ASSESSING THREAT VULNERABILITY FOR FOOD DEFENCE

ADELE ADAMS & KASSY MARSH
Food defence is a term that many haven’t heard of or if they have don’t quite understand the meaning. In simple terms it’s about putting a robust plan in place to deter those wishing to deliberately contaminate food supply systems. The motivations for such actions can vary from seeking economic gain, revenge or a deliberate attempt to cause harm to consumers. While many food companies may think that it is something that does not affect them history often shows otherwise. Criminals and food terrorists will seek out those companies which are easiest to breach in terms of being the most vulnerable to attack. Having in place a system to deter such actions, in my opinion, is of immense importance in terms of protecting your business and those that consume your products.

To implement such measures can seem like a near impossible task. Where do you start as a business to think about what your points of vulnerability might be, and how a criminal or terrorist may try and exploit them? I am a great believer in implementing a systems based approach to deal with complex problems.

I have studied the system developed by Adele Adams & Kassy Marsh, to provide a shield against food business infiltration by those seeking to cause damage, either directly or indirectly. It uses the well-known and acknowledged methodology of Hazard Analysis and Critical Control Point (HACCP). To me the implementation of their system seems logical and if followed correctly, will no doubt leave your business in a much better place in terms of defending against those who seek to commit criminal activities.

Professor Chris Elliott
Professor of Food Safety & Director of the Institute for Global Food security at Queen’s University Belfast
Preface

The issue of food defence is becoming increasingly important within the food industry. As a consequence, the need for a systematic approach to the task of identification and management of threats and vulnerabilities is accelerating and becoming incorporated into industry standards.

One of the main guiding documents within this topic is the PAS 96:2014 Guide to protecting and defending food and drink from deliberate attack. Most of the currently available guidance texts use PAS 96:2014 as a foundation. This publication aims to significantly build on the basics of PAS 96:2014 through the design of a simplistic, yet detailed, scored risk assessment process resulting in the robust assessment and management of threats and vulnerabilities.

At the time of publication there is currently much debate surrounding threat and vulnerability assessment within the food industry, accompanied by a certain amount of confusion.

It would appear that the confusion stems mainly from the desire to separate the topics of threat and vulnerability assessment and to devise separate systems to manage each i.e. TACCP (Threat Assessment and Critical Control Point) and VACCP (Vulnerability Assessment and Critical Control Point). In fact, these systems should not be separated, they are closely linked and should be assessed and managed under one threat and vulnerability management system. The aim of this text is to provide guidance on how this can be successfully achieved.

This document lays out a systematic and practical solution for threat and vulnerability assessment. Based primarily on the familiar and well-accepted methodology of Hazard Analysis and Critical Control Point (HACCP), this approach combines the two elements of threat and vulnerability into one risk assessment and management system.

The utilisation of this guidance should help businesses to design and implement comprehensive threat and vulnerability management systems.

Kassy Marsh
Techni-K Consulting

Adele Adams
Adele Adams Associates
Executive Summary

The intention of the authors is to produce detailed and robust methodology for the assessment of threats and vulnerabilities. The level of detail this publication contains, in terms of explained methodology, clear scoring system, defined terminology and suggested documentation surpasses many of the existing texts which lack much of the practical detail required for successful implementation.

The main section of this publication describes how a threat and vulnerability assessment can be applied to multiple business processes such as product manufacture, distribution, recruitment and management of people. This exceeds the current requirement in some standards such as British Retail Consortium (BRC), where the requirement for a vulnerability assessment is purely limited to raw materials. If the reader's interest is restricted to covering just raw materials and the supply chain in their assessment then they may choose to skip some chapters and concentrate on 'Chapter 4: Raw Material & Supply Chain Food Fraud', which deals with assessing raw materials.

The methodology defined within this publication is based, wherever possible, on the well accepted Codex Alimentarius HACCP approach (2003), this publication assumes that the reader has a working knowledge of this. Although not an exact fit, most of the steps from the Codex 12 step logic sequence are applicable. The authors take time to explain where a direct match can or cannot be found. Drawing parallels with HACCP lessens the need to absorb and understand unfamiliar techniques and should help to increase the speed of implementation.

Although the asset being protected is the same within HACCP and within a threat and vulnerability study, i.e. the consumer (and the consequential impact on the business within a threat and vulnerability study), the types of hazards or threats are different, although some overlap exists around those that could cause harm. This publication discusses potential types of threats and contamination; however, there is potentially an infinite number which will vary depending on many factors such as the product, nature of the business, geographical location etc. This publication does not intend to go into detail on the nature or characteristics of the types of threat or potential contaminants/agents. This information is available from many sources, some of which are listed at the end of this publication, page 127.

The scored risk assessment methodology has been pioneered by the authors and much consideration, trial and error has gone into its development. It was the authors opinion that a simplistic two by two scoring matrix was too limited when there are multiple factors that contribute to the assessment of vulnerability. This is the case even when the assessment is limited to just considering vulnerabilities in the supply chain and certainly when the scope is broadened to include other business processes, such as recruitment and security.

This publication also includes the use of a unique decision tree to aid the objective identification of, what the authors have termed, 'vulnerable threat points' (VTPs). Existing terminology and definitions have been amended by the authors to accommodate the differences between HACCP and threat and vulnerability assessment requirements.
It is hoped that the information within this publication is useful and enables the effective implementation of the methodology contained within it. As an industry, we are again standing on a cliff edge, as we were when HACCP was a new concept. The implementation of HACCP was a challenge for the industry. Over time the methodology has been refined and well adapted. We are in a similar position now, with the expectation that threat and vulnerability management systems will evolve and become part of our daily business functions.

What the future might look like

As the methodology develops, it is feasible to see its use being applied to manage threats and vulnerabilities within many other subjects. The same methodology can be used to protect different assets, such as the environment, business continuity or employees. Focusing on different assets clearly alters the scope of the study, for example the focus becomes the defence of the environment from contamination as opposed to the product, or protection of employees in terms of health and safety. There are many benefits to be gained from using similar methodology to protect different assets, ultimately these can be amassed into one threat and vulnerability assessment. Although sizeable, this consolidated system should provide business with a robust and holistic threat and vulnerability management system.
Contents

Forward iii
Preface iv
Executive Summary v
New Concepts ix
Glossary x
The Need for a Threat Vulnerability Study 1
HACCP and Threat Vulnerability Assessment 2
The Stages Involved in Carrying Out a Threat Vulnerability Study 5

CHAPTER 1: PREPARATION STAGES OF A THREAT VULNERABILITY STUDY 7
Obtain Senior Management Commitment 8
Define the Scope of the Study 10
1 Structure and start and end points 10
2 Processes covered 10
3 Defining the asset 12
4 Types of threat (threat categories) 12
5 Types of threat manifestation 14
6 Types of attacker 16
7 Reference documentation, guidance and legislation 18
Select the Team 20
Construct the Process Flow Diagram 23
On-site Confirmation of Process Flow Diagram 26
Describe the Process 27
Prerequisite Programmes 29
Protection Measures 31

CHAPTER 2: ASSESSMENT STAGES OF A THREAT VULNERABILITY STUDY 35
Assessing Threat Vulnerability 36
Establish & Define the Threats 37
Threat Assessment 43
Assessing the Impact 44
Assessing the Vulnerability 46
Risk Rating & Significance 48
Establishing Protection Measures & Prerequisites 51
Establishing Threat Management Techniques - Decision Tree 52
Implementing Techniques for Threat Management 56
Management of Threats - Risk Register 57
Management of Threats - Prerequisites 58
Management of Threats - CCP 60
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management of Threats - Vulnerable Threat Point (VTP)</td>
<td>61</td>
</tr>
<tr>
<td>Documenting the Assessment</td>
<td>66</td>
</tr>
<tr>
<td><strong>CHAPTER 3: CONTINUATION STAGES OF A THREAT VULNERABILITY STUDY</strong></td>
<td>77</td>
</tr>
<tr>
<td>Review</td>
<td>78</td>
</tr>
<tr>
<td>Maintaining the system</td>
<td>79</td>
</tr>
<tr>
<td><strong>CHAPTER 4: RAW MATERIAL &amp; SUPPLY CHAIN FOOD FRAUD</strong></td>
<td>83</td>
</tr>
<tr>
<td>Raw Material &amp; Supply Chain Food Fraud</td>
<td>84</td>
</tr>
<tr>
<td>Raw Material Risk Assessment</td>
<td>86</td>
</tr>
<tr>
<td>Vulnerability Assessment</td>
<td>88</td>
</tr>
<tr>
<td>Carrying out a Raw Materials Vulnerability Assessment</td>
<td>90</td>
</tr>
<tr>
<td><strong>Appendix 1</strong> - Case study (process flow driven)</td>
<td>100</td>
</tr>
<tr>
<td><strong>Appendix 2</strong> - Case study (raw material driven)</td>
<td>121</td>
</tr>
<tr>
<td><strong>Appendix 3</strong> - Information on emerging issues</td>
<td>127</td>
</tr>
<tr>
<td><strong>References</strong></td>
<td>128</td>
</tr>
<tr>
<td><strong>About the Authors</strong></td>
<td>129</td>
</tr>
</tbody>
</table>
New Concepts

This publication introduces a number of new concepts for assessing threats and vulnerabilities, which are summarised below. These concepts should enable manufacturers to carry out and implement robust and structured assessments and management systems for threats and vulnerabilities.

**Cumulative scoring system for risk assessment**
The authors have pioneered the use of a new scoring system which takes into account the multiple factors surrounding threats and vulnerabilities, exceeding the obvious limitations of a two dimensional method.

**Protection measures**
The widely accepted terminology of ‘control measure’ is not suitable for use within a threat and vulnerability assessment as many threats can only be detected and cannot be controlled. The term ‘protection measure’ has been introduced and defined to accommodate this key difference.

**Decision tree**
The unique decision tree included in this publication provides an objective and consistent way of identifying how significant risks should be managed. The tree includes multiple management options including management via prerequisites, through a risk register, via an existing CCP or by the creation of a VTP.

**Vulnerable threat points (VTPs)**
This publication details various potential options for the management of significant risks and creates a new option, a VTP. A VTP being the food defence equivalent of a CCP. Creating this new entity allows for those points which are critical to food defence to be identified and managed in a structured way.

**Differentiation of critical limits and protection measure criteria**
The authors have recognised the fact that protection measures for threats and vulnerabilities are often not as absolute as those required for food safety. For this reason, a distinction in terminology has been created, allowing for absolutes such as testing to be differentiated from those which are less so, such as supplier auditing.

**Validation and justification**
The differentiation between protection measure critical limits and protection measure criteria continues on to the area of validation. Here, a distinction is made between science-based validation and ‘justification’. Validation is applied to absolute critical limits but is not appropriate for protection measure criteria as these are not absolute values. Here the term ‘justification’ has been introduced, this being a rationale for the selection of the criterion where science-based validation techniques cannot be applied.

**Adaptation of methodology for raw materials and for wider application**
This publication explains how a threat and vulnerability assessment can be carried out solely on raw materials and also for a much wider scope including manufacturing processes, contracted services, people flows, and distribution chains. The methodology recognises and accommodates the differences between the two assessments and adapts the methodology where required.
## Glossary

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adulterant</td>
<td>A non-permitted substance</td>
</tr>
<tr>
<td>Asset</td>
<td>The entity requiring protection</td>
</tr>
<tr>
<td>Contaminant</td>
<td>Harmful or objectionable matter</td>
</tr>
<tr>
<td>Justification</td>
<td>Subjective rationale for the effectiveness of the protection measure criteria</td>
</tr>
<tr>
<td>Protection measure</td>
<td>An action, activity or monitoring technique designed to prevent, detect or reduce a threat to an acceptable level</td>
</tr>
<tr>
<td>Protection measure - criteria</td>
<td>Criteria which contribute to a reduction in vulnerability which cannot be validated but can be justified</td>
</tr>
<tr>
<td>Protection measure - critical limits</td>
<td>A value used to define acceptability for the protection measure and can be validated</td>
</tr>
<tr>
<td>Radiological threat</td>
<td>The introduction of radioactive material</td>
</tr>
<tr>
<td>Risk register</td>
<td>A register of identified significant threats where a protection measure cannot currently be applied</td>
</tr>
<tr>
<td>TACCP</td>
<td>Threat assessment and critical control point</td>
</tr>
<tr>
<td>Threat</td>
<td>A deliberate act by someone to cause loss or harm.</td>
</tr>
<tr>
<td>VACCP</td>
<td>Vulnerability assessment and critical control point</td>
</tr>
<tr>
<td>Validation</td>
<td>Objective evidence that the protection measure is capable of delivering the required level of protection</td>
</tr>
<tr>
<td>Vulnerable Threat Point (VTP)</td>
<td>A point in the process where protection is essential in order to detect, prevent or reduce a vulnerability to an acceptable level</td>
</tr>
<tr>
<td>Vulnerability</td>
<td>How exposed the business is to the threat having an impact on the consumer</td>
</tr>
</tbody>
</table>
The Need for a Threat Vulnerability Study

The need for a threat and vulnerability study has never been greater. Well publicised incidents such as the horsemeat contamination in 2013 have focused the attention of manufacturers, retailers, enforcers and consumers on the defence of our food supply.

Within Europe the horsemeat contamination incident did highlight the significant complexity in some supply chains which was previously unknown to many of those on the receiving end. It led to challenges of largely paper based, and at times superficial, supply chain controls which relied mainly on honesty and were certainly open to abuse. It was a key factor in bringing us to where we are today, with increased controls and requirements for vulnerability assessments from those who set standards.

However, horsemeat was just one incident; threats can come from many different sources and are certainly not restricted to the supply chain. As an industry we must ensure our supply chain controls are robust and effective. However, this aim must not blinker us from potential threats from different sources, such as malicious contamination from within our own operations.

Therefore this publication, and many of the guidance documents it refers to, takes a more holistic approach when assessing threats vulnerability. This broader scope can potentially include many different business processes such as recruitment, site security, management of contractors and supervision.

Another driver for the requirement to adopt a food defence system comes from developments in the US, where food businesses have been encouraged by the Food and Drug Administration (FDA) to implement such systems. Although based on similar principles, the U.S. have their own methodology. One such model being CARVER + Shock (U.S. Food and Drug Administration 2009), originally developed by the U.S. military, which has been adapted for food use and further developed into a computerised system.
HACCP and Threat Vulnerability Assessment

There are many parallels between the methodology used within HACCP and that which is described in this text for carrying out a threat and vulnerability assessment. This familiarity is beneficial as HACCP is so widely used and, in most cases, clearly understood by the food industry, avoiding the need to reinvent the wheel.

Generally HACCP has not been widely used to identify, detect or manage deliberate contamination, even though it may be vaguely stated in the scope of some HACCP plans.

The similarities between HACCP and a threat and vulnerability assessment, as described in this publication, can include:

- Both systems require a structured and systematic approach to gain the preventative benefits and effective risk reduction
- Both systems require genuine management commitment to enable their effective design, implementation and maintenance. The key resources required, such as key people, time and training are common between both systems. Both studies have the potential to highlight necessary capital spend, it is simply the focus of this spend which differs
- The use of a team is fundamental to both systems in ensuring that the required expertise is utilised, however, the type of expertise required will differ
- Clarity of scope and terms of reference are paramount to both approaches; perhaps even more so in a threat and vulnerability assessment as the scope can be much broader than the typical product flow as required in HACCP
- Effective prerequisite programmes are vital in both systems. The purpose of prerequisite programmes remains the same, i.e. to manage general hazards not specific to a process step. However, the specific prerequisite programmes required will differ, with systems such as site security taking more of a priority within a threat and vulnerability assessment
- A detailed and accurate flow diagram is required in both systems to provide structure to the risk assessment stage. The flow diagram within a threat and vulnerability study may, depending on the defined scope, include additional business processes such as recruitment. Flow diagrams in both studies must be confirmed and signed off as being an accurate representation. If the scope is limited to assessing vulnerability of raw materials then a flow diagram will not be needed, however, a description of the supply chain process flow is beneficial
- The risk assessment element also has commonalities between both systems in such that it needs a consistent approach based on valid methodology. Within a threat and vulnerability study the risk assessment element is multi-dimensional, rather than the typically simplistic severity and likelihood approach used within a HACCP study. Due to this increased complexity a numerical system is useful. Although some texts do suggest a two-dimensional approach, it is felt that this is too simplistic for such a multi-faceted topic
The options for control measures have parallels between the two systems, i.e. prerequisite systems and CCPs in HACCP and prerequisites and VTPs (Vulnerable Threat Points) in a threat and vulnerability study. VTPs are the food defence equivalent of CCPs, i.e. points in the process where control is essential in order to prevent or reduce a vulnerability to an acceptable level. The term VTP is unique to this publication and is the result of combining the consideration of threats and vulnerabilities into one study, as opposed to the segregated approach of Threat and Critical Control Point (TACCP) and Vulnerability and Critical Control Point (VACCP).

