initially in service areas then in manufacturing areas, led to the factory shut down. It also resulted in products being removed from retailer sale due to potential anaphylactic reactions from nut allergy sufferers. A police investigation into the incident discounted that the causes were accidental.

Production only resumed following a site-wide deep clean and a major revision, and implementation, of site protective security procedures. These measures were agreed with and supported by retail customers prior to the resumption of supply.

Fortunately no contaminated product left site so serious harm from anaphylactic shock was avoided.

Global, highly competitive food trade may seem an ideal target for malicious, ideologically motivated attack. This could cause mass casualties, economic disruption and widespread panic. In many ways the diversity of the food operations may seem to make the food supply highly vulnerable to attack. However, competition within the sector and the nature of food supply itself provides considerable intrinsic resilience.

Other forms of motivation have led to harmful attacks on foods. Extortion, coercion and criminal action to promote a 'cause' may be accompanied by some form of warning which would not be expected from a terrorist group. Information of any form about any attack or threat of attack should be passed to senior managers without delay. They should immediately implement crisis management procedures including the notification of police.

In practice, undertaking a major attack on the food supply chain is much more difficult than at first it may

be believed. However, even a limited attack can cause harm and economic loss, and could result in significant damage to 'brands'. With extensive consumer and media concern, this threat demands that companies and businesses take a responsible and proactive approach to food defence.

This PAS identifies three generic threats to food and drink:

1. Malicious contamination with toxic materials causing ill-health and even death;
2. Sabotage of the supply chain leading to food shortage;
3. Misuse of food and drink materials for terrorist or criminal purposes.

These threats could be carried out by a number of individuals or groups, including:

- people with no connection to the organization;
- those with a contractual relationship such as suppliers and contractors;
- alienated or disaffected staff.

Further, they could use both physical and electronic techniques to achieve their ends. This PAS attempts an holistic approach to food defence.

Food defence aims to:

- reduce the likelihood (chance) of malicious attack;
- reduce the consequences (impact) of an attack;
- protect organizational reputation (The Brand);
- reassure customers, press and public that 'proportionate' steps are in place to protect food;
- satisfy international expectations [1] and support the work of allies and other trading partners.

4 Broad themes of food defence

4.1 General

The food and drink industry can be seen as naturally vulnerable to attack but highly resilient. The vulnerability arises from relatively open access to sites, especially agricultural, retail and food service sites where the public is actively welcomed. It comes from major and short term (Just-in-Time) movements of materials and from staff turnover and the use of migrant and temporary labour. However, the intrinsic vulnerability is significantly moderated by the operation of established food safety systems which greatly reduce the opportunity for effective attack. The resilience of the sector comes from the overall availability of food, from competitiveness within the industry, and from the consumer's ability to substitute one food for another. Reducing vulnerability and increasing resilience can be achieved by greater control of access to materials, processes, services and premises generally and subjecting these to regular review.

4.2 Response levels

There are three response levels which can be implemented as the threat to a food organization develops:

1. The 'Normal' response level reflects routine protective security measures appropriate to the business concerned. Proportionate steps which build on prudent crime prevention arrangements by consideration of this PAS would form the 'Normal' response.
2. The 'Heightened' response level shows additional and sustainable protective security measures reflecting the broad nature of the threat combined with specific business and geographical vulnerabilities and judgements on acceptable risk, given confidential notice by the authorities that the threat levels for the area had increased. As an example, this 'Heightened' response could include the banning of all but essential vehicles from a site.
3. An 'Exceptional' response would be the implementation of maximum protective security measures to meet specific threats and to minimize vulnerability and risk. It may well be that the 'Exceptional' response involves executive action by the Police with which the organization cooperates.

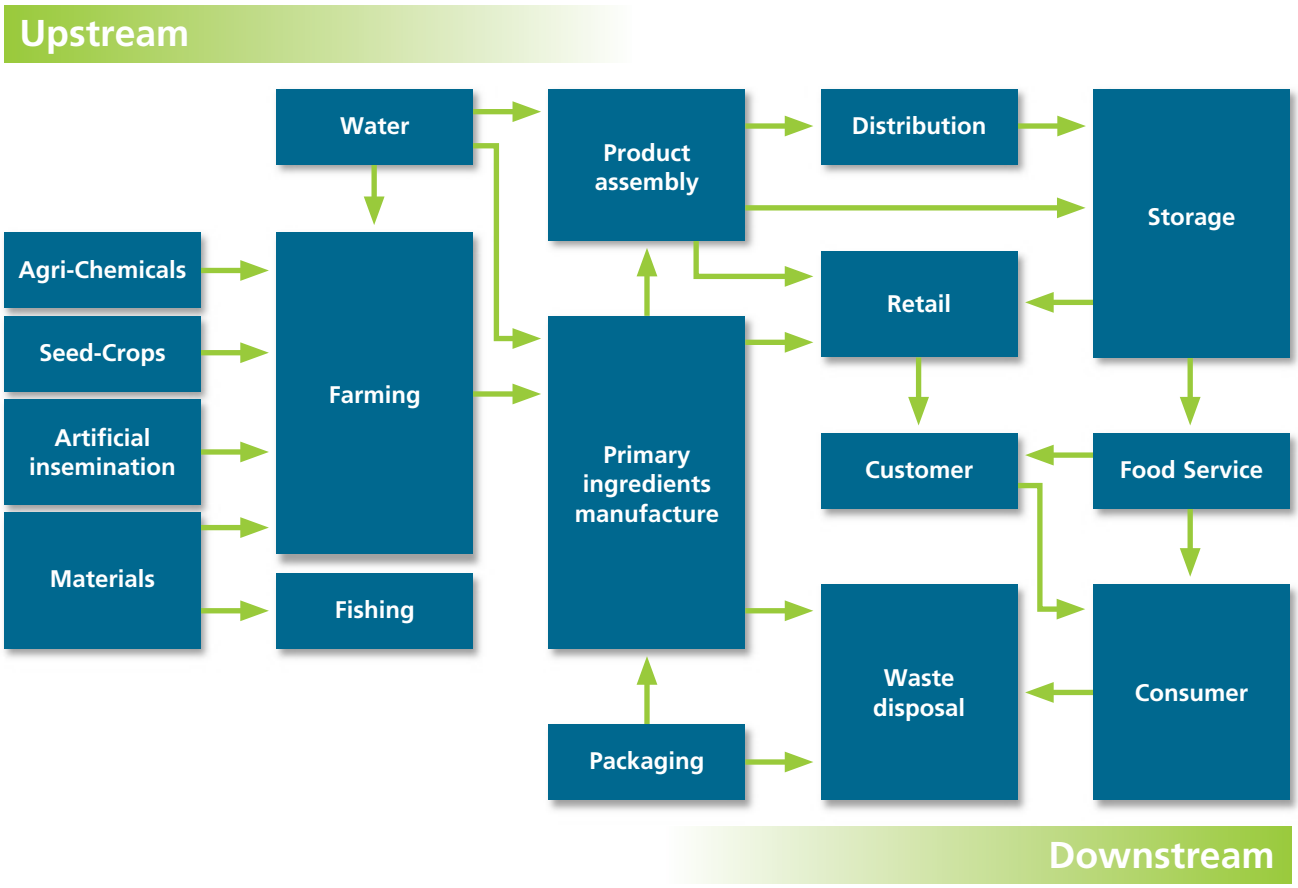
An organization may choose to identify an escalating scale of activities which it would implement as a threat develops.

4.3 The food supply web

Figure 1 illustrates some of the operations involved in modern food and drink supply.

It is not intended to be comprehensive. It is an over-simplified picture intended to illustrate the inter-relationships and to encourage a broad view.

Figure 1 – A food supply web



Successful attacks on operations 'downstream' (food service outlets or retail stores) are likely to have limited scope in terms of geographical area, number of cases or product type but could have traumatic impact (illness or even death). The Oregon State attack illustrates such an incident (see Clause **3** Case Study A).

'Upstream' businesses such as farms would be damaged economically by an effective attack that made large tracts of land unproductive. Manufacturers could suffer significant damage to brand reputation and there is also the potential for casualties to occur although such an attack may prove more difficult than 'downstream' scenarios. The Sudan 1 incident in 2005 (Case Study C) illustrates the point of economic loss.

Case Study C:

In February and March 2005 more than 500 food products were withdrawn from sale in the UK because of contamination with an illegal dye, Sudan 1. The pigment was present in chilli powder sourced from overseas. The chilli powder had been used directly as an ingredient and in compound products such as Worcestershire Sauce which were themselves used as ingredients in more complex products.

While there has been no suggestion of malicious intent, disposal cost the industry several hundreds of millions of pounds. The case also clearly illustrated the complexity of operating effective traceability regimes with long shelf life ingredients used in long shelf life products that are themselves compound ingredients.

5 Presumptions

Good product security builds on sound food safety practices to prevent, detect and remove adventitious contamination.

***NOTE** Adventitious contamination occurs by chance. It could include:*

- *parts of the original plant or animal from which the food has come e.g. a stone in a cherry or hide on a piece of meat;*
- *material closely associated with the original food source e.g. earth stones with dried fruit or oat grains in a wheat harvest;*
- *physical contamination from the process e.g. hair from an operative or pieces of process machinery.*

Further information on good practice in this area can be found in:

Assured Food Standards 'Red Tractor Scheme' [2];

Good Manufacturing Practice: A Guide to its Responsible Management [3];

FSA's Preventing and Responding to Food Incidents [4].

Businesses should have hygienic operations and use HACCP as an integral part of quality management systems. They should operate in line with recognized industry standards such as the British Retail Consortium's Global Standard for Food [5] or BS EN ISO 22000:2005, *Food safety management systems. Requirements for any organization in the food chain*. Smaller companies may find The Safe and Local Supplier Approval Scheme (SALSA) [6] useful.

***NOTE** Details of other industry standards are given in the bibliography.*

Positive management policies should be in place to control fire risks and health and safety issues. Crime prevention should be an ongoing concern. Generic guidance on crime prevention by design of premises is available from the Police [7]. It is recommended that management of food defence is the specific responsibility of a nominated officer with the necessary authority.

6 Threat Assessment Critical Control Point "TACCP"

6.1 General

Hazard Analysis Critical Control Point (HACCP) is the well-established and legally required approach for assuring the integrity of food. It encourages management teams to review established hazards which are typically adventitious in nature and about which there can be significant statistical information. In clear contrast to hazards, threats arise from individuals and groups with malicious intent. There may well be no direct precedent from which to learn; statistics may be irrelevant. There are no environmental or ecological principles which can be brought into use. The size of the threat depends upon three features:

- The motivation, innovation and capability of the would-be attacker;
- The vulnerability of the target;
- The prospective impact of a successful attack.

Food sector professionals will want to minimize the chances of loss of life, ill health, financial loss and damage to reputation which malicious attack could cause.

The threat assessment critical control point approach builds on HACCP and business continuity management philosophies. It is the systematic assessment of threats, examination of processes to identify vulnerable points, and implementation of remedial action to improve resilience against malicious attacks by individuals or groups. It specifically considers that malicious attack is likely to involve unforeseen agents or materials or strategies. The nature of the 'preferred' agent will be influenced by the nature of the food itself, such as its physical state, chemical composition, packaging and shelf life. Practitioners will recognize the protocol as following the established HACCP format; and will also recognize the key differences based on the predictable, random nature of hazards and the targeted, malicious nature of threats which requires creative thinking to anticipate modes of attack and identify deterrent precautions. TACCP is a preventative tool. It may be managed within business continuity procedures.

6.2 Assumptions behind the TACCP approach

1. That malicious intent needs a person, so the procedure is people-focussed. The person may be an individual or part of a group, and may be an insider;

NOTE *'Insiders' are employees or contractors who have legitimate access to an organization's assets, but motivation contrary to the organization's best interests.*

2. That an attacker will want to see a fairly immediate impact; so contamination leading to acute illness or harm is the concern, not potential long-term chronic disease;
3. That localized misdemeanour involving individual retail packs or food service products can be deterred but cannot be prevented, but such limited impact is unlikely to satisfy the aspirations of major groups;
4. That expert knowledge of, and access to, critical processing and packaging operations is a prerequisite of a successful widespread attack;
5. That protective measures will include physical, electronic and personnel security procedures;
6. That TACCP will be best applied to a specific product, viewed on a 'whole life' basis, and the 'lessons learned' applied generally to related products;
7. That food manufacturing and product assembly will be the focus of attention.

6.3 Objectives of TACCP

The objectives of TACCP are to:

1. Identify individuals or groups that might want to target the specific organization, location or product;
2. Assess the likelihood of contamination of that product meeting the needs of prospective attackers;
3. Assemble a body of evidence to inform judgments on the reality of malicious product contamination causing acute harm;
4. Reach consensus within an organisation as to the key vulnerabilities in the supply chain for the specific food product;
5. Attempt a semi-quantitative estimation of the impact of processing, packaging and storage on model contaminants;
6. Implement proportionate control procedures to make a successful attack highly unlikely.

6.4 Impact

The claim or even rumour of malicious food product contamination can alone lead to adverse media comment, customer aversion and consumer concern with negative implications for 'brand' image. A real attack may cause illness and even death as well as these psychological and economic consequences.

Food businesses want to protect their consumers. They also want to comply with food safety legislation under which they are obliged to take all reasonable precautions and exercise all due diligence to avoid an offence.

Use of this TACCP protocol cannot prevent a claim of malicious attack, but it would be of use in establishing the credibility of such a claim. Any such claim and any actual incident will invoke business continuity management systems, including media management and public relations strategies. TACCP does not replace such strategies, but it should complement them and may involve the same people.

The threat assessment and mitigation procedure can normally be generic to a specific production line

6.5 TACCP Process

A standing TACCP Team should be formed which could include individuals with the following areas of expertise:

i. Security;
ii. Human resources;
iii. Food technology;
iv. Process engineering;
v. Production and operations;
vi. Distribution.