HACCP clearly defines control measures as actions or activities used to prevent or eliminate a food safety hazard or reduce it to an acceptable level (Codex Alimentarius HACCP approach, 2003). This definition is not an exact match within a threat and vulnerability assessment as some threats may not have a robust control measure and may need to rely on a testing method to detect adulteration. Including tests (which are monitoring activities and not controls) as control measures is not accepted within HACCP and would upset many purists.

Both systems utilise a decision tree to aid the objective and consistent identification of CCPs/VTPs. Within this publication a unique decision tree has been created for the identification of VTPs or alternative options to manage the threat such as risk register, existing CCP or a prerequisite programme.

Due to their similarity, the management of the VTPs again has many elements in common with the established methodology for managing CCPs and can be documented in a similar format which is shown in later worked examples.

Validation remains an essential part of both systems and is itself attracting more emphasis in current HACCP systems. Both systems require validation, however within a threat and vulnerability assessment subjective ‘criteria’ are justified as opposed to validated, as validation requires an objective value.

The need for effective verification and review clearly applies to both systems with either system easily being rendered ineffective if neglected. The type of evidence gathered to verify each system will differ but the need for evidence of compliance remains the same. Within a threat and vulnerability assessment, verification activities rely more heavily on auditing. Instances or changes prompting review may be common to both systems or unique to either but the need to assess the potential impact of the change on the validity of the systems remains vital.

Much of the typical documentation formats for existing HACCP systems can also be used for a threat and vulnerability assessment. Using familiar formats can aid understanding of the system.

It is therefore evident that much of the existing HACCP methodology can be utilised within a threat and vulnerability assessment. However, this is not a perfect fit and the following differences should be noted.

**Areas where HACCP and a threat and vulnerability assessment can differ include:**

- The identification of the intended use and user of the product has much less relevance with a threat and vulnerability assessment. A HACCP study should already consider known instances of misuse by the consumer or customer, such as incorrect microwave heating. However these instances are rarely deliberate and although may lead to complaints, they are typically not seen as a ‘threat’. Many of the threats considered may not be harmful to the consumer therefore ‘high risk’ groups are not as pertinent as within HACCP but may still have some relevance in the consumer impact assessment.
• The term ‘control measure’ is not directly applicable within a threat and vulnerability assessment, this can be better replaced with the more relevant term of ‘protection measure’. A ‘protection measure’ is defined as ‘an action, activity or monitoring technique designed to prevent, detect or reduce a threat to an acceptable level’. This change in terminology reflects the fact that many significant risks from threats and vulnerabilities cannot be ‘controlled’, i.e. prevented, eliminated or reduced to an acceptable level. Some can only be detected by testing, such as species substitution/contamination due to criminality in the supply chain. It is a well established fact that within HACCP a ‘control measure’ differs from ‘monitoring’, the control measure being what is put in place to reduce the hazard (such as thorough cooking to reduce vegetative pathogens to a safe level) whereas the monitoring is finding out whether the control measure worked (probing product to find out if the required critical limit such as 75°C for 30 seconds was achieved). Detection is not a control, as it does not prevent, eliminate or reduce the hazard, it simply detects its presence or absence thus allowing subsequent corrective action to be taken.

• Where possible the criteria used around protection measures should include objective and measurable critical limits. This is possible with, for example, detection methods such as DNA testing. However, there will be other protection measures which contribute to a reduction in vulnerability but which cannot detect if the threat has occurred and do not control it by stopping it from happening. For example, supplier auditing may not detect or prevent a threat but it does improve the level of awareness at supplying sites as they know their systems will be scrutinised, therefore the likelihood of the threat occurring may be reduced. It is certainly not an absolute where objective critical limits could be applied but it does contribute to a reduction in vulnerability. To highlight this difference this publication utilises two terms to describe values used to define protection measures, these being ‘critical limits’ and ‘criteria’. Protection measures which can detect a threat will have ‘critical limits’ and therefore will require validation. Protection measures which provide additional control but are not an absolute will have defined ‘criteria’ which will need justification.
The Stages Involved in Carrying Out a Threat & Vulnerability Study

Preparatory Stages
- Obtain senior management commitment
- Define the scope of the study
- Select the team
- Construct process flow diagram
- Describe the process
- Define prerequisites

Assessment Stages
- Establish & define the threats
- Assess the impact
- Assess the vulnerability
- Calculate risk score & establish significance
- Define the protection measures
- Use decision tree to establish management techniques
- Implement management techniques
- Validation or justification & verification of VTPs

Continuation Stages
- Review
- Maintain the system
CHAPTER 1
PREPARATION STAGES OF A
THREAT VULNERABILITY STUDY
Obtain Senior Management Commitment

The need for management and workforce commitment applies equally to assessing and reducing threats and vulnerabilities as it does to any other management system such as HACCP. The key resources required are also likely to be similar, primarily being key people and time, both of which can be in great demand in many food businesses.

Without genuine management commitment the threat and vulnerability assessment is in danger of being a purely paper exercise to satisfy requirements with little or no impact on risk reduction. As with HACCP, gaining full attendance at regular meetings can be a challenge. However the need for a multi-disciplinary input and required expertise when carrying out threat and vulnerability assessments is just as vital and exposes the system to the same potential flaws if not achieved.

Along with the resources of people and time, the study may also highlight the need for capital expenditure such as improving security on site or increased raw material testing regimes, if identified as necessary. Any capital expenditure will also clearly need the budget holders to understand the rationale and be willing to release the required spend.

A threat and vulnerability management system cannot function with just management commitment alone. For successful risk reduction the workforce also need to be on board. In fact, many of the key controls rely on the eyes and ears of the workforce to recognise and react to threats and vulnerabilities.

As with HACCP, the findings, results and failures of the threat and vulnerability management system should be communicated back to senior management and other interested parties, to ensure that they remain aware of the effectiveness of the system. A member of the senior management team may well be part of the threat and vulnerability assessment team.

An ongoing resource will also be required to ensure the system remains effective. This may include refresher training for the team, resource of time or spend for information assessment of emerging issues or the implementation of additional protection measures.

It will be the responsibility of senior management to regularly review and maintain the risk register, which will contain known threats currently beyond the control of the organisation. Discussion of threats and items on the risk register should become part of the regular dialogue of the business and incorporated into established meetings and communication channels. This has been the case for many years for topics such as health and safety. It has taken most of the industry some time to achieve the same for food safety and raising threats and vulnerabilities to the same level may pose another challenge.
### Key points

- Management commitment is vital in ensuring that the system is taken seriously within the business and the required resources are released.

- The main resources required will be people and their time, training, access to information and perhaps an increased spend on areas such as supplier auditing or raw material testing, where necessary.

- The workforce must also be engaged and committed as they will be the ‘eyes and ears’ of the business, especially for on-site vulnerabilities.

- The commitment of both the management team and workforce must be maintained over time to allow the system to remain valid and supported.

- Management will need to take responsibility for the regular review of the risk register, where potential threats which cannot currently be controlled are listed.
Define the Scope of the Study

Agreeing and defining the scope and terms of reference of the study may be more challenging than initially expected, as a threat and vulnerability assessment does not necessarily have the neat boundaries defined within a HACCP system.

The scope and terms of reference of a threat and vulnerability assessment can potentially be very broad. Whichever way the business decides to define the scope of their assessment, the important point is to ensure that the scope is agreed, documented and followed.

The scope and terms of reference may include, but is not limited to the following:

1. Defining the start and end points of the study
2. Defining the processes covered
3. Defining the asset
4. Types of threat (threat categories)
5. Types of threat manifestation
6. Types of attacker
7. Reference documentation, guidance and legislation

1. Structure and start and end points

As with HACCP, the structure of the system should also be agreed and documented. A linear approach is simplest and helps to ensure that the system is viewed and considered in its entirety. A modular approach may be useful for larger companies with more complex business systems. Processes such as purchasing, recruitment and manufacturing could be classed as individual modules.

The start and end points of the study also require careful consideration. This will again differ from the HACCP approach where generally only steps under the direct control of the business are included with typical start and end points of intake and dispatch. As many of the threats considered within a threat and vulnerability assessment may come from the supply chain, or other external sources, the starting point clearly needs to be much further back than intake. The final stage to be considered could be defined as consumption by the consumer, as the product may be exposed to malicious contamination up until that point.

2. Processes covered

From the outset, the team must be clear about which business processes will be covered by the study. There is much flexibility here and different businesses will take their own approach to suit their specific needs. Currently many of the recent changes in industry standards, such as the BRC Global Standard Food Safety, have focused their attention predominantly, or exclusively, on the raw materials supply chain.
The team may decide to:

- Include all stages in the raw material supply chain, the internal product flow, inputs such as people, utilities, equipment, practices such as site security and follow the entire process through delivery right up until consumption
- Consider the supply chain and include assessment of potential malicious contamination on site
- Only consider the threats and vulnerabilities in the raw material supply chain in isolation, as currently required by the BRC Global Standard for Food Safety

Differing processes may need considering separately, for example:

- If the nature of the process affects the potential vulnerability. For example a process involving lots of manual input versus a process which is mainly enclosed
- If similar products differ in how they are packed and distributed. For example a retail product with tamper evident packaging versus a bulk product which is only loosely covered or tape sealed

In addition to the examples given above, potentially there will be a broad spectrum of differing sensitivities when assessing raw materials, suppliers and the supply chain.

Potentially many business processes can be included within the scope, this being clearly wider than just the intake, manufacturing and storage elements as considered within a typical HACCP study. The scope of a threat and vulnerability assessment can also include business processes such as recruitment and equipment commissioning. The following list provides some suggestions for inclusion. This is not an exhaustive list and all or many areas may not be applicable to or required by, all businesses.

- The sourcing, purchase and supply of raw materials including packaging
- The storage, preparation and manufacturing processes taking place on site
- The management of utilities/services and facilities
- Any activities such as contract packing carried out by third parties
- The storage and distribution of the finished product, including third party facilities and services
- The recruitment and management of people including agencies, contractors, visitors, access routes and security
- The management of service contracts such as catering or cleaning services
- The management of waste and by-products including animal by-products for use elsewhere
- The introduction and management of machinery and equipment

A multi-site business may carry out a study which covers various production sites; however it must be remembered that local differences, such as site security or activist groups, must be taken into account at a local level. Certain elements such as global threats may be considered by a central team or study. However, threat levels and types are likely to differ by region and certainly by country.
Defining the asset

Before progressing, the team must first be very clear about exactly which asset they are trying to protect. A system to assess threats and vulnerabilities for food defence clearly has the defence of food as its focus and objective. Therefore the scope and terms of reference can be initially defined as threats that could impact the product. It must be remembered that the fundamental asset we are trying to protect is the consumer. A food defence system clearly needs to have the product at its centre, ultimately this is in order to protect the consumer from harm, upset or repulsion. PAS 2014 states that “the focus of this PAS is on protecting the integrity and wholesomeness of food and food supply” (Department for Environment, Food and Rural Affairs (2014), PAS 96:2014 Guide to protecting and defending food and drink from deliberate attack, UK: The British Standards Institute).

The impact on the consumer must be a key consideration as any loss or harm to the business is generally due to the effect that it has on the consumer. As the team are considering threats to the product (including threats to elements which impact the product) it is valid to assume that any product-related threat which happens and reaches the market place will have an impact on the consumer in some form, ranging from upset to death. It is generally the level of impact on the consumer that drives the level of loss for the business.

It is unusual, although dependent on a talented public relations team, for any product related issue which gets into the public domain to have no financial impact on the company. Therefore the potential impact on the consumer becomes of primary concern and must be built into the threat and vulnerability assessment. This impact is not restricted to food safety, but also includes upset and or repulsion which covers potential non-harmful contamination such as incorrect species or dilution. If a threat was defined as having no potential impact to the consumer, then it is not a food defence threat and should not be included in the study.

Types of threat (threat categories)

When identifying and categorising threats, it is vital that the definition of a threat is kept in mind, this being ‘something that can cause loss or harm which arises from the ill-intent of people’ (Department for Environment, Food and Rural Affairs (2014), PAS 96:2014 Guide to protecting and defending food and drink from deliberate attack, UK: The British Standards Institute). Or, as defined by the authors, ‘a deliberate act by someone to cause harm to the consumer or loss to the business due to the effect on the consumer.’

Threats may be broadly grouped into the following categories:

- Economically motivated adulteration (EMA)
- Malicious contamination of food
- Fraudulent use of company name or branding
The threat categories listed above may manifest themselves in differing ways. These are listed differently in various texts, however, they may be grouped and summarised as shown below.

**Economically motivated adulteration**

Adulteration is the addition of something extraneous, improper or inferior. This includes:

- **Unapproved enhancements** - adding a substance to improve a characteristic e.g. melamine to increase protein content in milk powder
- **Substitution** - such as substitution of cheaper ingredient or raw material e.g. horsemeat, or a cheaper species of fish
- **Dilution** - expanding a more expensive raw material with cheaper alternatives e.g. the addition of cheaper varieties of oil to olive oil
- **Concealment** - the use of compounds for the concealment of inferior goods e.g. harmful colours on inferior fruit, use of bleach to disinfect unfit poultry meat

**Malicious contamination**

Malicious contamination is deliberately harmful in nature. This includes:

- **Malicious contamination to cause harm to the business** - e.g. by a disgruntled employee, welfare groups, or as a criminal offence by a member of the public
- **Terrorist or extremist activity** - with the intention of mass harm
- **Extortion** - adding, or claiming to have added, harmful contaminants with the purpose of financial gain

**Fraudulent use of company name or branding**

The aim of fraudulent activity is to deceive the consumer. This includes:

- **Counterfeiting** - passing off inferior goods as established brands for financial gain. This could be through the creation of counterfeit packaging and products or the theft of genuine packaging materials
- **Fraudulent labelling** - such as incorrect provenance, expired date code, non-organic being sold as organic, non-halal meat labelled as halal
- **Grey market** - this includes genuine products sold through routes which are unauthorised, unofficial or unintended by the manufacturer. Excess quantities of legitimate product are made in excess of agreed volumes for sale on the grey market. Stolen legitimate products may also end up for sale on the grey market. The black market involves the buying and selling of goods in an illegal manner

Some texts, for example PAS 96: 2014, include the threats of espionage and cybercrime. Some businesses may view these as outside the scope of the threat and vulnerability assessment as they are less likely to have a direct impact on the consumer, whilst other businesses may feel their inclusion is valid.
• Espionage, for example, theft of confidential recipe information or other intellectual property. However, there is a need for caution here, as although the threat may not have an immediate impact on the product it may lead to future counterfeiting which could cause potential upset to the consumer and loss to the company through brand damage and financial loss.

• Cybercrime, for example, the targeting of website sales which may result in theft from the consumer and the business but does not have a direct impact on the product. Therefore this is more likely to be considered under a business continuity study, or perhaps a separate assessment of cybercrime. There are ways in which cybercrime may have a more direct impact on the product, for example, hacking of a computerised business management system such as Systems, Applications and Products (SAP). Hacking of such a system may lead to a disruption in traceability, meaning product cannot be accounted for or is not located where it should be, leaving it exposed to theft or tampering.

5 Types of threat manifestation

The exact nature of the threat may be manifested in several ways. The number of manifestations for threats such as adulteration can be infinite and will vary dependent on the product, source, perpetrator or motivation. However, they are likely to belong to one of the following types. The terms ‘contamination’ or ‘agent’ may be used for some manifestations; however, these terms are not suitable for others such as, not being of the ‘legal nature’ intended. Therefore, using the term ‘threat manifestation’ is more encompassing. It must be remembered that a threat is a deliberate act.