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

NOTE 2 *For a small organization, the manager 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 would typically be an established and permanent group, able to review its decisions over time*

All nominees should be very knowledgeable of actual processes, highly trustworthy, discreet and aware of the implications of the study.

The TACCP team should:

1. Identify individuals or groups which may be a threat to the organization (see Clause **7**);
2. Identify individuals or groups which may be a threat to the specific operation (premises, factory, site);
3. Select an exemplar product which is representative of a particular process;
4. Identify individuals or groups which may wish to target the specific product;
5. Draft a detailed process flow chart for the product from 'farm to fork' including, for example, domestic preparation. The entire flow chart should be visible at one time, perhaps by being on a single sheet;
6. Carry out a detailed study of the process including:
   - Amending and validating the flow chart.
   - Listing job roles pertinent to each step in the process.
   - Nominating model contaminants appropriate to the product.

NOTE 4 *Model contaminants could include highly toxic agents, toxic industrial chemicals, readily available noxious materials and 'innocent but inappropriate' substances like allergens or ethnically unwholesome foodstuffs.*

   - Considering the impact of the process on these contaminants.

- Assessing the likelihood of routine QC/QA procedures detecting such contamination.
- Identifying most vulnerable points at which contamination might take place by malicious action of insiders or others.

NOTE 5 *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 might consider how an attacker might select 'attack' materials: availability, toxicity, physical form, safety in use, e.g. pesticides on farms and aggressive flavour materials in factories.*

- Attempting a (semi-)quantitative assessment of contamination levels needed to achieve a toxic effect in a 'reasonable worst case' portion of the finished product.
- Considering how quality procedures would impact on the scenario.
- Documenting outcomes from the assessment, both for the specific product and for the generic process being modelled.

7. Identify, record confidentially and implement proportionate preventative action ('critical controls').
8. Carry out a personnel security risk assessment [8] across the job roles identified in 6 above. Use consideration of the relatively higher risk roles to prioritise preventative action options.
9. Agree any further necessary preventative actions and a plan for implementation.

NOTE 6 *The TACCP Team will need a confidential reporting and recording system that allows management action on decisions but does not expose weaknesses to those without a need to know.*

10. Determine review and revise arrangements for the TACCP.

NOTE 7 *Review of the TACCP evaluation should take place after any alert or annually, as well as points at which new threats emerge or when there are significant changes in Best Practice.*

7 Assessing the threat

The product, the premises and the organization can be the target of attack and each element should be assessed separately. Managers should consider alienated employees and former employees, single issue groups, commercial competitors, media organisations, terrorist organisations, criminals and local pressure groups, and could ask the following questions.

For the product:

- Does this product have particular religious, ethical or moral significance for some people?
- Could this product be used as an ingredient in a wide range of popular foods?
- Does the product contain ingredients or other material sourced from overseas?

For the premises:

- Are premises located in a politically or socially sensitive area?
- Do premises share access or key services with 'controversial' neighbours?
- 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?

For the business:

- 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?
- Do we support visa applications from overseas visitors?

NOTE *These lists are not exhaustive.*

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 ('Operational Requirements').

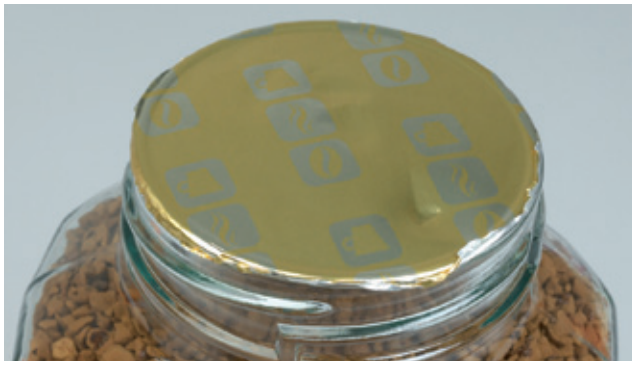
8 Assuring personnel security

NOTE *For extensive guidance on personnel security, please refer to www.cpni.gov.uk/ProtectingYourAssets/personnelsecurity-268.aspx [9].*

8.1 Pre-employment prudence

A significant attack on food supplies is most likely to involve individuals with knowledge of and/or access to food processes. Many food operations have rapid turnover of staff and may recruit on the basis of minimal information, and are therefore highly vulnerable. For detailed guidance on pre-employment screening please refer to www.cpni.gov.uk/Docs/pre-employment-screening.pdf CPNI [10]. Attention is also drawn to BS 7858:2006: *Security Screening of Individuals Employed in a Security Environment*. Recruiters should base their recruitment decisions on original documents, not photocopies, and should assure themselves that documents used to support an application are genuine. Similar considerations apply to visiting contractors; employers should assure themselves that their contractors operate secure personnel policies and be prepared to carry out checks themselves. The area of recruitment and employment is heavily regulated. Particularly pertinent examples are given in the bibliography [11 – 22].

All employees and visiting contractors within the food industry are to some extent in positions of trust. Employers should assure themselves that individuals are worthy of that trust. Some key or sensitive positions (e.g. security guards, goods reception and packaging supervisors, engineers and process control technicians) demand a high level of independence and trustworthiness and are pivotal to the success of operations. Systematic evaluation of job functions can identify these roles and enable the appointment of those with an appropriate record or who have satisfied a more stringent screening process.



8.2 Systems for control of temporary staff

The same requirements apply to temporary staff as apply to permanent employees. Temporary staff from recognized agencies may be treated like contractors for security purposes.

To control and monitor the use of casual and sub-contract staff the company should consider adjusting contracts to give them the power to externally audit recruitment and screening processes of supplier staff deployed on their contract.

8.3 Building employee inclusiveness

Managers will recognize that alienated or disenchanted employees are more likely to be disruptive or to overlook disruptive behaviour of others. They should encourage the development of an operational team spirit to encourage both loyalty to the operation and the reporting of unusual employee behaviour.

Managers should be aware that both they and trusted staff are open to coercion or deception by those of a malicious disposition and should give thought to how unusual behaviour should be managed.

CPNI has published advice on ongoing personnel security [23].

9 Controlling access to premises

9.1 General

Access of people, vehicles and materials onto premises should be restricted to those with a clear business function. This reduces the opportunity for malicious intrusion. For example, it could be more effective to control pedestrian access for staff and visitors with car parking external to the secure premises than to examine every vehicle regardless of need for access. In many situations, such as primary agriculture, access cannot be controlled in this way. Similarly, controls cannot be used where the general public has business access such as retail and food service outlets. In such situations, organizations will apply controls to appropriate buildings or parts of buildings.

Visible and comprehensive perimeter fencing may act as a deterrent to intruders, and an associated alarm system can give indication should intrusion take place. Advice on the specification of perimeter fencing depends upon operational requirements provided by the threat assessment. Unauthorized access may be monitored using CCTV and security guarding, given a suitable external lighting system.