Threat manifestations can be split into the following types:
<table>
<thead>
<tr>
<th>Type of contamination</th>
<th>Example</th>
</tr>
</thead>
</table>
| **Biological**        | • Pathogenic organisms including vegetative bacterial cells, spores and toxins such as *Clostridium botulinum* toxin  
  • Biological disease-causing agents such as smallpox or Ebola virus  
  • Parasites |
| **Chemical**          | Contaminants from the supply chain (outside the businesses activities)  
  • Misuse of chemicals in the supply chain such as pesticides or veterinary medicines  
  • Adulterants in the supply chain such as melamine in milk  
  • Environmental contaminants - toxic waste knowingly being released into the environment, e.g. the deliberate poisoning of fish stocks  
  • Chemical agents more likely to be used by terrorist organisations to contaminate product (directly or indirectly) such as cyanide or ricin  
  Deliberate contamination arising from malicious activities on site  
  • Excess additives  
  • Use of non-permitted additives  
  • Migration from substandard packaging or equipment |
| **Physical threats**  | • Deliberate physical contaminants which may cause harm, upset or repulsion to the consumer such as needles, razor blades, glass, etc. |
| **Allergic/immune response** | • Deliberate contamination by allergens |
| **Radiological threats** | • Deliberate introduction of radioactive material into food directly or indirectly |
| **Nature, substance & quality** | Deliberate actions rendering the product not of the correct:  
  • Nature  
  • Substance  
  • Quality |
Types of attacker

A threat is ‘a deliberate act by someone to cause harm to the consumer or loss to the business due to the effect on the consumer’. Therefore it is paramount to consider the people who could be involved. An awareness of motivated individuals should be a core component of the assessment. Without motivated individuals or groups the idea of an attack will not be conceived let alone carried out.

Who could the attacker be?

Understanding the potential attacker is vital in order to establish effective controls and implement these in the areas of greatest vulnerability. Potential attackers can be split into four categories relating to their proximity to the business:

- **Insiders** (e.g. current employees on permanent or temporary contracts, agency staff) are perhaps the most significant category of potential attacker due to their possibly high level of legitimate access to the production areas and products. This high level of a legitimate access can make direct product or raw material contamination much more feasible. Insiders are also likely to have the most emotional connection with the business.

- **Suppliers and contractors** (contracted staff such as security, cleaning, catering and maintenance personnel) may also have legitimate access to parts of the process. A lack of effective on-site controls may enable these trusted and familiar individuals to have easy access to sensitive parts of the operation required for an attack.

- **Supply chain personnel** (access to supply chain) may be further removed from the business with no direct contact, but may have direct access to raw materials and the finished product. These areas can be more challenging for the business to control due to their remoteness.

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

Potential attackers who are more remote from the target business may also have far less loyalty or connection with the business. In this regard, the attacker may see the business as an entity rather than a team or people with jobs and livelihoods to protect.

For a successful attack the attacker needs motivation to carry out the attack. This can be broadly considered as either being financially or ideologically driven. A successful financially motivated attack results in financial gain for the attacker, loss and cost for the business and, depending on the nature of the threat, may or may not result in harm to the consumer. Whereas a successful ideologically driven attack is more likely to result in harm to the consumer, along with loss and cost for the business, such as a terrorist contaminating a food supply with toxic agents. Simple spite of a disgruntled employee may also provide sufficient motivation for an attack.
When considering motivation, the following categories, as stated in PAS 96:2014, may be a useful starting point:

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

A successful deliberate attack on a food product or supply chain generally requires three elements to come together.

- Motivated attacker
- Capability/tactics - including the agent or contaminant
- Opportunity

If any of these elements are missing then a successful attack is unlikely. For example:

- **Lack of motivation** - an open food production process such as sandwich manufacture may seem vulnerable. However, if none of the workforce are motivated to carry out an attack then it is not likely to happen

- **Lack of capability** - an extortionist may claim to have contaminated a particular food with a harmful biological agent without any obvious access to the agent. These situations can be very hard to judge and businesses are likely to be cautious rather than take the risk of the claim being false

- **Lack of opportunity** - a disgruntled employee may have the motivation for revenge, but if the product is processed within an enclosed system to which they have no access and they are not a ‘lone worker’ then they lack the opportunity to carry out an attack

Reference documentation, guidance and legislation

Although this is a relatively new topic for many businesses, there are a number of texts which can be referred to for guidance. These will inevitably grow and be revised as the food industry gets to grips with the topic and the methodology is refined. It is therefore recommended that the team keep a list of all guidance and reference information and retain it so it can be produced on request.

There will be several pieces of pertinent legislation with relevance to threats and vulnerabilities. This text does not intend to cover or list these, however, further information can be found via the Food Standards Agency website at [www.food.gov.uk](http://www.food.gov.uk).

Retailer and industry codes of practice and standards will also be major sources of guidance for many businesses, depending on the markets they supply.

Further reading, useful websites and references can be found on page 127.
Key points

• The scope and terms of reference must be clearly defined, documented and followed
• The scope of a threat and vulnerability assessment can potentially be very broad and is certainly not as consistent as within most HACCP systems
• The scope may be limited to threats in the supply chain or broadened to include many other business processes such as the manufacture of the product, staff recruitment and site security
• The start and end points of the study will differ from HACCP, with the inclusion of supply chain steps before the raw material arrives on site
• A modular approach may be useful where additional and potentially complex business processes are defined within the scope
• The asset being protected must be clearly defined
• The number of potential threats and types of contaminant or agent is perhaps infinite, therefore a pragmatic approach coupled with expertise is essential
• The types of potential attacker must be considered, identifying the types to be included within the scope
Select the Team

Carrying out a threat and vulnerability assessment can require specialist expertise and is unlikely to be exactly the same as that required for HACCP. A multi-disciplinary approach covering the key functions of the business is required to ensure a robust system is designed. The team should also include an inter-hierarchical dimension, including junior management or operatives, as and when appropriate.

The specific constitution of the team will be driven by the defined scope and terms of reference of the study. However, a typical team for a threat and vulnerability assessment may include:

- **Security** - with knowledge of site access points and controls for deliveries, staff, visitors and contractors
- **Purchasing or supply chain staff** - including those with responsibility for ‘goods in’ with knowledge of sourcing, purchasing, acceptance and supplier management procedures
- **Production and operations staff** - with a detailed understanding of production methods, the production environment and staffing requirements
- **Technical or technologist** - with an understanding of the product characteristics and existing food safety control measures. This individual(s) may also need knowledge of the packaging system and pack security controls. Access to the consumer and customer complaints system will also be required as this may be the first indication of an incident
- **Engineer** - with knowledge of the equipment and processes used on site including those related to services, utilities and facilities
- **Distribution or logistics** - with knowledge of the storage and distribution processes and requirements, including those carried out by third parties
- **Human resources** - with responsibility for the recruitment of both permanent and temporary staff (including staff from contracted services such as cleaners or catering staff). Knowledge of on-site and third party disciplinary and grievance procedures will also be required
- **Information technology** - with knowledge of systems for the prevention of cybercrime and methods for data recovery in the event of loss (if applicable to the scope)

As with HACCP, the details of the team should be documented including:

- Name of each member
- Job role or title
- Identification of the team leader
- Individual experience and relevant knowledge
- Date of joining and leaving the team
Due to the inclusion of the supply chain within a threat and vulnerability assessment, personnel from key suppliers and customers may also need to be included. The information sources and expertise drawn on by the team will differ from much of that used within HACCP. When carrying out a threat and vulnerability study the team must ensure they look outwards for potential and emerging threats and consider global events and changes.

Larger companies may choose to establish a core threat and vulnerability assessment team and support this with additional members who can be called upon to provide specialist knowledge when required or to stand in for absent core members. Some companies may already have established teams for business continuity or risk management; overlap between such teams would be recommended to ensure efficiency and consistency of approach. Within smaller operations multiple roles may be covered by one individual thereby reducing the size of the team.

Ensuring the team have undergone training in how to carry out a threat and vulnerability assessment is vital to ensure success and prevent wasted effort and confusion. The team should also have an identified leader who can drive progress and provide feedback to senior management.

It is recommended that the team include a representative from senior management. As with any system, certain resources, particularly time and key people, will be required and senior management support will need to be in place to enable the on-going release of these resources.

To ensure the study and system can continue to function effectively, each member of the team should have a suitably experienced stand-in to cover their absence. As with HACCP, continued absence of individual members should not be tolerated due to the impact this may have on the validity of the plan.

The threat and vulnerability team have certain responsibilities which include:

- Ensuring the correct mix of expertise is available to the team
- Carrying out the threat and vulnerability study accurately and consistently
- Validating or justifying the protection measures relied upon within the study
- Implementing the measure deemed necessary within the study
- Ensuring the workforce is aware of the importance of the system and trained in the necessary protection measures as they relate to their roles
- Verifying that the protection measures are effective in reducing or detecting the identified significant risks and vulnerable threat points
- Reviewing the system in response to change, such as new information on threats, and periodically to ensure it remains valid
- Maintaining the system and the elements that support it such as the team membership, information assessment and on-site awareness

As with HACCP, it is good practice to retain minutes from the team meetings and also include information from the threat and vulnerability assessment into the management review process.
Key points

• The use of a suitably experienced and knowledgeable team is essential for the creation of a robust and valid system

• Team members should be carefully selected and their details recorded

• The composition of the team will differ from that of a typical HACCP team

• The team must draw information and expertise from a broad range of sources and take a global viewpoint

• The team must be made aware of their responsibilities

• The team must be maintained to ensure the longevity of the system
Construct the Process Flow Diagram

As with HACCP, the risk assessment element of the threat and vulnerability assessment is easier to complete if driven by a clear and accurate flow diagram of the process(es) as defined within the scope of the study. The purpose of the flow diagram is to provide a detailed illustration of the processes being considered. This is especially important for processes which may be less commonly understood across the site such as recruitment or waste management.

The following points could be included in the flow diagram, where applicable as defined in the scope, this is not an exhaustive list:

- Sequence and interaction of all steps and business processes being considered
- Inputs including raw materials, packaging, processing aids, utilities/services (such as water, steam, gas, air, coolants) and equipment
- Inputs of people (including permanent and temporary staff including agency, visitors, contractors and contracted staff, customers and auditors)
- Outputs such as finished product, intermediate products, by-products, rework, waste and recycling
- Outsourced processes and subcontracted work
- Additional flow diagrams to show further detail of specific activities should be produced where necessary

The flow diagram for a threat and vulnerability assessment may become quite complex. Ideally all the diagram should be visible on one page with a linear approach taken. However, it may be necessary to create more detailed sub flows for complex areas and processes. It is good practice to give each step a unique identification by the use of a numbering system. Arrows are useful to show the direction of flow. Colour coding can aid clarity on complex flow diagrams and it is useful to define any colours or symbols used in the process flow diagram in a key.

On the following page is an example process flow diagram for raw material and supplier approval.
1. Notification of new supplier or raw material
2. Request documentation
3. Agent/Broker requests documentation from supplier
4. Assess received documentation
5. Carry out risk assessment
6. Review of risk assessment output
6a. Supplier not approved
6b. Carry out audit
7. Approved supplier
8. Purchase raw materials
9. Assess supplier performance
10. Input new data into risk assessment

**Key**
- Optional step
- Process step
Flow diagrams should be produced for all processes defined within the scope of the study, which may include:

- The sourcing, purchase and supply of raw materials including packaging
- The storage, preparation and manufacturing processes taking place on site (this should already be in place for the existing HACCP system)
- The management of utilities/services and facilities
- Any activities carried out by third parties such as contract packing
- The storage and distribution of the finished product, included third party facilities and services
- The recruitment and management of people including agencies, contractors, visitors, access routes and security
- The management of service contracts such as catering or cleaning services
- The management of waste and by-products including animal by-products for use elsewhere
- The introduction and management of machinery and equipment

**Key points**

- A clear and accurate flow diagram is essential to ensure the process being considered is understood by the team
- The flow diagram should include detail such as the sequence and interaction of all steps, inputs, outputs and subcontracted activities
- Sub-flows or modules may be useful for complex flows or where the scope includes multiple business processes
On-site Confirmation of Process Flow Diagram

Once completed it is vital that the flow diagram is confirmed as being accurate by the team members, including additional expertise where required. Omissions or errors may result in pertinent threats and vulnerabilities being missed, leaving the businesses potentially exposed. It is useful to document the confirmation process as evidence of its completion. As within HACCP, variations across shift patterns, seasons, etc. should be taken into account.

It is good practice to ensure that the confirmed final version of the flow diagram is signed off by the team and kept up to date.

Key points

- A thorough on-site confirmation of the flow diagram is essential to ensure its accuracy
- Inaccuracies may lead to threats and vulnerabilities being missed or the inaccurate assignment of controls
- The flow diagram should be confirmed and signed off by the team
Describe the Process

The business processes which need to be described will vary according to how the team define the scope of their study, i.e. exactly which business processes are to be included. This could be a narrow scope of just the raw material supply chain or a much broader scope including inputs of personnel, services, manufacturing and forward supply chain processes. All processes included within the scope should be described.

HACCP teams will be familiar with how to describe the processes involved in production and distribution, however, additional business processes such as recruitment and human resources processes may also need describing (if included within the scope). The purpose of the process description is to provide clear information about the key parameters which are pertinent to, or influence, the level of vulnerability around the business process under consideration, such as site security protocols or packaging tamper controls.

Within HACCP systems, there is a clear requirement to describe the product in a detailed and structured way. However, this level of detail is generally not required within a threat and vulnerability assessment as the assessment focuses on the processes in and around the manufacture of the product and not purely on the product itself.

Any product detail which is required, such as packing method, ability to support pathogenic growth, allergenic content, and whether it is ready-to-eat or requires cooking by the consumer, can be included within the process description against the relevant step. Some teams may choose to create a full product description, however this is unlikely to be relevant in all circumstances.

Additional business processes which may be included within the scope, and therefore require describing, could include:

- The sourcing, purchase and supply of raw materials including packaging and any security measures such as tamper evident packaging
- The storage, preparation and manufacturing processes taking place on site
- The management of utilities/services and facilities
- Any activities carried out by third parties such as contract packing
- The storage and distribution of the finished product, included third party facilities and services, including any security measures such as seals
- The recruitment and management of people including agencies, contractors, visitors, access routes and security
- The management of service contracts such as catering or cleaning services
- The management of waste and by-products including animal by-products for use elsewhere
- The introduction and management of machinery and equipment
When compiling a description of the production process the following factors could be included:

- Areas where lone workers are permitted
- Description of storage facilities for raw materials and other product inputs along with their respective security controls such as silos
- Points in the process where the product is exposed and more vulnerable to deliberate contamination, such as de-bagging or mixing
- Areas of the process where the product is contained in equipment or protected thereby making deliberate contamination more challenging
- Pathogen reduction steps where the product may subsequently become ready-to-eat and hence deliberate post process biological contamination may pose more of a risk
- Security controls such as areas covered by CCTV
- The point at which the product becomes protected in its final packaging and the tamper evident controls of the packaging

Once completed the process description should be documented and kept up to date. An example of how to document the process description is shown within the case study.

Key points

- The content of the process description will be driven by the defined scope
- All processes included within the scope should be described
- The information within the process description should include key parameters which are pertinent to, or influence, the level of threat and vulnerability
- The process description should be documented and kept up to date
Prerequisite Programmes

The concept and purpose of prerequisite programmes (PRPs) is now well understood by the food industry. Exactly what is classed as a prerequisite continues to differ between businesses, depending on the circumstances and level of development, but they generally contain many well recognised topics.

The general idea that PRPs control general, often site-wide, hazards which are not specific to a particular process step is well accepted. Other controls such as those around critical control points (CCPs) or operational prerequisite programmes (OPPRPs) are designed to control significant food safety hazards at specific steps in the process.

For the purposes of a threat and vulnerability study, a PRP can be defined as a set of generic protection measures which are not specific to a process step.

Typical PRPs for a threat and vulnerability study may include the following, noting that not all of these will be relevant to all businesses and additional ones may be required:

- Site security - including access to systems or equipment control panels and settings
- Staff recruitment and agency management
- Storage and distribution
- Waste and by-product management
- Supervision and management
- Chemical and foreign body control
- Product packaging
- Site services/utilities
- Facilities management
- Crisis and incident management

Due to there being numerous types of threats it is difficult to produce any definitive list of relevant prerequisite programmes. This in itself would be invalid as the required prerequisites will differ and should be specific to each operation.