Perimeter controls should also consider the site situation (roads, waterways, other buildings, planning constraints) as well as technological issues like pest control. Perimeter controls should be viewed as a whole so that weakness in one part does not negate strengths in other parts. Any business contemplating the development of a new site should build protective security considerations into the design process.

Event activated lighting is a familiar feature

Even modest perimeter fencing can deter intruders

Rising bollards can control traffic

9.2 Access for motor vehicles

Entry to vehicles on essential business should be through monitored access points. Approach roads which minimize the speed of the vehicle and maximize the opportunity for inspection and rejection would be helpful.

Consideration should be exercised in site planning and maintenance. Access to and from the site should be clear and able to be surveyed. Excess foliage should be regularly cleared to facilitate total surveillance.

NOTE 1 *Guidance on the manufacture and testing of hostile vehicle restraint measures (e.g. crashproof barriers) can be found in PAS 68:2010 Specification for vehicle security barriers.*

NOTE 2 *Guidance on traffic calming and the layout and installation of vehicle restraint measures can be found in PAS 69: 2006 Guidance for the selection, installation and use of vehicle security barriers.*

Deliveries of materials should be scheduled in advance and unscheduled deliveries should not be accepted. Staff responsible for receiving goods should check documentation and the integrity of loads so far as is possible, and record serial numbers from any tamper-evident tags. Deliveries of goods other than those for trade purposes (e.g. for staff canteen) should not be overlooked as potential carriers of malicious material. Staff should be aware of the dangers of the unlawful use of emergency service and other liveried vehicles ('Trojan' vehicles) which are not what they seem, of deception to gain access, and of coercion of legitimate drivers to carry malicious materials. They should investigate, when possible, any vehicles missing scheduled delivery times.

9.3 Access points for people

Automatic entry to individuals may be granted based on what they have (e.g. a key or token such as a swipe card) or of what they know (e.g. a password or PIN code) or, preferably, of both. This last approach should be used to limit access to sensitive areas like bulk storage silos and process control rooms to trusted staff.

Other than persons on official business, all visitors should have appointments and be under management endorsement and supervision.

Secure doors are available for the widest of doorways

9.4 Screening of visitors

As a general rule, and with the exception of retail and food service customers, only visitors with a justified reason should be allowed on food premises and then only by appointment. Casual visitors should be excluded unless from a recognized authority. All visitors should present reasonable proof of identity on arrival and a record of their attendance should be maintained. A nominated person should meet and accompany the visitor throughout the visit. Visitors should agree to cooperate with a security search should one be felt necessary.

9.5 Identification of 'unauthorized' visitors

For all but very small operations, positive identification of staff and visitors at all times is recommended. This could be by means of marked workwear and/or identity passes. Staff should be trained and encouraged to be vigilant in order to identify, monitor and report intruders and to report hostile surveillance. Appropriate use of closed circuit television (CCTV) could have value if operated according to the principles of the Data Protection Act 1998 [12] and if operators are appropriately licensed and trained. The police should be contacted immediately if an intruder is found on the premises.

9.6 Secure mail handling

Postal and courier services have been used to deliver noxious materials to premises. In the light of a threat assessment, managers may consider whether centralized and/or remote reception and examination of such deliveries is needed. Further advice on mail handling is available in PAS 97:2009 *A specification for mail screening and security* [24].

9.7 Restrictions on portable electronic equipment

Modern cameras and audio/visual equipment including mobile phones can be used to undermine the security of premises by informing criminals about levels of protection. In the light of a threat assessment, managers may consider whether to restrict the use of such equipment.

CCTV can monitor access to restricted areas

10 Controlling access to services

Attack on factory services (mains power, fuel oil, gas supplies, potable water, mains drainage, telecommunications systems, refrigeration, cleaning systems, etc) would sabotage operations and could lead to malicious contamination. Air inlets to ventilation systems can be vulnerable to noxious gases or aerosols and may merit protection. Managers may identify sensitive areas and limit access to nominated responsible individuals and deputies. They should liaise with suppliers of services so there is no avoidable gap in security between supplier owned and operator owned infrastructure.

11 Secure storage of transport vehicles

Managers should ensure that vehicles under their control are not misused and should ensure that storage at the depot and when en-route is secure.

12 Controlling access to materials

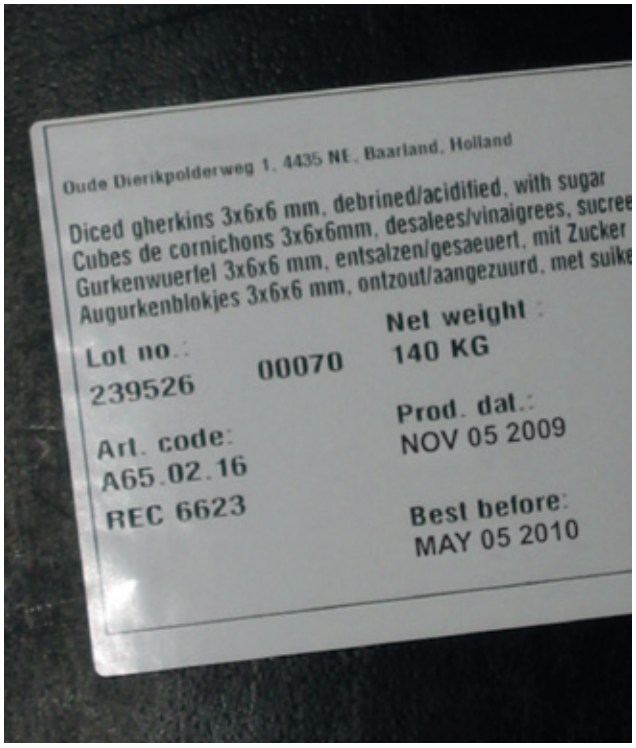
Secure storage of foodstuffs and packaging materials will reduce the opportunity for contamination. Lockable storage areas and numbered tamper-evident seals on access ports to bulk silos are recommended. Secure storage of product labels will reduce the chance of attack with counterfeit goods.

Hazardous materials, in particular cleaning and sanitising chemicals which can themselves be misused for malicious purposes, should be handled safely and in locked storage under the control of a trusted manager. Guidance on the control of ammonium nitrate fertiliser [25] in agriculture (see Annex B.1) may be adapted for use with peroxide based sanitizers, noxious additives and pesticides. Effective stock reconciliation should form a constant element of control of such materials, as does tamper-evidence (on intake and discharge) of distribution and storage containers. The same considerations apply to any toxic or pathogenic material used as laboratory agents.

Reception arrangements for raw materials should include checks of the integrity of tamper-evident seals. Suspicious materials or those with damaged seals should not be used without further investigation and clearance.

Employees should be provided with lockable storage for personal property to enable its separation from the process.

Secure covers for storage chamber access points



Clear labelling is essential to ensuring traceability

Distribution and storage containers should be tamper-evident

13 Controlling access to processes

13.1 General

Critical process control rooms should be secure and access limited to authorized staff. Where electronic process controls are in use, access should be by secure identification and authentication mechanisms such as usernames and passwords. Detailed guidance on the protection of process control (including SCADA – supervisory control and data acquisition) systems is available from CPNI [26]. By clear marking of staff, as often used to distinguish 'high care' (typically, post-process) from 'low care' (typically, pre-process) areas, individuals who are in the wrong place can be quickly identified.

13.2 Assuring business processes

In addition to specifically food technologies, the sector is dependent on external services of the wider economic community.

The transport infrastructure is critical to a 'Just-in-time' approach to food supply. Managers should have contingency routes as back up to their normal distribution network. They may liaise with neighbouring operations to ensure alternative access to local sites in the event that the primary entrance is out of use.

Modern business processes (e.g. sales and bought ledger, order receipt and processing, production scheduling, point of sale stock control and payments systems) are typically based on generic electronic platforms (e.g. SAP, ORACLE, Microsoft Windows, Unix) and are vulnerable to malicious attack regardless of the sector involved. Information technology managers should implement ISO 27001 compliant electronic security measures. They should maintain topical and current virus checking software and firewalls, and should install patches and upgrades as soon as they become available. They should consider to what extent hot standby (i.e. ready to operate), warm standby (i.e. can quickly be made operational) and cold standby (i.e. archived records) or other back up systems are needed and whether duplication of information technology systems is needed to provide the necessary resilience. Access rights for administrators should be based on separate and independent identification and authentication. This provides an audit trail for, for example, the allocation of user access rights, the

management of anti-virus and firewall installation and patch application. Some operations rely on bespoke rather than off-the-shelf systems. These may be less likely to attract malicious attention, but may be more difficult to defend. The increasing use of internet protocols, for example to enable remote working, makes operations increasingly open to attack and merits vigorous implementation of security measures. CPNI offers specific advice to the national infrastructure to help mitigate threats to electronic security [27].

13.3 Assurance that sources of materials are reliable and threat aware

The integrity of materials supplied to premises is fundamental to good practice. Operational managers, in their vendor approval routines (especially for new suppliers) may want to assure themselves that their suppliers are aware of security issues and have taken a proportionate approach.

Casual purchases should be subject to strict internal technical and quality control checks. Casual purchases should be the exception rather than the norm; care should be taken to ensure that casual suppliers do not become permanent suppliers without first being subject to appropriate checks and controls.

13.4 Product security – tamper-evident consignments

Where malicious contamination cannot be prevented, tamper-evidence provides an important protection against damage and harm. For bulk supplies of materials including packaging materials, protective seals using numbered tags assures integrity and contributes to product traceability. For ingredients used in only small quantities and for retail packages, tamper-evidence can initiate quarantine and investigation prior to use.

Partially manufactured 'work in progress' should be covered and could be made tamper-evident if stored. Finished product packs for retail display should normally be tamper evident.

13.5 Reception arrangements for materials

All foodstuffs, packaging, and business services should be treated as quarantined on arrival at Goods-In. Staff should record vehicle details and tamper-seal numbers, and confirm there are no damaged packs in the consignment.

Sensory examination of ingredients and other foodstuffs for unusual odours or appearance is recommended for positive release into materials storage.

Secure quarantine and disposal of all waste material, especially printed packaging, is needed to ensure that it does not become a source of contamination or misuse.

13.6 Quality control arrangements

Managers should concentrate on quality assurance techniques to defend food and drink, and not rely on quality control testing. When trying to spot a very infrequent event which would have dire consequences, quality control techniques based on sampling are not sufficiently effective and only 100% examination is adequate, as used for metal detection. Such examination would need to be by non-destructive testing which is not practicable for unpredictable hazards. Having said that, sensory examination can be a most useful tool, as many contaminants will influence the colour, odour, texture or flavour of a foodstuff at levels at which they do not cause acute harm. Investigation of incidents can make use of specialist analysis of hazardous materials, or research associations that can examine materials against an established profile and thereby identify discrepancies. Some routine checks such as chlorination checks of mains water could indicate sabotage of services.

Tamper-evidence provides an important protection against damage and harm

14 Contingency planning for recovery from attack

Use of business continuity management principles complying with BS 25999 *Business continuity management*. *Part 1: Code of Practice* will give good resilience to react to and recover from malicious attack. Managers may want to review regularly, the balance between their provision of just-in-time supply versus just-in-case provision. Some fall-back source of key services may be advisable, in addition to those of electronic service discussed in Clauses **10** and **13.2**. While duplication of mains services is likely to be appropriate for only a very small number of very large 'sole suppliers'; some thought could be given to alternative arrangements.

Emergency and crisis management procedures should be developed and rehearsed with close liaison with local government and agencies (the Local Resilience Forum) to maximize collaboration and minimize confusion in the event of attack or accidental emergency.

Organizations should maintain an emergency key contacts list including both internal (senior executives, key post holders, and deputies) and external partners (Environmental Health Officers, Trading Standards Officers, public analysts, Food Standards Agency).

All staff should be trained in emergency procedures.

Arrangements for media management and informing the public in order to minimize over-reaction to an event should be key elements of a business continuity plan. In the event of a malicious attack however, control of these activities is likely to be in the hands of the Police and the Food Standards Agency.

An effective traceability system, both upstream to ingredients and downstream of products should be developed to minimize the consequences of an attack. Product recall arrangements should be rehearsed to ensure that such procedures are as effective as possible.

Special arrangements for the disposal of contaminated materials may be necessary.

All policies relating to security and general risk management (including Business Continuity and Disaster Planning) should be overviewed and collated to ensure that there are no contradictions or anomalies and that there are appropriate supporting procedures in place.