There will be elements of many existing prerequisite programmes that could be relevant within a threat and vulnerability study. For example, calibration may initially seem irrelevant. However, a disgruntled insider may see sabotaging the calibration of key measuring devices, such as temperature probes at heat processing steps, as a potential way of allowing under-processed product to reach the market.
One of the key catalysts for the uptake of threat and vulnerability assessments has been events in the supply chain, the most widely publicised being the horsemeat contamination in 2013. These events placed the prerequisite programme of supplier assurance under increased scrutiny. Previous to the horsemeat incident, most companies had systems in place, often placing considerable reliance on extensive supplier questionnaires, with many companies cutting back on supplier auditing due to financial or time constraints. These systems did not detect or prevent the fraudulent activity in the supply chain as routine species testing was not common place and the supply chains affected were very complex.

Within a typical HACCP system supplier assurance would generally be treated as a PRP. This is typically because, within a HACCP system, the steps before the raw material arrives on site are not included. Therefore supplier assurance is applied in its entirety as a holistic control measure at the step of intake, even though it covers a range of steps which take place before the raw material arrives on site and before a HACCP study begins.

Whereas within a threat and vulnerability assessment, the steps within the supply chain are broken down and considered individually, meaning a specific pertinent element of the supplier assurance system can be assigned as a protection measure at each step. Therefore the supplier assurance system is broken down into its component parts and individual protection measures become much more specific. Consequently, supplier assurance no longer meets the definition of a PRP (‘a set of generic controls which are not specific to a process step’) and is not treated as such.

Stating a control of ‘supplier assurance’ at each step in the supply chain is vague and fails to define exactly which elements of this sizeable system are actually being relied upon. An effective threat and vulnerability assessment requires detail. Vague and generic protection measures do not allow for specific and robust threat management.

Key points

- Prerequisite programmes play an important role in reducing the level of vulnerability
- The type and nature of the prerequisites required for threat and vulnerability management will differ in parts from those typically relied upon for food safety
- Dependent on the scope, a threat and vulnerability management system generally places much more emphasis on the supply chain and raw materials
- For the effective management of threats and vulnerabilities in the supply chain, it is necessary to dissect the supplier approval system and treat it as a series of individual protection measures which can then be assigned to the specific steps in the supply chain where they are relied upon
Protection Measures

Historically the principles of HACCP, as defined by Codex Alimentarius 2003, have defined a control measure as an action or activity which is used to prevent, eliminate or reduce a hazard to an acceptable level.

Therefore monitoring activities cannot be included as a true control measure as defined by HACCP. However, it is known that this is not always achievable and at times the only way of ensuring that the product is safe is to apply a monitor, such as a test or a check. If at this stage it was to be found to be unsafe there are procedures that would be put in place to either correct the problem or stop the product from being released.

An example is the hazard of glass or brittle hard plastic directly over open product. There is no control for this hazard, as there is currently no reasonably practicable technology that would stop a breakage of glass or brittle plastic over open product occurring. The only way to ensure that the finished product is safe is to apply a check to these items at a frequency which will ensure that any breakages are highlighted while the product is still within the control of the manufacturer. Thereby allowing any possibly affected product to be quarantined and not released to the customer or consumer.

Currently the only way of managing this restriction in HACCP is to word the monitor as a control. For example rather than stating ‘glass and brittle hard plastic checks’ the wording of ‘glass and brittle hard plastic procedures’ would be used.

Ultimately it is understood that the two above statements mean the same thing, but it does cause restrictions within the HACCP system that are not reflective of the contemporary food manufacturing industry. In addition, there is no reason to look upon the application of monitoring systems negatively in situations where no control measures can be applied, it is just a different type of management, one of reaction rather than prevention. By facing the fact that a reactive monitor is required, it actually highlights the issue and enables the application of stricter controls where necessary.

For this reason the system of assessing threats vulnerability for food defence requires a more pragmatic approach, which allows both controls and monitoring systems to be applied. To overcome this conflict the term ‘protective measures’ has been chosen.

Therefore the original HACCP definition of control (Codex Alimentarius 2003) which is:

‘An action or activity to prevent, eliminate or reduce a hazard to an acceptable level’

Is amended to become:

‘An action, activity or monitoring technique designed to prevent, detect or reduce a threat to an acceptable level’
Note that the word ‘eliminate’ has been removed as it would be too strong to state that a threat could be eliminated.

The word ‘detection’ also appears in the amended definition. Many threats will occur outside the visibility of the food processor and therefore there may be times when the only way to establish if a threat has occurred is to carry out some sort of test in order to detect it.

As with HACCP many protection measures are managed through a prerequisite programme, as discussed in the earlier prerequisite section (page 29).

**Key points**

- Protection measures are the equivalent of control measures within HACCP
- A threat and vulnerability study requires a more pragmatic approach as it lacks many of the absolutes of food safety management
- The definition of ‘protection measure’ allows for the inclusion of monitoring and detection methods
- The reference to elimination has been removed as it would be very difficult to claim or prove that a threat had been totally eliminated
- Many of the protection measures will sit within prerequisites, either existing or highlighted as necessary by the study
CHAPTER 2
ASSESSMENT STAGES OF A THREAT VULNERABILITY STUDY
Assessing Threat Vulnerability

The following section details how the threat and vulnerability assessment should be carried out.

This process involves the following stages:

- Establish and defining the threat
- Assessing each threat for impact and then vulnerability
- Using the impact and vulnerability scores to calculate the risk rating to determine significant risks
- Establishing the protection measures and prerequisites for each threat
- Putting each protection measure for each significant risk through the decision tree to identify the required management techniques, which could be:
  - Risk register
  - Prerequisite programme
  - Current CCPs
  - Vulnerable threat point (VTP)

Each of the following sections detail the requirements and process for completing each element of the threat and vulnerability assessment.
Establish & Define the Threats

A threat is something that can cause harm or loss which arises from the ill-intent of people. The pertinent threats at each process step should be listed, in line with the threat categories stated in the scope.

There are many potential threats to consider. To help with this process it can be useful to consider some specific questions under particular categories (this is not an exhaustive list).

Product & raw materials

- Have there been any significant cost increases to the raw materials being used?
- Are any of the suppliers under known financial pressure?
- Are any of the suppliers being affected by redundancies or pay issues?
- How complex is the raw material supply chain and how many steps does it include?
- Are agents or brokers used?
- Do any of the ingredients being used have provenance which makes them more at risk from substitution or adulteration?
- Are there any shortages or crop issues that may affect raw material supply, which make them more susceptible to substitution or dilution?
- Are there any raw materials that are plentiful, or overproduced?
- Are any of the ingredients organic which may make them susceptible?
- Does the product or raw materials used have significant religious significance such as kosher or halal?
- Does the product or raw materials used have any ethical or moral significance, such as animal welfare?
- Do any of the raw materials require treatment or processing that is high cost compared to other similar lower cost alternatives?
- Are any of the raw materials sourced from overseas?
- Are there any known issues with any of the raw materials?
- How are raw material access points protected, including outside storage such as silos and vessels?
- Are any of the brands or the advertising campaigns for the products controversial?
- Are any raw materials or products that are not required or substandard sent to a third party for sale or distribution?
- How are waste raw materials or product handled?
- Are raw materials delivered in a sealed vehicle?
- Is product dispatched in a sealed vehicle?
- What are the controls around re-sealing at border control for imported raw materials and exported products?
Premises & people

- Is the location of the premises politically or socially sensitive?
- Is access to the site restricted?
- Is access shared, such as public rights of way or neighbouring businesses?
- Are there controls in place to ensure employees are effectively screened prior to commencing employment?
- How are contractors managed as they arrive at site and during their work?
- How are permanent on-site contractors such as hygiene crews or caterers managed?
- How are access control systems such as key cards managed?
- How are leavers managed?
- How are services protected, such as access to water, gas and air?
- Are there any hazardous materials stored on-site and how are they protected?
- Is the site open to the public and if so, how is their security managed?
- Have there been any previous incidents of disgruntled employees?
- Have there been any instances of malicious contamination?
- Are there any business plans which may affect staff morale?
- Have there been, or are there due to be, any redundancies?
- Have there been or are there any plans for changes to pay and conditions?
- Has there been any whistle blowing activity?
- Does the site have CCTV and does it cover all areas?
- What staff supervision controls are in place?
- Is staff boredom a problem?
- Is it difficult to recruit the correct number and calibre of personnel and what risks does this pose?
- Have there been any recent health and safety issues?

Third parties

- Are third parties used to store raw materials and how is their security managed?
- Are there any links to celebrity or high profile individuals or businesses (such as branding or licensing) that may make the product more susceptible?
- Is the product or raw material transported by a number of parties and what security controls does each party use?
- Are contract manufacturers or packers used, if so how are they managed?
Customers

- Is the product being produced and delivered to any large or high profile events?
- Is the product used as an ingredient which may go into a large range of foods, leading to a wide ranging effect?

National security

- Is there a heightened level of threat from activists or terrorists?

In their shoes exercise

A useful exercise for the team to carry out is to try to put themselves in the potential attacker’s shoes and consider the following question.

“If you were the attacker what would you do, where would you do it and how?”

This ‘in their shoes’ exercise can be very enlightening and enable some free and detailed thinking.
Documenting the threat

In order to achieve a consistent result, it is beneficial to establish a defined and repeatable way of describing the threat. This will help to ensure an objective result rather than a subjective or emotive one.

In order to ensure that the threat is outlined consistently the following method can be used:

- How the asset is affected
- Caused by
- The threat and where the threat occurred
- Due to
- The motivation and the event

For illustrative purposes, an example of malicious contamination with vegetative pathogens is built up below.

How the asset is affected

As defined in the scope, the asset ultimately being protected is the consumer and the subsequent effect that the consumer has on the business. In this example, the effect on the consumer is one of harm in the form of food poisoning.

Food poisoning of the consumer

The threat and where the threat occurred

The agent or entity that caused the effect on the asset (consumer) then needs to be defined. For example, the entity that actually caused the ‘food poisoning’. It is also important to be clear about where this threat could occur, as this will affect the result of the assessment. The level of vulnerability to a threat will differ depending on where it occurs in the process. For example, it is harder for an attacker to tamper with a product once it is in its final packaging compared to when it is open during a mixing process.

When referring to biological threats it is essential to provide as much information as possible, as biological threats can be very varied in type and nature. The stated example elaborates that the pathogens are vegetative. This detail becomes important when analysing the threat, as food production processes which include heat treatment may remove the threat if it was to occur prior to the cooking process. This also emphasises the need for detail concerning where in the process the threat occurs, as heat treatment would not reduce the threat of vegetative pathogens introduced after heating. Depending on the level of heat treatment, vegetative cells may be reduced but spores may not, hence the need for detail.

The threat could be defined as follows:

Food poisoning of the consumer
Caused by
Malicious vegetative pathogenic contamination pre heat treatment
The motivation and the event

The final part of the threat detail is to define the motivation behind the threat and the event in which it would occur. It is crucial to detail why the threat would happen, i.e. the motivation and how it would occur (the opportunity).

For the examples given above, this may look as follows.

![Diagram](image)

It should be noted that the opportunity surrounding the upset employee includes the fact that they are a lone worker. It is essential to detail this, because the lone worker would have more opportunity to carry out a threat than a worker who works in a group (an accompanied worker).

The following example shows how a dismissed employee has the opportunity to carry out the threat. Without detailing that it was due to the dismissed employee not being escorted off site, it would be unclear as to what protection measure would be required to reduce this risk.

![Diagram](image)

This additional example shows how the threat could be defined for substitution of horsemeat instead of beef:

![Diagram](image)
Key points

- The threat needs to be carefully and accurately defined to enable the rest of the study to be precise
- The methodology for detailing the threat should be defined, documented and consistently applied
- Sufficient detail should be included in the threat identification to ensure that the threat is thoroughly understood and an appropriate protection measure can be applied
Assessing Threat Vulnerability for Food Defence

Threat Assessment

The aim of the threat assessment is to:

- Establish and score what impact the threat would have
- Establish and score the level of vulnerability to the threat occurring
- Define if there is a significant risk, by calculating the overall risk score
- Determine how significant threats should be managed

A two dimensional assessment such as the severity and likelihood model used within HACCP is not sufficient for assessing threats vulnerability. A multi-dimensional assessment is required, which allows for individual scores to be combined to generate an overall conclusion.

The assessment takes into account the impact on the consumer and the subsequent impact on the business, providing a system for grading and scoring the overall impact.

It then progresses to consider the vulnerability of the business to that threat. This is decided upon by considering the motivation of the attacker and the opportunity that they have to apply the threat. Again, a system for grading and scoring the vulnerability is applied.

Once an impact and vulnerability score has been achieved the system provides a technique for calculation of the risk and a cut off point which defines which risks are significant.

Once significant risks have been established the system provides a decision tree which can be used to identify how each of the protective measures should be managed.

There are four possible management techniques resulting from the use of the decision tree:

1. The threat is managed through a risk register
2. The threat is managed through the application of current prerequisites, through the amendment of a current prerequisite or introduction of a new prerequisite
3. The threat is managed through current CCPs
4. The threat is managed through the application of a vulnerable threat point (VTP)

The following sections provide further detail on each management technique, explaining how they are applied. The latter sections explain how the information generated by the study could be documented.
Assessing the Impact

The first aspect to assess is the impact that the highlighted threat could have on the asset i.e. its impact on the consumer, and the subsequent impact on the business which is driven by the effect on the consumer.

To do this objectively and consistently a scoring system for each impact is required. The following example illustrates how this may look:

<table>
<thead>
<tr>
<th>Consumer Definition</th>
<th>Score</th>
<th>Business Definition</th>
<th>Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>Death</td>
<td>9</td>
<td>Closure</td>
<td>4</td>
</tr>
<tr>
<td>Hospitalisation</td>
<td>8</td>
<td>Major financial loss</td>
<td>3</td>
</tr>
<tr>
<td>Minor harm</td>
<td>7</td>
<td>Minor financial loss</td>
<td>2</td>
</tr>
<tr>
<td>Repulsion/Disgust</td>
<td>6</td>
<td>Disruption</td>
<td>1</td>
</tr>
<tr>
<td>Upset</td>
<td>5</td>
<td>None</td>
<td>0</td>
</tr>
<tr>
<td>None</td>
<td>0</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

It must be noted that the scoring system is higher for the consumer than for the business, this is because the consumer is the primary concern. Any loss or harm to the business is generally a consequence of the effect that the threat has on the consumer, resulting in loss of sales or financial impact due to fines, recalls etc.

Unlike HACCP, repulsion and upset have been included in the impact on the consumer. Food defence is not restricted to food safety and therefore repulsion and upset of the consumer must be included. The recent horsemeat issue was found not to be a food safety concern as the positive tests for the equine painkiller bute (phenylbutazone), showed only low levels. However, the emotional angle of the issue caused upset to the consumer. In the same way it could be said that meat traces in a vegetarian meal, whilst not a food safety issue, would still cause the consumer upset, or more probably repulsion and could be a threat to the business.

This highlights that the impact to the consumer will depend on factors such as the type of product being produced and the target consumer. For example, the effect on a consumer who receives a product made of horsemeat rather than beef in the UK will be different from a consumer in countries where horsemeat is generally accepted, such as France.

Within this system, the scores for consumer impact and business impact are added together. The addition of the numbers ensures that the impact to the consumer has a greater weighting as this is the ultimate asset to protect.
Key points

- The potential impact is the first aspect to be assessed and scored
- The impact on both the consumer and the consequential impact on the business must be considered
- The impact on the consumer is given a higher weighting as the consumer is the ultimate asset to protect
- The levels of impact are not limited to food safety but also include upset and repulsion
Assessing the Vulnerability

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

Once the overall impact has been assessed, the team must progress to assess how vulnerable the business is to the highlighted threat having the defined impact.

As with impact, a scoring system for each vulnerability is required. The following example illustrates how this may look:

<table>
<thead>
<tr>
<th>Motivation</th>
<th>Opportunity</th>
<th>Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>Terrorism or extremism</td>
<td>The threat is undetectable &amp; the product is open</td>
<td>4</td>
</tr>
<tr>
<td>Fraud or extortion</td>
<td>The threat is detectable &amp; the product is open</td>
<td>3</td>
</tr>
<tr>
<td>Welfare groups</td>
<td>The threat is undetectable &amp; the product is enclosed but with access</td>
<td>2</td>
</tr>
<tr>
<td>Personal grievance or disgruntled individuals</td>
<td>The threat is detectable &amp; the product is enclosed but with access</td>
<td>1</td>
</tr>
<tr>
<td>None</td>
<td>None</td>
<td>0</td>
</tr>
</tbody>
</table>

The vulnerability to the threat has been broken down into motivation and opportunity. In order for the business to be vulnerable to the threat there has to be a motivation for the attacker to cause harm or damage and also the opportunity for them to actually be able to carry out the act.
The motivation for the attacker to carry out such an act will depend on many factors, which may vary depending on the situation. When deciding the score it is essential to think pragmatically about the worst case situation. Failure to do so will mean that the assessment needs to be updated much more frequently, each time there is change. For example, at the time of the assessment there may be no disgruntled employees, however a loss of a contract and subsequent changes to shift patterns or redundancies may change this. It is advisable to think about the worst case, keeping common sense in mind, as this will ensure the protection measures applied are more effective in a wider range of circumstances.

The motivation applied will also be influenced by:

- The product being produced, such as battery farmed eggs being targeted by animal welfare groups
- The target consumer (if this target consumer is aligned to a specific targeted group) and the country, such as countries involved in current conflicts
- The branding, such as controversial advertising campaigns
- The ethics, such as child labour

For a successful attack, the attacker must have the opportunity to carry out the act. This is generally dependent on whether the attacker has access to the target product or raw material and whether they can do this undetected.

Individuals who have access to the site such as employees, agency staff or contractors have a greater opportunity and this level of risk increases further with open product.

Perhaps the greatest risk is where the act may happen undetected. This may be due to lone workers in the production area or when the act happens outside the businesses control or visibility, e.g. during production of an ingredient or after dispatch through a third party. Therefore the scoring system shows that there is a higher risk where the act can happen undetected and also where the product is open.

As with the impact scoring, the scores for motivation and opportunity are added together to give an overall vulnerability score.

Key points

- Vulnerability is the next aspect to consider once the overall impact has been assessed
- Vulnerability is made up of two separate elements, which are motivation and opportunity
- A successful attack requires a motivated attacker with the means and opportunity to carry out the threat
Risk Rating & Significance

Once the overall scores for impact and vulnerability have been calculated, these two numbers are then multiplied together to give the risk score for that threat.

The reason for multiplying these figures is to allow situations where the motivation and opportunity score are deemed to be zero, to mitigate the impact score, giving a result of zero. This is because no matter how high the impact of the threat, if there is no vulnerability to it, there is no risk.

<table>
<thead>
<tr>
<th>Impact</th>
<th>Consumer</th>
<th></th>
<th>Business</th>
</tr>
</thead>
<tbody>
<tr>
<td>Definition</td>
<td>Score</td>
<td>Definition</td>
<td>Score</td>
</tr>
<tr>
<td>Death</td>
<td>9</td>
<td>Closure</td>
<td>4</td>
</tr>
<tr>
<td>Hospitalisation</td>
<td>8</td>
<td>Major financial loss</td>
<td>3</td>
</tr>
<tr>
<td>Minor harm</td>
<td>7</td>
<td>Minor financial loss</td>
<td>2</td>
</tr>
<tr>
<td>Repulsion/Disgust</td>
<td>6</td>
<td>Disruption</td>
<td>1</td>
</tr>
<tr>
<td>Upset</td>
<td>5</td>
<td>None</td>
<td>0</td>
</tr>
<tr>
<td>None</td>
<td>0</td>
<td>None</td>
<td>0</td>
</tr>
</tbody>
</table>

Consumer impact + business impact = impact score

<table>
<thead>
<tr>
<th>Vulnerability</th>
<th>Motivation</th>
<th>Opportunity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Definition</td>
<td>Score</td>
<td>Definition</td>
</tr>
<tr>
<td>Terrorism or extremism</td>
<td>4</td>
<td>The threat is undetectable &amp; the product is open</td>
</tr>
<tr>
<td>Fraud or extortion</td>
<td>3</td>
<td>The threat is detectable &amp; the product is open</td>
</tr>
<tr>
<td>Welfare groups</td>
<td>2</td>
<td>The threat is undetectable &amp; the product is enclosed but with access</td>
</tr>
<tr>
<td>Personal grievance or disgruntled individuals</td>
<td>1</td>
<td>The threat is detectable &amp; the product is enclosed but with access</td>
</tr>
<tr>
<td>None</td>
<td>0</td>
<td>None</td>
</tr>
</tbody>
</table>

Motivation + opportunity = vulnerability score
Impact score x vulnerability score = risk score.
### Impact

<table>
<thead>
<tr>
<th>Threat</th>
<th>Consumer</th>
<th>Business</th>
<th>Impact Score</th>
<th>Motivation</th>
<th>Opportunity</th>
<th>Vulnerability Score</th>
<th>Risk Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>Food poisoning of the consumer due to malicious spore forming pathogenic spiking of the uncooked product by upset lone worker</td>
<td>9</td>
<td>3</td>
<td>9+3=12</td>
<td>1</td>
<td>4</td>
<td>1+4=5</td>
<td>12x5=60</td>
</tr>
<tr>
<td>Upset to the consumer from Illegal by nature finished product from incorrect species due to fraudulent activity in the supply chain caused by insufficient monitoring</td>
<td>5</td>
<td>3</td>
<td>5+3=8</td>
<td>3</td>
<td>4</td>
<td>3+4=7</td>
<td>8x7=56</td>
</tr>
<tr>
<td>Illegal by quality finished product from non-halal meat being sold as halal due to fraudulent activity in the supply chain caused by insufficient monitoring</td>
<td>6</td>
<td>3</td>
<td>6+3=9</td>
<td>3</td>
<td>4</td>
<td>3+4=7</td>
<td>9x7=63</td>
</tr>
</tbody>
</table>

### Significance

A significant threat is a threat to which the consumer and subsequently the business is unacceptably vulnerable.

The methodology described in this publication uses a cut-off point for a significant threat as any score of 44 or more. The rationale for this is described below. However, it may be necessary for the business to reassess or amend this score depending on the current circumstances or business requirements.

The cut-off score of 44 has been defined by taking a minimum score for what would be deemed as a totally unacceptable impact on the consumer and the business, and similarly for motivation and opportunity, as described below.

Although it is unacceptable to cause the consumer any harm at all, it would be totally unacceptable to put them in hospital, therefore the score which would cause a significant impact to the consumer is 8 and above.

It is reasonable to expect a business to recover from a minor financial loss, however it would be much more difficult for the business to recover from a major financial loss. Therefore the score which would cause a significant impact to the business is 3 and above.

**The total significant impact score is 8 + 3 = 11.**

Any motivation by a person intending to cause harm to the consumer is totally unacceptable and therefore the score which would cause a significant motivation is 1 and above.
The opportunity for a threat to be carried out when the product is not exposed is limited, where the product is exposed the risk is higher. Therefore the score which would cause significant opportunity is where the product is open, which is 3 and above.

**The total significant vulnerability score is** \( 1 + 3 = 4 \).

These scores have then been multiplied together to give the significance score.

Therefore the overall significant score is \( 1 \times 4 = 4 \). Giving a minimum score for a threat to become significant of 44.

**Summary of scoring methodology**

- **Consumer impact + business impact = impact score**
- **Motivation + opportunity = vulnerability score**
- **Impact score x vulnerability score = risk score**

**Key points**

- The risk rating is arrived at by multiplying the overall score for impact with the overall score for vulnerability
- The multiplication of these factors allows a zero rated impact or vulnerability score to create an overall risk score of zero, where the business has no vulnerability to the threat or the threat has no impact on the consumer or business
- Within this guidance the boundary for significance has been identified as 44, based on deeming what would be totally unacceptable for the consumer impact, business impact, motivation and opportunity
Establishing Protection Measures & Prerequisites

Protection measures should be identified for each of the identified threats. Protection measures are required for both significant and non-significant risks.

As determined previously the protection measures applied can be controls or monitoring activities. The aim of the protection measure is to prevent, detect or reduce the threat to an acceptable level.

The protection measure(s) assigned to each threat may already be in place, or the threat may necessitate the identification and implementation of new protection measures, which may or may not be known.

It may be necessary to consult with internal resources such as research centres or head office specialists or where additional assistance is required, external private resource centres, trade associations or government sources.

Protection measures which prevent the threat clearly should be the first focus, however if these are not available options for detection and then reduction should be considered.

Generally, the more protection measures that can be assigned to the threat the better, as this obviously reduces the vulnerability but will also give the business more flexibility with regard to cost of implementation and maintenance.

Each protection measure should be assigned to a prerequisite programme, where applicable. In doing so it may become apparent that additional prerequisite programmes are required, which specifically manage threats. It may also be necessary to add protection measures to existing prerequisites which originally were outside the scope of the typical HACCP prerequisites.
Establishing Threat Management Techniques - Decision Tree

All significant threats should be put through the decision tree to establish how each of the protection measures should be managed.

It is expected that a higher number of threats and associated protection measures will be put through the decision tree than would be expected within a HACCP study. This is because the standard CCP decision tree only has two outputs - to be managed through the prerequisite programmes or as a CCP. However, in this threat and vulnerability methodology the decision tree allows for a number of outputs, each of which provide effective and appropriate management techniques.

Each protection measure should be considered individually, to establish how they should be managed.

The decision tree can be found on the following page.
Question 1: Can the threat be eliminated?

Yes → Implement changes to eliminate threat

No

Question 2: Is there a protection measure in place?

No → Question 2a: Can an immediate protection measure be added?

Yes → Add protection measure & reassess

No → Add to Risk Register

Yes

Question 3: Is the protection measure a generic measure managed by a PRP?

No → Question 4: Is this protection measure at this process step designed to protect against this specific threat?

Yes → Continue to manage through CCP

No → Question 5: Is this protection measure managed by an existing CCP?

Yes

Manage as a PRP

No → Add to existing PRP or generate new PRP

VTP

Question 2a: Can an immediate protection measure be added?

Yes

No → Add to Risk Register

Yes

Manage as a PRP

No → Add to existing PRP or generate new PRP

VTP
The following section explains each of the questions within the decision tree and how they should be applied. Each protection measure for each threat should be put through the decision tree individually. The result of each question should be recorded.

**Question 1: Can the threat be eliminated?**

It is important to not just accept all threats that have been identified and manage them as such. Prior to accepting the threat it should be reviewed to ensure that it cannot be eliminated and where it can, it should be.

Where threats have been identified and can be eliminated, record ‘yes’ to question 1. It is advisable to document the corrective actions applied to eliminate the threat.

If the threat cannot be eliminated answer ‘no’ and proceed to question 2.

**Question 2: Is there a protection measure in place?**

It is not always possible to apply a protection measure to every threat and therefore it is key to highlight where the consumer and the business is exposed to threats, due to the lack of protection measures.

If a protection measure can be applied, record ‘yes’ and move to question 3.

Where a protection measure is not currently in place, record ‘no’ for question 2 and move on to question 2a.

**Question 2a: Can an immediate protection measure be added?**

Review whether an immediate protection measure can be applied. Where, following a review, a protection measure can be applied, document the protection measure, any relevant prerequisites, record ‘yes’ for question 2a and reassess.

Where following a review an immediate protection measure cannot be applied, record ‘no’ for question 2a and add this threat to the risk register. For further details on the risk register, see the following threat management section (page 57).

**Question 3: Is the protection measure a generic measure managed by a PRP?**

If the protection measure is generic and is managed through a prerequisite, then no additional management is required, record ‘yes’ to question 3.

If the protection measure is not managed by a prerequisite or it is not a generic measure then additional management is required. If this is the case, record ‘no’ and move to question 4.
**Question 4: Is this protection measure at this process step designed to protect against this specific threat?**

When answering this question it is important to remember that the question applies only to the particular process step that is being assessed. If the protection measure is not specific to that process step it is considered a generic protection measure and therefore it should be managed through the prerequisites. Therefore document 'no' to question 4.

However, if the protection measure has been designed to manage the threat at this particular process step, answer 'yes' to question 4 and move on to question 5.

**Question 5: Is this protection measure managed by an existing CCP?**

If the protection measure has been designed to specifically control the threat at the process step being assessed it is possible that it may already be managed through HACCP for food safety purposes as a critical control point. Therefore, if this is the case no further management is required. If this is the case document 'yes'.

If the protection measure is not managed through HACCP as a critical control point, record 'no' to question 5. If this is the case it must be controlled as a vulnerable threat point. For more information on managing vulnerable threat points, see the following threat management section (page 61).

For each protection measure that is put through the decision tree, document the threat management system which will be either via a PRP, Risk Register, CCP or VTP.

**It must be remembered that there may be more than one protection measure for each threat and each of these protection measures may be managed in different ways.**

**Key points**

- The decision tree provides an objective and repeatable way of identifying the management technique required for the threat
- Each protection measure must be considered individually through the decision tree as their management may differ
- The results of the decision tree will be to manage the threat either via a risk register, through prerequisites (current or additional), through current CCPs or via a vulnerable threat point (VTP)
Implementing Techniques for Threat Management

Once each of the protection measures has been put through the decision tree, it will result in it being managed in one of the four ways detailed below:

1. The threat is managed through a risk register

2. The protection measure(s) for the threat are managed through the application of current prerequisites, through the amendment of a current prerequisite or introduction of a new prerequisite

3. The threat is managed through current CCPs

4. The protection measure(s) for the threat are managed through the application of a vulnerable threat point (VTP)

Each of these management techniques is explained in the following sections.
Management of Threats  
- Risk Register

In the event that a significant threat identified does not have a protection measure, it is essential that the business is aware of it, so that it can be regularly reviewed for improvement and action taken where the threat becomes real.

It may be that there are currently no protection measures available, but future developments in the industry may mean that they become available at a later date. Regular review of the risk register will ensure that these developments are included and they should be recorded.

In addition, the risk register must be reviewed following developing threats in the industry. There should be a system in place to ensure that the business has clear and defined sources of information regarding new and emerging threats. The process for reviewing this information and including it in the risk register should be defined.

The risk register should retain details of the original assessment, as well as the revised scores as the register is reviewed and amended regularly to reflect current threat impact and vulnerabilities. The rationale for including a threat on the risk register must be robust and clearly documented.

The risks must include short, medium and long-term actions for how protection measures will be implemented. Once these protection measures are available, they should be assessed again through scoring and the decision tree system.

The frequency of review and the triggers for unscheduled reviews should be defined. The minutes from reviews and actions, with close out, should be recorded within the risk register.

In the event of a threat becoming real, it is expected that this would be managed through the implementation of the crisis management system. The system must be reviewed to ensure that it provides the required processes for the threats identified on the risk register. Where there are specific requirements for the management of these threats through the crisis management system, these should be clearly detailed on the risk register. In addition, crisis management tests should include the challenge of the threats identified.
Management of Threats
- Prerequisites

Although the management of quality and food safety hazards is generally accepted and well established within the food industry, it is to be expected that when assessing threats vulnerability for food defence not all protection measures will be already included in the current set of prerequisites. It is likely that new prerequisites, such as human resources, which are not currently within HACCP prerequisites, will be required to manage food defence threats.

Therefore it is likely that when carrying out a threat and vulnerability assessment for the first time there will be changes required to the current prerequisite programmes and new topics may be created.

The decision tree assists in defining when a protection measure should be managed through the current defined prerequisite or added to the prerequisite suite, whether that is as an existing prerequisite or as a new topic.

Where the protection measure is to be managed through an existing prerequisite, the documentation for this prerequisite should be amended. The documentation should clearly show how the protection measure is managed and that this element of the prerequisite is managing a significant risk for food defence.

Where the decision tree defines that the protection measure should be added to the prerequisite suite it should be first established if a new prerequisite topic is warranted. If this is the case, the new topic documentation should be written, establishing the criteria for how the protection measure is to be managed. Again, the prerequisite documentation should clearly show that the protection measure is managing a significant risk for food defence.
4.2. Security

1.0 Purpose
Security has been defined as a prerequisite within the quality management system. The aim of this prerequisite is to ensure that raw materials, in-process product and finished products are protected from contamination.