15 Audit and review of food defence procedures

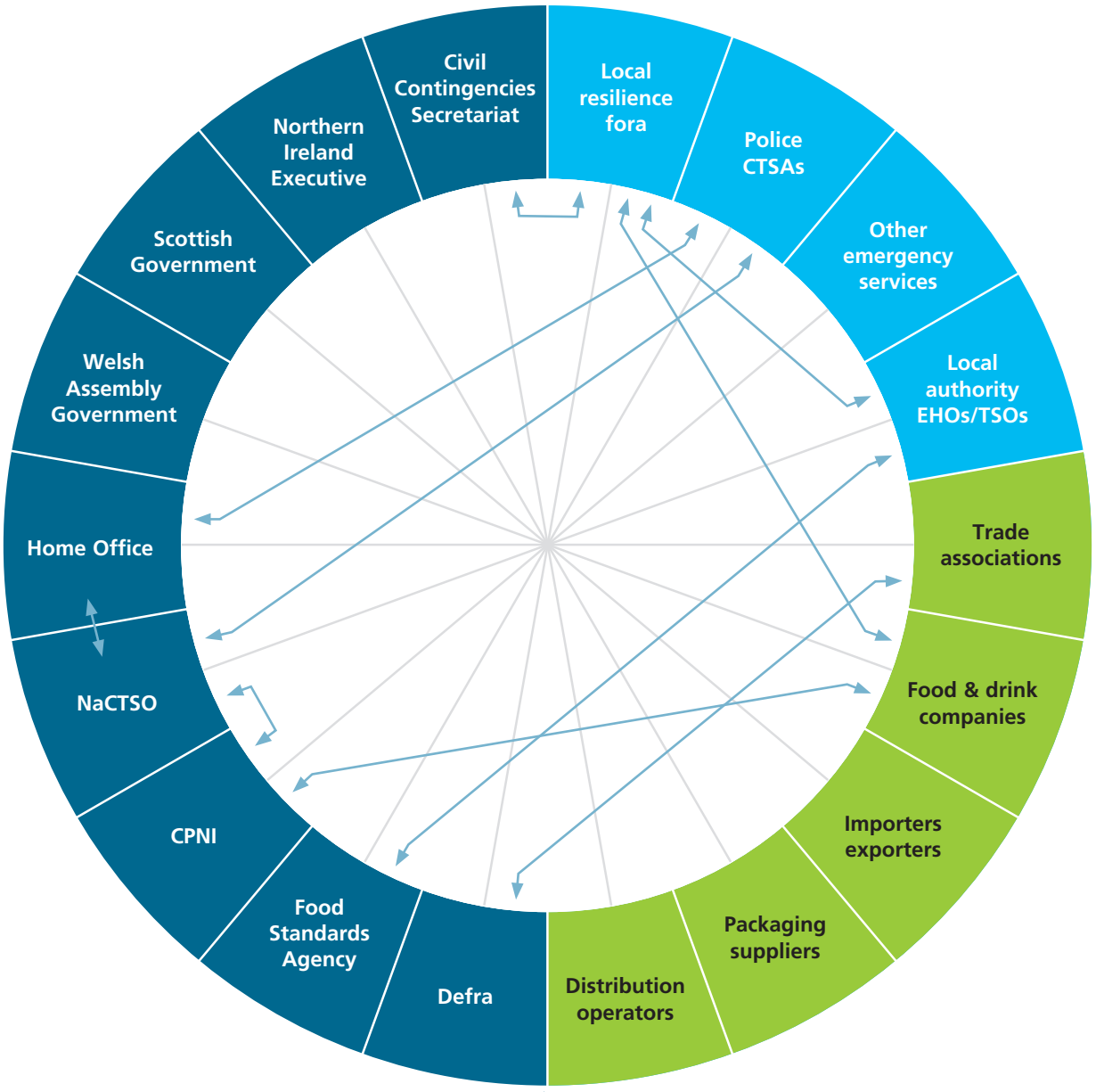
It is vital that breaches and suspected breaches of security be immediately reported to the nominated manager who will decide if a full review is needed.

The TACCP Team should monitor the Security Service website [28] for updates in the national threat assessment. The local situation can be reviewed frequently and briefly against changes to conditions pertaining at the premises. A concise report of the review should be given only limited circulation.

Effective lot (batch) coding facilitates product recall

Annex A (informative)

Organization of some key sources of advice and information



Acronym	Organization and role	Website
Government		
CCS	**The Civil Contingencies Secretariat:** Sits within the Cabinet Office at the heart of central government. It works in partnership with government departments, the devolved administrations and key stakeholders to enhance the UK's ability to prepare for, respond to and recover from emergencies.	www.cabinetoffice.gov.uk/ukresilience.aspx
CPNI	**The Centre for the Protection of National Infrastructure:** The Government authority which provides protective security advice to businesses and organizations across the national infrastructure.	www.cpni.gov.uk
Defra	**The Department for Environment Food and Rural Affairs:** Leads government work in support of a secure and sustainable food supply.	www.defra.gov.uk/foodfarm/index.htm
FSA	**The Food Standards Agency:** An independent Government department set up in 2000 to protect the public's health and consumer interests in relation to food.	www.food.gov.uk/foodindustry
Home Office	**Home Office:** Responsible for protecting the UK from the threat of terrorism.	www.homeoffice.gov.uk/counter-terrorism/index.html
NaCTSO	**The National Counter Terrorism Security Office:** A police unit co-located with the CPNI. It contributes to the UK government's counter terrorism strategy (CONTEST) by supporting the Protect and Prepare strands of that strategy. NaCTSO provides training, tasking and co-ordination of CTSAs	www.nactso.gov.uk
Northern Ireland Administration	Food supply chain resilience is one work-stream of the Civil Contingencies Policy Branch in the Office of First Minister and deputy First Minister	www.ofmdfmni.gov.uk/emergencies
The Scottish Government	Manages the resilience of food and drink supply arrangements in Scotland.	www.scotland.gov.uk/Topics/Business-Industry/Food-Industry
Welsh Assembly Government	Promotes food and drink business in Wales.	www.wales.gov.uk/topics/environment countryside/foodandfisheries/?lang=en
Local bodies		
CTSAs	**Counter Terrorism Security Advisers:** Police staff who have the core role of identifying and assessing locations within their police force area that might be vulnerable to terrorist or extremist attack.	www.nactso.gov.uk/ctsa.php
EHOs	**Environmental Health Officers:** Work within local authorities to enforce food safety law.	www.lacors.gov.uk www.cieh.org/policy/food_safety_nutrition.html
LRF	**Local Resilience Forum:** Operate at police force level and coordinate preparedness for and recovery after an emergency.	www.cabinetoffice.gov.uk/ukresilience/preparedness/ukgovernment/lrfs.aspx
Research Associations (public sector)	Government funded research and analytical/investigatory bodies such as the Institute of Food Research and The Food and Environment Research Agency	www.ifr.ac.uk www.fera.defra.gov.uk/foodDrink
TSOs	**Trading Standards Officers:** Enforce consumer protection legislation within local authorities.	www.tradingstandards.gov.uk www.lacors.gov.uk
Food and drink businesses		
Trade Associations	**Trade Associations:** Represent corporate members in their business areas and may coordinate continuity planning advice.	
Research Associations (commercial)	Membership organisations which provide consultancy and analytical services, for example Campden BRI and Leatherhead Food Research	www.campden.co.uk www.leatherheadfood.com

Annex B (informative)

Guidance for specific parts of the food and drink supply chain

B.1 Primary producers including agriculture

Many of the provisions of Assured Food Standards (the "Red Tractor Scheme") for agriculture are pertinent to food defence [2].

Farmers are strongly advised to maintain effective levels of biosecurity which minimize unnecessary contact between animals and between people and animals. It is recommended that equipment and premises be cleaned and disinfected as far as is practicable. Signs of disease should be reported as early as possible. Guidance on biosecurity can be found at www.defra.gov.uk/animalh/diseases/control/biosecurity/index.htm.

The Gangmasters Licensing Authority [29] aims to curb the exploitation of workers in the agriculture, horticulture, shellfish gathering and associated processing and packaging industries and offers advice on the use of casual teams of workers. Farmers should not assume that members of regulated gangs are necessarily trustworthy.