2.0 Responsibilities
It is the responsibility of the site management team to ensure that the requirements laid out in this document are implemented and effectively enforced. The responsibility for security on the perimeter and the gatehouse has been contracted to a third party.

3.0 Food Defence - Threat Management
Security has been identified through the threat vulnerability assessment as a key protection measure, to manage:

3.1 The acceptance and approval of access of raw materials as they enter the site.
   The security guard on duty is responsible for ensuring that the driver of raw materials delivery can provide an official (with company logo) delivery note and that the company responsible for the delivery is expected and on the approved supplier list.

4.0 Quality Management

4.1 All external raw material storage areas including tanks, silos and intake pipework must be locked.
Management of Threats - CCP

Where a protection measure has been defined as being managed through an existing CCP, it should be recorded within the threat and vulnerability assessment, but no further additional management is required as HACCP takes precedence.

The HACCP plan should be updated to include, in the CCP summary, that the CCP is not only managing a food safety hazard, but has also been identified as managing a threat. The corrective action section of the CCP summary should also define the CCP failures and their corrective actions should be fed into the threat and vulnerability reviews.

<table>
<thead>
<tr>
<th>Process step</th>
<th>Hazard</th>
<th>Control measure</th>
<th>Critical limit</th>
<th>Monitoring</th>
<th>Correction &amp; Corrective Action</th>
<th>Verification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cooking</td>
<td>Pathogenic survival and subsequent outgrowth in the finished product due to insufficient heating</td>
<td>Effective cooking</td>
<td>≥85°C for 1 second</td>
<td>Core temperature of the product at the top, middle and bottom of the rack is checked, to ensure that it meets the critical limits as a minimum. Responsibility: Cooking operative Record: Ref 3.27 Cooking Record Sheet</td>
<td>Place product back into the cooker until the critical limit is achieved, or the product must be put to waste. Responsibility: Operator Record: Ref 6.12 Non conforming product form Investigation into reason for temperature failure Resp: Supervisor Record: Ref 4.28 Root cause analysis form</td>
<td>Cook record sheets checked and signed off by supervisor Complaints data Routine pathogen surveillance on finished product CCP audits</td>
</tr>
</tbody>
</table>
Management of Threats - Vulnerable Threat Point (VTP)

The main difference between CCPs and VTPs is that a CCP must be controlled to ensure that every product that is released to the consumer is safe to eat. Therefore critical limits, monitoring and frequency are designed to be effective at all times.

With vulnerable threats this is not as certain. Just because vulnerability has been identified it does not necessarily mean that the threat is consistently there. In addition, the business may be working within constraints making continuous management of the threat cost prohibitive, perhaps even making the product not cost effective to produce.

Therefore a degree of pragmatism is required and so validation of the VTPs is important. The validation of the protection measures does not always, as with CCPs, require evidence that the system is effective at all times, but can also include a degree of justification for the criteria set out by the protection measure.

The justification should take into account how many protection measures there are to manage the vulnerable threat point and their cumulative effect. It should also take into account how effective these protection measures are at controlling or detecting the threat. The justification should detail the overall level of protection through either detection measures or the number of protection measures in place.

For example, two protection measures identified to manage the VTP of threat of incorrect species of meat, due to fraudulent activity in the supply chain may be:

- Supplier auditing
- DNA testing

The supplier auditing is not a method that would detect if the threat had occurred and it does not control it by stopping it from happening. It does improve the level of awareness at the supplying site and assists in reducing the likelihood of the threat occurring. The cost of carrying out regular audits at suppliers is also expensive. The DNA testing however is a detection method, that depending on how it is applied in terms of frequency, could detect the threat of every batch of meat supplied. Testing of every batch for positive release before use may be cost prohibitive for some businesses, depending on their resources.

The validation in this situation could include the justification that the application of the two protection measures together, to allow for the frequency to be balanced to suit the business. It could be justified that the on-site auditing of the supplier would be less, perhaps six-monthly, but with an additional monthly off-site audit through a traceability exercise including mass balance. In addition, the DNA testing would support this and be carried out as surveillance, monthly rather than on a positive release basis.
Using the same theory for the threat of non-halal meat being supplied rather than halal meat, a protection measure of supplier auditing may be identified to control the VTP. Testing will not differentiate between halal and non-halal and therefore this cannot be applied as a protection measure. In this instance the validation cannot use the additional testing as justification and therefore the frequency applied to the auditing of the supplier would be greater.

In order to ensure that the vulnerable threat points are managed as effectively as possible, they should be structured in a similar way to CCPs within the HACCP system.

**Therefore the following should be established, implemented and recorded on a VTP summary:**

- Protection measures criteria, monitoring procedures and records
- Corrective actions
- Validation & justification
- Internal auditing (verification)
- Review

**Protection measures - critical limits & criteria**

For each protection measure either critical limits or criteria should be applied.

A critical limit is an objective measure, one that can be determined through validation, by proving that the limits provide the results that are required within the process specified. For example a critical limit could be applied to DNA testing, as the test would have limits for pass and fail.

A criterion is a subjective measure, one that cannot be validated, but can be justified. For example supplier auditing could not be validated, therefore the criteria for the pass or fail of an audit (such as the number of non-conformances) would need to be justified.

**Protection measures procedures & records**

For each VTP protection measure there must be a procedure which defines who is responsible, how it should be managed, when the measure should be applied and at what frequency, the critical limits or criteria and how the result should be recorded.

**Protection measure corrective actions**

The procedure must include what corrective action is required in the event of the measure not meeting the set criteria, who is responsible for applying it and when it should occur.
**Corrective action should be considered for the three main types of failure (to meet the set criteria):**

- Where the threat has occurred without detection
- Where the threat has occurred and has been detected
- Where the threat has not occurred, but the protection has been found to have failed

Where the threat has occurred and has not been detected, as a minimum the crisis management system must be implemented. Additional actions may also be required, these may include additional protection measures or increased frequency of protection measures, while the threat remains heightened.

Where the threat has occurred but has been detected and the protection measure has been successful in preventing the threat from affecting the asset (the consumer and subsequently the business) the action required will be based around removing the source of the threat.

For both instances where the threat has occurred and is thought to be criminal in nature, the necessary authorities must be notified, to allow and assist in a full investigation.

Where the threat has not occurred and the set protection measure criteria or critical limits have been found to have not been met (through supervision or internal auditing), the corrective action should be based around the prevention of a failure in the future. This should include investigation and root cause analysis as to why the protection measure was not effective.

**In all cases the corrective action applied should consider where possible:**

- Correction of the current threat
- Action to prevent the vulnerability to the threat reoccurring
- Investigation as to how the vulnerability occurred and corrective action using root cause analysis, to prevent re-occurrence

**Supplier assurance**

All vulnerable threat points (VTPs) that are related to the supply of raw materials should be fed back into the supplier assurance systems that are in place. In addition the results of the protective measures should be used as part of the supplier review process.

**Internal auditing (verification)**

Verification is defined here specifically as internal auditing. Within HACCP systems there is a range of verification activities, such as end product testing or confirmation micro testing. However, within the threat and vulnerability assessment, typical verification activities such as checks and tests are now classed as valid protection measures. Therefore the only true verification activity is internal auditing.

This makes internal auditing an essential control and therefore it is important to define the essential elements of the internal system which will verify that the protection measure is effective.
For example, when defining the key internal audit elements for the protection of DNA testing, it may include:

- Observing the operator carry out the test against the procedure
- Challenging the competency of the operator
- Ensuring that the operator is trained to the current version of the procedure
- Ensuring that the testing machine is calibrated
- Reviewing sampling techniques
- Reviewing the previous test results for compliance
- Reacting to failures and any relevant corrective actions

It is vital to ensure that the activity is well managed, through the use of trained and experienced auditors. This may require shadowing of auditors and also calibration to ensure that the results are consistent and to the required standard. Any non-conformances arising from the audits must be managed effectively and closed out in a timely manner to root cause. The results of the audits should also be trended and analysed in management meetings and threat and vulnerability reviews.

Validation & Justification

It is essential that validation and justification is documented for all protection measure(s) managing the VTP.

As detailed previously unlike HACCP, validation may include a level of justification. The first aspect to consider when working through the protection measure(s) for a VTP, is whether each protection measure requires validation or justification.

Protection measures which can detect a threat will have objective critical limits and therefore will require validation.

Protection measures which provide additional control but are more subjective will require justification.

The frequency of application of the protection measures in both cases will require a clear rationale.

All validations and justifications should be documented. The level of detail should be sufficient to explain the theory and methods used, this should allow other trained individuals to be able to follow, understand and, where necessary, replicate the data.
To do this, the following should be used as a guide when creating the document:

- **Background** - explain the threat and how it affects the asset
- **Legislation** - detail any legislation that may be applicable and explain how it impacts on the validation or justification
- **List of protection measure(s)** that manage the threat. For each protection measure it should be explained why each is either objective and therefore requires validation, or subjective and therefore requires justification
- **Where equipment is used as part of the protection measure**, the specification should be included. The functionality of the equipment should be explained and any limitations highlighted. Where there are limitations that will affect the consistency or effectiveness of the equipment these should be challenged, to show how they will be controlled
- **Establish critical limits** - if critical limits are applied, they should be challenged and the results of these challenges recorded. Where possible, trials should be carried out and for the worst case scenario, for example, at the extremes of the critical limits, to prove that they work
- **Where protection measure criteria are to be applied rather than critical limits**, the justification should be documented
- **Challenge the process** - for protection measures which have critical limits or criteria the process should be challenged, either in theory or in practice. What could happen that would cause the protection measure to be ineffective? Is there a part of the process that, if not controlled, may have an effect on the critical limits? Where these are identified they should be documented and validated or justified.
- **Review** - the frequency of review for validation or justification and what the review should include

### Key points

- The required threat management techniques should be identified using the decision tree
- A risk register is used for threats which currently have no feasible protection measure. Threats on the risk register must be regularly reviewed and included within information assessments
- Many of the required PRPs may already be in place, others may need expanding or amending to include the required protection measure. PRP documentation should show a clear link to how the significant threat is managed within the PRP
- Where existing CCPs have been identified as also controlling a threat, this should be stated on the CCP summary. Failures in CCPs should be fed back into the threat and vulnerability assessment review
- VTPs are a new concept and have many parallels with food safety CCPs
- Limits around VTPs are not as absolute as those around CCPs. VTP critical limits and criteria need careful consideration
- VTP critical limits require validation, whereas protection measure criteria require justification. Both of these should be robust and documented
- Verification within a threat and vulnerability study mainly comprises internal auditing activities
Documenting the Assessment

This section provides an example of how the threat and vulnerability assessment could be documented.

For the purpose of this guidance, it is presumed that prior to documenting the assessment, the team will have already documented their assessment methodology. The introductory information including, the team, the scope, the terms of reference, process description and confirmed flow diagram for the process(es) under consideration should also have been documented by the team.

This section provides guidance on how to document the following elements:

- Table of threat impacts
- Threat and vulnerability assessment table:
  - The threats
  - The protection measures and PRPs
  - Impact assessment
  - Vulnerability assessment
  - Overall risk scoring
  - The decision tree assessment, including the result
- Risk register
- VTP summary

Table of threat impacts

Prior to detailing the threats at each process step, it is recommended that standardised threat impacts are defined. This helps to ensure that the way in which the threats are evaluated is consistent, to both the consumer and the business. Like severity within a HACCP assessment, the impact of the threat in a vulnerability assessment is less variable and has an element of repetition.

In the same way that likelihood in HACCP is variable, the vulnerability to the threat in the assessment is variable. The variability depends on many factors, such as which process step is being evaluated and the current threat environment. However, the impact of that threat on the consumer and subsequently on the business is more than likely going to remain consistent, unless there were major business changes which would prompt their own review. Therefore the impact to the consumer and the business can be predefined and standardised, allowing them to be used consistently throughout the whole assessment. Spending time working through these will ensure that the same types of threat are assessed consistently, ensuring that the methodology determines the answer rather than any predisposed emotive response.
Using the following as an example:

‘Food poisoning of the consumer caused by malicious vegetative pathogenic contamination’

<table>
<thead>
<tr>
<th>Impact</th>
<th>Consumer</th>
<th>Score</th>
<th>Business</th>
<th>Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>Death</td>
<td>9</td>
<td>Closure</td>
<td>4</td>
<td></td>
</tr>
<tr>
<td>Hospitalisation</td>
<td>8</td>
<td>Major financial loss</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>Minor harm</td>
<td>7</td>
<td>Minor financial loss</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>Repulsion/Disgust</td>
<td>6</td>
<td>Disruption</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Upset</td>
<td>5</td>
<td>None</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>None</td>
<td>0</td>
<td>None</td>
<td>0</td>
<td></td>
</tr>
</tbody>
</table>

On assessing the impact to the consumer, vulnerable groups would need to be included and as the type of pathogen used would need to be classed as worst case, the impact result could be death. Consumer impact score would score 9.

The result of such a threat on the business would depend on the size of the business, but could be standardised for the business in question. For this example, presuming the business is a small family run operation, where the loss of sales could cause major financial loss the business impact score would be 3.

**In order to confirm why the score has been defined as 9 for the consumer and 3 for the business, it is advisable to document the theory behind it. They could look something like this:**

<table>
<thead>
<tr>
<th>Asset Threat</th>
<th>Consumer</th>
<th>Impact</th>
<th>Score</th>
<th>Business</th>
<th>Impact</th>
<th>Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>Food poisoning of the consumer</td>
<td>Food poisoning may be fatal for vulnerable groups</td>
<td>9</td>
<td>The threat may cause loss of sales which may have a major financial impact to the business</td>
<td>3</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

This process needs to be repeated for all the threats highlighted, resulting in an impact table of all the threats to the assets. This can then be used when evaluating each of the threats at each process step.

Where new threats are highlighted these should be added to the table.
Documenting the threats

As previously discussed the threat should be laid out clearly and describe:

- How the asset is affected
- Caused by
- The threat and where the threat occurred
- Due to
- The motivation and the event

In order to show how and where information should be documented the text entry points on the subsequent tables have been labelled with (step 1), (step 2) and so on.

Each threat should be listed against each process step. To do this document the process step and step reference (step 1), then number each threat for that process step (step 2) as this will assist in referencing later. Finally, list each of the threats (step 3), as shown in the example below.

<table>
<thead>
<tr>
<th>Process Step</th>
<th>Threat Reference</th>
<th>Threat</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Step 1)</td>
<td>(Step 2)</td>
<td>(Step 3)</td>
</tr>
<tr>
<td>3. Procurement</td>
<td>1</td>
<td>Upset to the consumer caused by illegal by nature ingredients at the point of delivery from incorrect species due to fraudulent activity in the supply chain, caused by insufficient monitoring</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>Repulsion to the consumer caused by illegal by quality ingredients at the point of delivery from non-halal meat being sold as halal due to fraudulent activity in the supply chain caused by insufficient monitoring</td>
</tr>
</tbody>
</table>
Documenting the impact assessment

Using the impact table assign the correct impact assessment to each threat, ensuring that for each score (steps 4) for the consumer and for the business the reason behind the score is defined (steps 5). Calculate the impact score by adding the two scores together (step 6).

<table>
<thead>
<tr>
<th>Threat</th>
<th>Consumer</th>
<th>Score</th>
<th>Business</th>
<th>Score</th>
<th>Impact Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>Upset to the consumer caused by illegal by nature ingredients</td>
<td>Consuming or purchasing a product which is not to the quality expected</td>
<td>5</td>
<td>The impact may cause loss of sales which would have a major financial</td>
<td>3</td>
<td>8</td>
</tr>
<tr>
<td>caused by fraudulent activity in the supply chain caused by insufficient monitoring</td>
<td>as it contains species which are not generally accepted for consumption would cause upset to the target consumer</td>
<td></td>
<td>impact on the business</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Repulsion to the consumer caused by illegal by quality ingredients</td>
<td>Consuming or purchasing a product which is not the quality expected</td>
<td>6</td>
<td>The impact may cause loss of sales which would have a major financial</td>
<td>3</td>
<td>9</td>
</tr>
<tr>
<td>caused by fraudulent activity in the supply chain caused by insufficient monitoring</td>
<td>as it does not meet religious requirements would cause repulsion to the target consumer</td>
<td></td>
<td>impact on the business</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

© Techni-K Consulting Ltd & Adele Adams Associates Ltd
Assessing Threat Vulnerability for Food Defence | 69
Documenting the vulnerability assessment

Repeat the exercise for the vulnerability assessment, again ensuring that the scores (steps 4) and the explanation of the score (steps 5) are included. Again, add the two scores together to give the overall vulnerability score (step 6).