Farms make use of many chemicals which can be misused to cause severe harm. Agri-chemicals should be stored in a secure manner which deters theft and should be stored and handled separately from food materials and equipment. Ammonium nitrate fertiliser has been misused to make explosive devices and should be handled in accordance with NaCTSO advice [25].

B.2 Ingredients manufacturers

Mass production of ingredients may be highly automated with little manual input. Such operations should assure themselves of the integrity of contractors providing engineering services to the plant.

The Meat Hygiene Service [30] controls and advises slaughterhouse operators who should be alert to symptoms of unusual or exotic disease in the animals they handle. They will have precautionary procedures for quarantine in the event of suspected zoonotic disease.

B.3 Packaging suppliers

Producers of primary (food and drink contact) packaging should be alert to opportunities for contamination and keen to adopt rigorous personnel security practices.

B.4 Food and drink processors and packers

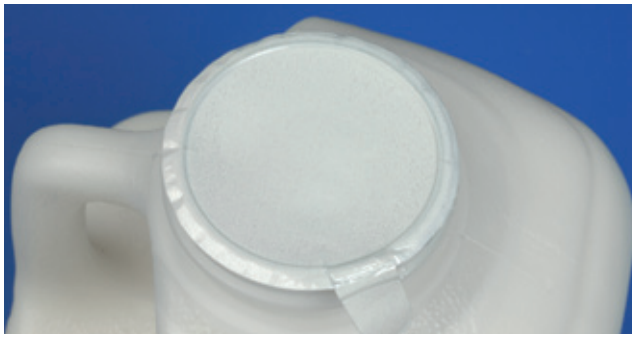
Highly labour intensive food assembly operators should recognize their considerable vulnerability to malicious, ideologically motivated attack. For example, 'just-in-time' supply of very short shelf life food products can exert great pressure for casual recruitment of staff to fill unskilled vacancies on packing lines. Should adequate pre-employment screening be impossible, employers are advised to appoint to lower risk jobs (e.g. handling packaged food only) under trusted supervision and limit access to a small strictly defined area.

Processors and packers of liquid foods including bottled water will recognize the ease with which contaminants may be dispersed through the product.

Handling of detergents and sanitizers, especially in concentrated form, is hazardous and requires skilled trained staff. The potential for misuse makes secure storage and effective stock control essential.

Storage and effective stock control are essential

The integrity of packaging is core to product protection



Diaphragm seals can give effective tamper-evidence for packs of liquid and solid foods

B.5 Transport distribution and storage

Stopovers during long distant haulage provide opportunity for malicious attack. Drivers should check tamper-evident seals (including those used on input and output ports of road tankers) after each break and before loading or off-loading and report anything unusual promptly to allow forensic investigation.

Distributors involved in transport of food products across national borders should be familiar with the Authorised Economic Operator (AEO) and Customs-Trade Partnership Against Terrorism (C-TPAT) requirements of the European Union and the USA respectively, and similar provisions of other nations.

The Road Haulage Association publishes security guidance to fleet operators [31]

B.6 Food and drink retailers

Retail outlets are public places and individuals have ready access to food products. NaCTSO has a training programme (Project ARGUS [32]) which helps retailers identify malicious behaviour at an early stage. Diligence on the shop floor can deter and detect undesirable activity.

A key threat to retailers comes from the individual or group which tampered with a packaged product then returned it to the display shelf. The integrity of packaging is core to product protection.

B.7 Caterers and restaurateurs

Being close to point-of-consumption puts employees in food service outlets into a position where they could attack the food and see the impact almost immediately. With common food contaminants, malicious attack may not be suspected and residual food could have been disposed of before symptoms appear preventing forensic examination.

Some outlets cater specifically for vulnerable groups (e.g. the elderly, those with immune deficiencies) and will want to be particularly diligent.

Caterers supplying the air travel industry will recognize strict regulations which control their operations.

Being close to point-of-consumption puts employees in food service outlets into a position where they could attack the food and see the impact almost immediately

Annex C (informative)
Defending food: A food and drink defence checklist

Business managers should select items pertinent and proportionate to their operation, and should add other Items as indicated by the TACCP process.

Table C.1 – Location of key guidance

No.	Item	Clause
1	Sound food safety practices?	5
2	Nominated responsible manager?	5
3	Effective TACCP team?	6
4	Prudent recruitment procedures?	8.1
5	Key and sensitive positions identified?	8.1
6	Prudent use of contractors and agency staff?	8.2
7	Inclusive management culture?	8.3
8	Secure boundaries?	9.1
9	Perimeter alarm system?	9.1
10	Monitoring of unauthorized access?	9.1
11	Monitored access for vehicles?	9.2
12	Are perimeter and approach roads covered by surveillance?	9.2
13	Delivery vehicles by appointment only?	9.2
14	Serial numbers of tamper-evident tags recorded?	9.2
15	Proof of identity required for visitors?	9.4
16	Positive identification of employees?	9.5
17	Vigilance training for employees?	9.5
18	Secure mail handling?	9.6
19	Nominated sensitive secure areas and jobs?	10
20	Regulated access to secure areas?	10
21	Water supplies protected?	10
22	Transport vehicles stored securely?	11
23	Sealed access to food stores, silos, trailers?	12
24	Secure storage of labels?	12
25	Secure, audited chemicals storage?	12
26	Secure lab control of toxins, pathogens, etc?	12
27	Secure protection of electronic process control systems?	13.1
28	ISO 27001 compliant electronic security procedures?	13.2
29	Casual purchases of materials by exception only?	13.3
30	Open food minimized?	13.4
31	Unique security tags used on consignments?	13.4
32	Product packages are tamper-evident?	13.4
33	Inspection of delivery vehicles before reception?	13.5
34	Sensory examination effective?	13.6
35	Crisis management procedures rehearsed?	14
36	Collaboration with neighbours and Local Resilience Forum?	14
37	Security contacts list?	14
38	Effective product traceability?	14
39	Effective product recall system?	14

Table C.2 – Checklist

No.	Item	Completed
1	Sound food safety practices?	☐
2	Nominated responsible manager?	☐
3	Effective TACCP team?	☐
4	Prudent recruitment procedures?	☐
5	Key and sensitive positions identified?	☐
6	Prudent use of contractors and agency staff?	☐
7	Inclusive management culture?	☐
8	Secure boundaries?	☐
9	Perimeter alarm system?	☐
10	Monitoring of unauthorized access?	☐
11	Monitored access for vehicles?	☐
12	Are perimeter and approach roads covered by surveillance?	☐
13	Delivery vehicles by appointment only?	☐
14	Serial numbers of tamper-evident tags recorded?	☐
15	Proof of identity required for visitors?	☐
16	Positive identification of employees?	☐
17	Vigilance training for employees?	☐
18	Secure mail handling?	☐
19	Nominated sensitive secure areas and jobs?	☐
20	Regulated access to secure areas?	☐
21	Water supplies protected?	☐