<table>
<thead>
<tr>
<th>Threat</th>
<th>Motivation</th>
<th>Score</th>
<th>Opportunity</th>
<th>Score</th>
<th>Impact Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>Upset to the consumer caused by illegal by nature ingredients at the point of delivery from incorrect species due to fraudulent activity in the supply chain caused by insufficient monitoring</td>
<td>There is known fraudulent activity in the supply chain as this has occurred previously, due to the cost of fraudulent meat</td>
<td>3</td>
<td>The ingredient (meat) is out of direct control, within the supply chain and could occur undetected prior to delivery</td>
<td>4</td>
<td>7</td>
</tr>
<tr>
<td>Repulsion to the consumer caused by illegal by quality ingredients at the point of delivery from non-halal meat being sold as halal due to fraudulent activity in the supply chain caused by insufficient monitoring</td>
<td>There is known fraudulent activity in the supply chain as this has occurred previously, due to the cost of fraudulent meat</td>
<td>3</td>
<td>The ingredient (meat) is out of direct control, within the supply chain and could occur undetected prior to delivery</td>
<td>4</td>
<td>7</td>
</tr>
</tbody>
</table>
Documenting overall risk scoring

Document the overall risk scoring by multiplying the impact and vulnerability scores (Step 7). Anything above the significance score of 44 should be highlighted, to show that it should be taken through the decision tree.

<table>
<thead>
<tr>
<th>Impact Score</th>
<th>Business Score</th>
<th>Consumer Score</th>
<th>Motivation Score</th>
<th>Vulnerability Score</th>
<th>Opportunity Score</th>
<th>Risk Score</th>
<th>Step 4</th>
<th>Step 5</th>
<th>Step 6</th>
<th>Step 7</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>3</td>
<td>3</td>
<td>The ingredient (meat) is out of direct control within the supply chain and could occur undetected prior to delivery.</td>
<td>4</td>
<td>7</td>
<td>56</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>8</td>
<td>8</td>
<td>There is known fraudulent activity in the supply chain as this has occurred previously, due to the cost of fraudulent meat.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>5</td>
<td>5</td>
<td>Consuming or purchasing a product which is not to the quality expected as it contains species which are not generally accepted for consumption would cause upset to the target consumer.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Documenting the protection measures & PRPs

Document a reference for each protection measure (Step 8), then the protection measure (Step 9) and which PRP if applicable that the protection measure relates to (Step 10). The reason each protection measure is listed with its own reference, is because each one has to be taken through the decision tree individually. Giving each one its own row makes this easier and clearer to read. It is recommended that a different referencing system, than that used to reference the threats is used. For example, if threats have been referenced through a sequential number, sequential lettering could be used for protection measures.

<table>
<thead>
<tr>
<th>Protection Measures</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ref</td>
</tr>
<tr>
<td>(Step 8)</td>
</tr>
<tr>
<td>A</td>
</tr>
<tr>
<td>B</td>
</tr>
</tbody>
</table>

Documenting the decision tree assessment, including the result

In order to ensure that the answers to the decision tree questions are captured it is advisable to document them.

To document, record the answer to each question as yes or no. Where the set of questions comes to an end also record ‘stop’ and record the threat management result. The examples below demonstrate how each possible assessment route should be recorded.

<table>
<thead>
<tr>
<th>Risk Decision Tree</th>
</tr>
</thead>
<tbody>
<tr>
<td>Q1</td>
</tr>
<tr>
<td>(Step 11)</td>
</tr>
<tr>
<td>Yes, stop</td>
</tr>
<tr>
<td>No</td>
</tr>
<tr>
<td>No</td>
</tr>
<tr>
<td>No</td>
</tr>
<tr>
<td>No</td>
</tr>
<tr>
<td>No</td>
</tr>
<tr>
<td>Yes</td>
</tr>
<tr>
<td>Yes</td>
</tr>
<tr>
<td>Process step</td>
</tr>
<tr>
<td>--------------</td>
</tr>
</tbody>
</table>
| Dispatch     | Upset, repulsion or harm to the consumer caused by illegal by contamination of products at the point of dispatch or during delivery due to fraudulent activity in the distribution chain | Currently there is no evidence to suggest that there is an imminent threat. The use of security seals on each fastening point has cost and time implications which, at present, are not viewed as warranted. The ideal solution is to permanently move away from using curtain sided vehicles. Relevant standards and customers are satisfied with current protection measures | Action: Monitor changes in threat level via information assessments  
Responsibility: Threat team leader  
Timescale: As intelligence is received  
Review: 6-monthly | Action: Use security seals on each fastening point of curtain sided vehicle  
Responsibility: Transport Manager and third party haulier  
Timescale: 1 year  
Responsibility: Senior management team  
Timescale: Within 2 years  
Review: Annually |
| Open product areas | Harm to the consumer caused by malicious contamination of ingredients or product at open points during the process due to disgruntled employee | Currently there is no CCTV on site. Installing CCTV within open product areas and around site access points would involve significant capital expenditure. There are no known instances of malicious contamination by employees to date | Action: Monitor changes in staff morale and factors potentially affecting staff morale  
Responsibility: Senior management team and human resources team  
Timescale: Continuous  
Review: 6-monthly | Action: Increase the level of supervision if threat of malicious contamination increases, e.g. pay freezes or job losses  
Responsibility: Production supervisors and human resources team  
Timescale: When increased threat is identified  
Review: 6-monthly | Action: Install full CCTV system covering site access points and open product areas.  
Responsibility: Senior management team  
Timescale: Within 2 years  
Review: Annually |
### VTP summary

The following example is for illustrative purposes only.

<table>
<thead>
<tr>
<th>Process step</th>
<th>Threat</th>
<th>Protection measure</th>
<th>Critical limit /Criteria</th>
<th>Procedure &amp; Frequency</th>
<th>Corrective Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Delivery</td>
<td>Upset to the consumer by nature at the point of delivery from fraudulent activity in the supply chain</td>
<td>DNA Testing</td>
<td>Clear result for detectable non-beef DNA</td>
<td>Sample to be tested at the point of delivery on positive release basis</td>
<td>Where the threat has occurred without detection: Investigate the extent of the contamination and the root cause. Put on hold all the business's product within the business's control. Assess the scale of impact and implement withdrawal or recall where necessary. Where the threat has occurred and has been detected: Do not release ingredient and put contingency supply process for ingredient in place. Do not take any more ingredient from affected supplier until investigation of the root cause is complete</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Key audit aspects:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>- Observing the operator carry out the test against the procedure</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>- Challenge the competency of the operator</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>- Ensuring that the operator is trained to the current version of the procedure</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>- Reviewing the previous test results for compliance</td>
</tr>
</tbody>
</table>
Key points

- A threat and vulnerability assessment can be documented in various ways, this guidance provides suggested examples
- Documentation must include enough detail to withstand interrogation of the system by interested parties
- As with any system, documentation must be subject to robust controls
CHAPTER 3
CONTINUATION STAGES OF THREAT VULNERABILITY STUDY
Review

The team need to review the threat vulnerability assessment on a routine basis, the frequency of which should be defined.

The reviews should be documented and any actions arising from the review should be assigned and formally closed out.

Routine reviews should include evaluation of:

- Risk register
- VTP protection measure results, including trends where possible
- Investigations or corrective actions from protection measure failures
- Investigations or corrective actions from positive detection of threats
- Complaints
- Supplier audits, results of supplier risk assessments and supplier reviews
- Internal audits relating to threats, such as security and human resources
- Security risk assessments
- Business plans which may affect future threats and vulnerabilities
- The output of information assessment on emerging issues

Routine challenge of the crisis management system should form part of the review. This should include tests of the crisis process for the management of the specific threats within the risk register.

In addition to the routine review, additional reviews should take place when:

- Changes to the product or process occur
- Changes to staffing or human resources policies occur
- Changes to threat level or where threats occur
- New information is received through internal or third party sources, including websites
- New technologies or updates to protection measures occur
- Concerns are raised through audits, such as audits on suppliers
- Information highlights a new or emerging threat
Maintaining the system

Once implemented the system will require maintaining, which is an additional activity to review. System maintenance activities include ensuring the maintenance of elements that support the system such as, but are not limited to:

- **The team** - both in terms of members and knowledge/competency
- **The information sources** - updates, alerts, emerging issues
- **The documentation** - typically through an existing document control system

**Information Sources**

It is likely that systems for updating and keeping abreast of change are already in place as this is required in many widely used standards. However, the scope of the updating activities may need widening to include sources which may highlight potential or emerging threats.

It is a relatively easy task to draw up a list of information sources and subscribe to the updates supplied however, a structured approach of how to handle and implement changes based this information is required.

The following points provide a potential process for establishing an information system.

1. Identification of and, where appropriate, subscription to, pertinent and reliable intelligence information
2. Receipt and review of intelligence information by designated and suitably competent individual (member of the threat assessment team)
3. Pertinent issues requiring further action are escalated to management and prompt a meeting of the threat team
4. The team review the threat against the original assessment (if a known threat) and consider the threat and the possible need for further or heightened protection measures
5. Identification of further or heightened protection measures, including validation or justification of critical limits or criteria
6. Implementation of further or heightened protection measures
7. Verification of further or heightened protection measures
8. Record outcome of information assessment and continue maintenance activities

Sources of information can be found in Appendix 3.
Key points

• Review of the threat and vulnerability management system is vital to ensure its continued effectiveness
• Review should be scheduled and in response to change
• The potential triggers for a review should be documented by the team
• Records of review activities should be maintained
• Maintenance of the supporting elements of the system (the team, the information sources and documentation control) is essential
• Sourcing information plays a vital role in the identification of emerging or increasing threats
• A structured process for assessing information should be designed and implemented
CHAPTER 4
RAW MATERIAL & SUPPLY CHAIN
FOOD FRAUD
Raw Material & Supply Chain

Food Fraud

This section of the guide explains how a vulnerability assessment can be conducted solely looking at raw materials. This may be designed as a stand-alone system or as an additional module to bolt on to a broader scope, process driven assessment.

The Global Food Safety Initiative (GFSI) has been supporting a Food Fraud Think Tank, created in 2012, to look at ways in which businesses may strengthen their food safety management systems to protect consumers against harm from food fraud.

In 2014 the GFSI released a white paper – GFSI Position on Mitigating the Public Health Risk of Food Fraud, July 2014 detailing its intentions to add two food fraud mitigation steps into their guidance, which is to be issued in 2016. The guidance will include the requirement for businesses to:

1. Perform a food fraud vulnerability assessment
2. Implement a control plan

The GFSI Position on Mitigating the Public Health Risk of Food Fraud, July 2014 states that a food fraud vulnerability assessment should include an evaluation at the appropriate points along the supply chain. They define these points as being raw materials, ingredients, products and packaging. The aim here is to identify and prioritise vulnerabilities for food fraud.

Although the detail of the guidance will not be clear until it is issued in 2016, the fact that GFSI have included the terms ‘points along the supply chain’ and ‘products’, not just raw materials in their statement, alludes to the fact that it may be necessary to carry out a vulnerability assessment from raw material supply into the manufacturing site, through product processing, dispatch and perhaps further out to the delivery to the customer or consumer.

The threat and vulnerability process explained in the main body of this document will assist in the completion of this process driven assessment.

The British Retail Consortium (BRC) released its new Global Standard for Food Safety in 2015 and this is the first standard to take and implement some of the guidance from the Food Fraud Think Tank and GFSI.

The BRC Global Standard for Food Safety Issue 7 defines food fraud to be:

“Fraudulent and intentional substitution, dilution or addition to a product or raw material, or misrepresentation of the product or material, for the purposes of financial gain, by increasing the apparent value of the product or reducing the cost of its production.”
In addition, the BRC Global Standard for Food Safety Issue 7 confirms that food fraud is one element of food defence, through the following definition:

“Procedures adopted to assure the safety of raw materials and products from malicious contamination or theft”

The requirement in the standard now states that food fraud should be included by:

- Adding food fraud threats to the raw material risk assessment, for the purposes of supplier and raw material approval and performance monitoring
- Carrying out a raw material vulnerability assessment to assess the potential for substitution or adulteration

This following section of the guidance has been written to assist in the application of the new requirements specifically to meet the Global Standard Food Safety, and how the threat and vulnerability assessment previously described can be used.
Raw Material Risk Assessment

Historically raw materials risk assessments have been used to determine the method of supplier approval and monitoring, however, although the two are fundamentally linked, they have two separate aims.

The aim of a raw material risk assessment is to assess the inherent risk to safety, quality and legality from the raw materials as they are delivered to the manufacturer.

It should take into account the processes in place at the manufacturing site and also highlight any additional processes required, including acceptance criteria, treatment and testing to reduce or eliminate the potential food safety, quality or legality risks.

One crucial output of the raw material risk assessment is to define which food safety hazards must be included in the manufacturer’s HACCP plan, due to the inherent risk of the raw material. This needs to include assessment of raw materials as they come onto site, during processing into finished product and the impact on the shelf life of the finished product.

This is different from the assessment that is required for supplier approval and monitoring, although the results of the raw material risk assessment must be included. This is reiterated by the Global Standard for Food Safety Issue 7.

“The risk assessment shall form the basis for the raw material acceptance and testing procedure and for the processes adopted for supplier approval and monitoring.”

One key difference is that a raw material risk assessment can be carried out by assessing types of individual raw materials, or by assessing a group of raw materials together. Whereas a supplier risk assessment must be carried out on individual suppliers, for each of the raw materials or groups of raw materials that they supply.
This can be explained in the following example risk assessment flow below.

In order to meet the requirements of the standard, an additional assessment of substitution and fraud must be carried out as part of the raw material risk assessment. This is in addition to the original assessment for safety, quality and legality, which includes potential for allergens, foreign bodies, microbiological and chemical contamination. However, the substitution or fraud requirement of the Global Standard for Food Safety can be completed as part of the raw materials vulnerability assessment.
Vulnerability Assessment

The section of Product Authenticity, Claims & Chain of Custody of the Global Standard for Food Safety now requires a vulnerability assessment to be carried out on all food related raw materials (ingredients and packaging) or groups of raw materials.

**This should take into account:**

- Historical evidence of previous issues
- Emerging issues, which may come from information sources
- Climate and availability factors which may result in more desirable economic gains
- Ease of raw materials through the supply chain (the length and complexity of the supply chain)
- Available testing to identify fraud
- The type of raw material in question and the opportunity for fraud
- Value of the raw material
- Country of origin

It is important to understand how each of the above issues can have an effect on the raw materials being supplied, in order to be able to establish the pertinent threats that apply to the business in question.

**Historical evidence of previous issues**

Lessons from previous issues and incidents is a useful way of broadening the knowledge of what could happen today and in the future.

**Emerging issues, which may come from information sources**

Assessing information received for emerging threats in other areas of the food industry or other areas of the world, can help in pre-empting issues which may be applicable to the business. In appendix 3 there is a list of some of the resources that are available. For further details on information sources see ‘Maintaining the system’ on page 79.

**Climate and availability factors which may result in more desirable economic gains**

Adverse climate conditions can have a significant effect on crop yield, which in turn can affect the availability of food ingredients. Ingredient shortages inevitably cause price increases. Such increases can make substitution or dilution of this higher value ingredient more desirable to fraudulent individuals or companies. For raw materials that are affected by weather conditions or availability issues these threats must be included in the assessment.
Increases in demand for certain commodities such as milk, may also have the same effect of raising the price of a raw material. This may also include secondary effects, for example an increased demand for milk would have an impact on any manufacturer, where milk or its derivatives are a substantial ingredient.

Ease of raw materials through the supply chain

The more steps there are in the supply chain from farm to delivery to the manufacturer in question, the more complex the chain and the easier it is for the food to be affected. Each time a raw material changes hands, the lines of responsibility are challenged and could be open to abuse.

Agents and brokers are now under pressure to ensure that they take responsibility for the raw materials while they are under their custody. They must understand where the materials they are buying and selling have come from.