No.	Item	Completed
22	Transport vehicles stored securely?	☐
23	Sealed access to food stores, silos, trailers?	☐
24	Secure storage of labels?	☐
25	Secure, audited chemicals storage?	☐
26	Secure lab control of toxins, pathogens, etc?	☐
27	Secure protection of electronic process control systems?	☐
28	ISO 27001 compliant electronic security procedures?	☐
29	Casual purchases of materials by exception only?	☐
30	Open food minimized?	☐
31	Unique security tags used on consignments?	☐
32	Product packages are tamper-evident?	☐
33	Inspection of delivery vehicles before reception?	☐
34	Sensory examination effective?	☐
35	Crisis management procedures rehearsed?	☐
36	Collaboration with neighbours and Local Resilience Forum?	☐
37	Security contacts list?	☐
38	Effective product traceability?	☐
39	Effective product recall system?	☐

Bibliography

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

Standards publications

BS EN ISO 22000, *Food safety management systems. Requirements for any organization in the food chain*

BS EN ISO 22005, *Traceability in the food and feed chain – General principles and basic requirement for system design and implementation*

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

BS 7858, *Security screening of individuals employed in a security environment. Code of practice*

BS 25999, *Business continuity management. Part 1: Code of practice*

PAS 68, *Specification for vehicle security barriers*

PAS 69, *Guidance for the selection, installation and use of vehicle security barriers*

Other publications and websites

[1] *Terrorist Threats to Food. Guidance for Establishing and Strengthening Prevention and Response Systems*. World Health Organization. Food Safety Issues (WHO). 2008.

[2] *Assured Food Standards* (Red Tractor Scheme) (www.myredtractor.org.uk) including:

Assured British Meat (ABM) for beef and lamb

Assured British Pigs (ABP)

Assured Chicken Production (ACP)

Assured Combinable Crops Scheme (ACCS)

Assured Produce (AP) for fruit, vegetables and salad crops

Assured Dairy Farms (ADF)

and related schemes including:

Farm Assured Welsh Livestock (FAWL) (www.fawl.co.uk)

Northern Ireland Farm Quality Assurance Scheme (NIFQAS) (www.lmcni.com)

Quality Meat Scotland (QMS) (www.qmscotland.co.uk)

Genesis Quality Assurance (GQA) (www.genesisqa.com)

Soil Association Farm Assured (SAFA) (www.soilassociation.org)

[3] *Good Manufacturing Practice: A Guide to its Responsible Management*. Institute of Food Science and Technology.

[4] *Principles for Preventing and Responding to Food Incidents*. Food Standards Agency. www.food.gov.uk/foodindustry/guidancenotes/incidentsguidance/principlesdoc

[5] *BRC Global Standard for Food Safety*. British Retail Consortium.

[6] *The Safe and Local Supplier Approval Scheme*. www.salsafood.co.uk.

[7] *Secured by Design*. Association of Chief Police Officers. www.securedbydesign.com.

[8] *Risk Assessment for personnel Security: A Guide* CPNI. www.cpni.gov.uk/Docs/Risk_Assessment_Pers_Sec_Ed_2.1.pdf

[9] *Personnel Security: Threats, Challenges and Measures*. CPNI. www.cpni.gov.uk/docs/pers_sec_TCM_v2.pdf

[10] *A Good Practice Guide on Pre-Employment-Screening*. CPNI. www.cpni.gov.uk/docs/pre-employmentscreening.pdf

[11] Great Britain. *The Asylum and Immigration Act 1996*. London. The Stationery Office.

[12] Great Britain. *Data Protection Act 1998*. London. The Stationery Office.

[13] Great Britain. *The Disability Discrimination Act 1995*. London. The Stationery Office.

[14] Great Britain. *The Employment Rights Act 1996*. London. The Stationery Office.

[15] Great Britain. *The Equal Pay Act 1970 (as amended).* London. The Stationery Office.

[16] Great Britain. *The Private Security Industry Act 2001*. London. The Stationery Office.

[17] Great Britain. *The Race Relations Act 1976*. London. The Stationery Office.

[18] Great Britain. *The Race Relations Amendment Act 2000*. London. The Stationery Office.

[19] Great Britain. *The Rehabilitation of Offenders Act 1974*. London. The Stationery Office.

[20] Great Britain. *The Sex Discrimination Act 1975/86*. London. The Stationery Office.

[21] Great Britain. *The Sex Discrimination (Gender Reassignment) Regulations 1999*. London. The Stationery Office.

[22] Great Britain. *Sex Discrimination (Indirect Discrimination and Burden of Proof) Regulations 2001*. London. The Stationery Office.

[23] *Ongoing Personnel Security: A Good Practice Guide*. CPNI. www.cpni.gov.uk/Docs/HYPERLINKED_OPS_May_2009.pdf

[24] *PAS 97, A specification for mail screening and security*. BSI.

[25] *Secure Your Fertiliser. The National Counter-Terrorism Security Office*. www.secureyourfertiliser.gov.uk.

[26] *SCADA*. CPNI. www.cpni.gov.uk/protectingyourassets/scada.aspx

[27] CPNI. *Products and Services*. www.cpni.gov.uk/productsServices.aspx

[28] *Current Threat Level in the UK*. Security Service MI5. www.mi5.gov.uk

[29] *The Gangmasters Licensing Authority*. www.gla.gov.uk.

[30] *The Meat Hygiene Service*. www.food.gov.uk/foodindustry/meat/mhservice

[31] *The Road Haulage Association*. www.rha.uk.net/search?terms=security

[32] *Project ARGUS. Protecting Against Terrorist Attack*. www.nactso.gov.uk/argus.php.

BSI – British Standards Institution

BSI is the independent national body responsible for preparing British Standards. It presents the UK view on standards in Europe and at the international level. It is incorporated by Royal Charter.

Revisions

British Standards are updated by amendment or revision. Users of British Standards 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 this Publicly Available Specification would inform the Information Centre.

Tel: +44 (0)20 8996 7111
Fax: +44 (0)20 8996 7048
Email: info@bsigroup.com

BSI offers members an individual updating service called PLUS which ensures that subscribers automatically receive the latest editions of standards.

Buying standards

Orders for all BSI, international and foreign standards publications should be addressed to Customer Services.

Tel: +44 (0)20 8996 9001
Fax: +44 (0)20 8996 7001
Email: orders@bsigroup.com

Standards are also available from the BSI website at www.bsigroup.com/shop.

Information on standards

BSI provides a wide range of information on national, European and international standards through its Library. Various BSI electronic information services are also available which give details on all its products and services. Contact the Information Centre.

Tel: +44 (0)20 8996 7111
Fax: +44 (0)20 8996 7048
Email: info@bsigroup.com

Subscribing members of BSI 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)20 8996 7002
Fax: +44 (0)20 8996 7047
Email: membership@bsigroup.com

Information regarding online access to British Standards via British Standards Online can be found at www.bsigroup.com/bsol.

Further information about BSI is available on the BSI website at www.bsigroup.com.

Copyright

British Standards Institution
389 Chiswick High Road
London W4 4AL
United Kingdom
www.bsigroup.com

ISBN 978-0-580-70039-2