In order to reduce the risk it may be necessary to reduce the number of steps within the process and buy raw materials directly from manufacturers, rather than purchasing them through longer distribution chains. Where this is not possible the threats incurred within long supply chains should be included in the vulnerability assessment.

Available testing to identify fraud

Testing to identify fraud should be used where possible, but the actual testing for fraud should be classed as a protection measure (see ‘Protection Measures’ on page 31), rather than a threat. As testing methods develop, the opportunity to implement more effective testing to highlight fraud will give greater control. In the meantime, the lack of testing for significant threats should be managed through the risk register (see ‘Management of Threats - Risk Register’ on page 57).

The type of raw material in question and the opportunity for fraud

The type of raw material can increase its susceptibility to fraud and this may be due to the similar visual appearance of two materials. A whole chicken compared to a whole turkey may clearly be different, however when it is processed such as mincing or dicing – the two types of meat may appear the same. The same would be true for ingredients which should have been produced in a defined way, such as organic, kosher or halal.

Value of the raw material

The higher the value of the raw material, the more likely it will be at risk from substitution, adulteration or dilution, due to the economic gain involved. Raw materials, which in essence look the same but one may have provenance and so greater value, would be at risk, for example comparing Stilton with a generic blue cheese.

Country of origin

The country of origin of particular raw materials can give them valued provenance, such as olive oil from Italy or Mānuka honey from New Zealand or Australia, whereas on face value the material looks the same.
Carrying out a Raw Materials Vulnerability Assessment

To meet the requirements of the BRC Global Standard for Food Safety the raw materials can be assessed individually or in groups. The vulnerability assessment can be added to an existing raw material risk assessment, as long as it takes into account all of the threats discussed in the previous section and there is documented information and methodology supporting it.

The methodology described in the main body of this guidance can be used to conduct this vulnerability assessment, with a few amendments to make it specific to assessing threats by raw material, rather than by process steps.

To aid understanding of the method to be applied, it is highly recommended that the main body of this guidance is read prior to working through this section.

As discussed in the main body of the guide Supplier & Raw Material Approval & Performance Monitoring, cannot be classed as a prerequisite programme for threat and vulnerability assessments. This is because prerequisites are a set of generic activities; they are not specific to one point of the process. In the case of a raw material vulnerability assessment this point is even more essential as supplier assurance is very specific to the assessment and therefore cannot be classed as a prerequisite.

The flow chart on the following page shows the method that should be used to conduct a vulnerability assessment of raw materials.
Preparatory Stages

- Obtain senior management commitment
- Define the scope of the study
- Select the team
- Describe the raw materials & the supply chain process

Assessment Stages

- Establish & define the threats
- Assess the impact
- Assess the vulnerability
- Calculate risk score & establish significance
- Define the protection measures
- Use decision tree to establish management techniques
- Implement management techniques
- Validation or justification & verification of VTPs

Continuation Stages

- Review
- Maintain the system
In order to explain each of these steps and the particular points that are key when assessing raw materials, each step has been broken down and where applicable referenced back to the main sections of this guidance where additional detail is given.

1. Preparatory Stages

Obtain senior management commitment

As with an assessment carried out against a process flow, it is essential to obtain senior management commitment. The Senior Management Commitment section of The Global Standard for Food Safety has been expanded to include the need for senior manager reviews to encompass an evaluation of food defence and authenticity. For further information on obtaining senior management commitment see section ‘Obtain Senior Management Commitment’ on page 8.

Define the scope of the study

In order to ensure that the study covers all of the elements required and it is clear which are in and out of scope, the scope and terms of reference must be agreed and documented.

The scope and terms of reference may include the following, but is not limited to:

- Describe the raw materials and the supply chain process
- The claims on pack, which may attract fraud
- Types of threat manifestation
- Types of attacker
- Reference documentation, guidance and legislation

Further information can be found in the section ‘Define the Scope of the Study’ from page 10.

Select the team

Details on selecting the team can be found in section ‘Select the Team’ on page 20. However, when carrying out a vulnerability assessment of just the raw materials the members of the team would be biased towards any specialists in raw material purchasing, approval and supply.

Describe the raw materials and the supply chain process

The raw materials to be assessed should be listed and where grouping is carried out, it should describe how the groups are established and which raw materials are included in each group.

For a process driven threat and vulnerability assessment the scope defines the start and end points of the study in order to be able to put together the required process flow(s) and how the flow(s) will be laid out (linear or modular). Clearly with raw material assessments a process flow does not need to be included, but it essential to define what parts of the supply chain are to be included.
The process (supply chain) for the raw materials that are delivered to the business must be included. It is important to ensure that all key elements of the raw material supply are explained for each raw material or group of raw materials. This should include where materials are purchased through agents or brokers.

**To do this, the supply chain steps can be detailed with the raw material or group of raw materials, as shown below.**

<table>
<thead>
<tr>
<th>Raw Material/ Raw Material Group</th>
<th>Supply Chain Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Liquid egg</td>
<td>Farm &gt; processing plant &gt; agent &gt; delivery</td>
</tr>
<tr>
<td>Olive oil</td>
<td>Producer &gt; processing plant &gt; broker importer &gt; agent &gt; delivery</td>
</tr>
</tbody>
</table>

**Claims on pack**

Listing all the claims on pack within the scope, is a really good way of pinpointing where there may be opportunity for food fraud. Using this list, it is then possible to work through these, to establish if there are any associated threats.

**Prerequisites**

Typically the only prerequisite that would be applicable here would be Supplier & Raw Material Approval & Performance Monitoring. However, Supplier & Raw Material Approval & Performance Monitoring cannot be applied as a prerequisite as it does not manage generic activities, it includes a very specific set of activities designed to manage raw materials.

There are no other prerequisites that would be applicable to raw material assessment and therefore they do not apply to this type of assessment. For this reason, prerequisites have been removed as a management technique for threats that apply to raw materials and so reference to them has been removed from the decision tree.

**2. Assessment Stages**

**Establish and define the threats**

Clearly the threats that are documented need to be those that are specific to the raw materials and their supply chain. This must take into account the elements as defined by the Global Standard for Food Safety and explained previously. Where there are no pertinent threats for a raw material or a group of raw materials, it may be appropriate to add a statement in the assessment next to the raw material which says “There are currently no known threats pertinent to this raw material”.

There is more information on how to establish the threats and also a list of questions which will aid the team’s discussion in section ‘Establish & Define the Threats’ on page 37.

**Assess the impact and vulnerability**

The definitions and measures for assessing the impact of the threats and the vulnerabilities are shown below, for ease of use. If further details are required, they can be found in ‘Assessing the Impact’ on page 44 and ‘Assessing the Vulnerability’ on page 46.
Impact Assessment:

<table>
<thead>
<tr>
<th>Impact</th>
<th>Consumer</th>
<th>Score</th>
<th>Business</th>
<th>Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>Death</td>
<td>9</td>
<td></td>
<td>Closure</td>
<td>4</td>
</tr>
<tr>
<td>Hospitalisation</td>
<td>8</td>
<td></td>
<td>Major financial loss</td>
<td>3</td>
</tr>
<tr>
<td>Minor harm</td>
<td>7</td>
<td></td>
<td>Minor financial loss</td>
<td>2</td>
</tr>
<tr>
<td>Repulsion/Disgust</td>
<td>6</td>
<td></td>
<td>Disruption</td>
<td>1</td>
</tr>
<tr>
<td>Upset</td>
<td>5</td>
<td></td>
<td>None</td>
<td>0</td>
</tr>
<tr>
<td>None</td>
<td>0</td>
<td></td>
<td>None</td>
<td>0</td>
</tr>
</tbody>
</table>

Consumer impact + business impact = impact score

Vulnerability Assessment:

<table>
<thead>
<tr>
<th>Vulnerability</th>
<th>Motivation</th>
<th>Score</th>
<th>Opportunity</th>
<th>Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>Terrorism or extremism</td>
<td>4</td>
<td></td>
<td>The threat is undetectable &amp; the product is open</td>
<td>4</td>
</tr>
<tr>
<td>Fraud or extortion</td>
<td>3</td>
<td></td>
<td>The threat is detectable &amp; the product is open</td>
<td>3</td>
</tr>
<tr>
<td>Welfare groups</td>
<td>2</td>
<td></td>
<td>The threat is undetectable &amp; the product is enclosed but with access</td>
<td>2</td>
</tr>
<tr>
<td>Personal grievance or disgruntled individuals</td>
<td>1</td>
<td></td>
<td>The threat is detectable &amp; the product is enclosed but with access</td>
<td>1</td>
</tr>
<tr>
<td>None</td>
<td>0</td>
<td></td>
<td>None</td>
<td>0</td>
</tr>
</tbody>
</table>

Motivation + opportunity = vulnerability score

Impact score x vulnerability score = risk score
Calculate risk score & establish significance

A significant risk score for this method is deemed to be 44 or more. However, the business may decide that their situation or the product they produce makes it necessary to redefine this boundary. A summary of the calculation is shown below.

**Consumer impact + business impact = impact score**

**Motivation + opportunity = vulnerability score**

**Impact score x vulnerability score = risk score**

Define the protection measures

The definition of protection measures is detailed in section ‘Protection Measures’ on page 31.
Carry out the threat and vulnerability assessment

Assess each of the significant protection measures through the decision tree. The tree for assessment of raw materials has been slightly amended so that it is specific to the assessment of non-process driven threats, as shown below.

Question 1: Can the threat be eliminated?

Yes → Implement changes to eliminate threat

No

Question 2: Is there a protection measure in place?

Yes → Question 2a: Can an immediate protection measure be added?

Yes → Add protection measure & reassess

No → Add to Risk Register

No

Question 3: Is this protection measure designed to protect against this specific threat?

No

Question 4: Is this protection measure managed by an existing CCP?

Yes → Continue to manage through CCP

No → Manage through supplier management procedures

VTP
The following pages explain each of the questions within the decision tree and how they should be applied. Each protection measure for each threat should be put through the decision tree individually. The result of each question should be recorded.

**Question 1: Can the threat be eliminated?**

It is important to not just accept all threats that have been identified and manage them as such. Prior to accepting the threat it should be reviewed to ensure that it cannot be eliminated and where it can, it should be.

Where threats have been identified and can be eliminated, record ‘yes’ to question 2. It is advisable to document the corrective actions applied to eliminate the threat.

If the threat cannot be eliminated answer ‘no’ and proceed to question 2.

**Question 2: Is there a protection measure in place?**

It is not always possible to apply a protection measure to every threat and therefore it is key to highlight where the consumer and the business is exposed to threats, due to the lack of protection measures.

If a protection measure can be applied, record ‘yes’ and move to question 3.

Where a protection measure is not currently in place, record ‘no’ for question 2 and move on to question 2a.

**Question 2a: Can an immediate protection measure be added?**

Review whether an immediate protection measure can be applied. If following a review, an immediate protection measure can be applied, document the protection measure, record ‘yes’ for question 2a and reassess.

Where following a review a protection measure cannot be immediately applied, record ‘no’ for question 2a and add this threat to the risk register. For further details on the risk register, see the following threat management section.

**Question 3: Is this protection measure designed to protect against this specific threat?**

When answering this question it is must be remembered that the question asks if the protection measure is designed to protect against a specific threat.

The protection measure of routine supplier audits which assess the compliance of the supplier to the quality management system is not specifically designed to protect against a specific threat. It is designed to protect against a range of issues, not just threats.

However, an audit designed around the protection of a specific threat, such as mass balance for Mānuka honey, or a provenance audit would be specifically designed to manage a specific threat.

It is important when defining the protection measures to establish if the protection measure identified is
specific enough.
If the protection measure identified is not specific, document 'no' to question 3. The criteria around this protection measure must be added to the supplier management procedures.

If the protection measure has been specifically designed to manage this specific threat, answer 'yes' to question 3 and move on to question 4.

**Question 4: Is this protection measure managed by an existing CCP?**

If the protection measure has been designed to specifically control the specific threat being assessed it is possible that it may already be managed through HACCP for food safety purposes as a critical control point. Therefore, if this is the case no further management is required. If this is the case document 'yes'.

If the protection measure is not managed through HACCP as a critical control point, record 'no' to question 4. If this is the case it must be controlled as vulnerable threat point. For more information on managing vulnerable threat points, see the following threat management section.

For each protection measure that is put through the decision tree, document the threat management system which will be either via the Risk Register, a CCP, a VTP or through Supplier Management Procedures.

It must be remembered that there may be more than one protection measure for each threat and each of these protection measures may be managed in different ways.

**Establish & implement management techniques**

From the decision tree the management techniques can be established as either an existing CCP, the risk register, a vulnerable threat point (VTP) and additionally for raw material assessment, through supplier management procedures.

The management technique of prerequisite programmes has been removed, as they do not apply to raw material assessment.

Details on how each of these management techniques should be conducted are described in the sections ‘Implementing Techniques for Threat Management’ from page 56, with the exception of supplier management procedures, which is detailed below.

**Supplier management procedures**

Where there is a protection measure in place that is not designed to protect against a specific threat, but that threat is significant, the management technique to be applied should be supplier management procedures. These may need to be reviewed to ensure that they are robust enough to manage the protection measure effectively.

The result of the raw materials vulnerability assessment must be included in the supplier approval and monitoring risk assessment, to ensure that protection measures for the significant threats are included.
By using the diagram used previously on page 87 the vulnerability assessment can be incorporated and it would now look as follows:

Validation or justification & verification of VTPs

For details of how to conduct validation, justification and verification of VTPs see ‘Management of Threats - Vulnerable Threat Point (VTP)’ on page 61.

3. Continuation Stages

Maintain the system
Maintenance of the system must be carried out, and is defined in section ‘Maintaining the system’ on page 79.

Review
Reviews must be carried out in-line with the requirements set out in section ‘Review’ on page 78.
Appendix 1
Case study (process flow driven)

Vegetarian Sausages Threat & Vulnerability Assessment

This case study has been created to give an example of how the methodology described in the guide can be applied in practice.

It does not include all the threat and vulnerability assessment – but just extracts.

For the utilities process, only the water input has been provided as part of the example.

This example is fictitious and for illustrative purposes only.

Site background information

The case study is based on a vegetarian sausage product produced by a medium sized, independent manufacturer called Veggie Sausages Ltd, supplying branded product to discount retailers. The case study focuses on process driven assessments and considers a selected number of steps through the scoring system.
Veggie Sausages Ltd

Threat & Vulnerability Assessment

Scope

The aim of this study is to identify and manage the potential threats and vulnerabilities to the product, which could have an impact on the consumer and thereby a consequential impact on the business.

This assessment is for vegetarian sausages and covers the activities of:

- The storage, preparation and manufacturing processes taking place on site
- The management of utilities/services and facilities
- Any activities such as contract packing carried out by third parties
- The storage and distribution of the finished product, included third party facilities and services
- The recruitment and management of people including agencies, contractors, visitors, access routes and security

The study is split into modules of the sausage manufacturing process (including utilities) and people flow.

There are separate flow charts for sausage manufacturing (including utilities) and people flow and these are linear in structure.

Start and end points - Sausage Production
The study starts at receipt of raw materials and finishes at delivery to customer depot for the manufacturing flow.
Raw materials are not included in the scope of this study, the company has carried out a separate vulnerability assessment for raw materials.

Start and end points - Utilities
The study starts at intake from the supplier through to usage in the process, waste is not included in the scope of this study.

Start and end points - People
The study starts at the application form and finishes at escort off site in the event of dismissal.
Types of threat

The types of threat covered by this study include:

1. Deliberate contamination of, tampering with, persuasion of or substitution of inputs into the process such as:
   - people
   - utilities such as water or air supply which can have a direct impact on product.
2. Fraudulent use of company name, product or branding such as fraudulent use of packaging to pack inferior product into for sale or sale of surplus product on grey market
3. Deliberate adulteration, substitution or dilution on site due to price or supply pressures.

Types of manifestation of threats

This study considers the following categories, although this is not an exhaustive list:

<table>
<thead>
<tr>
<th>Biological including:</th>
<th>Chemical including:</th>
</tr>
</thead>
<tbody>
<tr>
<td>pathogenic organisms</td>
<td>excess additives</td>
</tr>
<tr>
<td>biological disease causing agents</td>
<td>use of non-permitted additives</td>
</tr>
<tr>
<td>parasites</td>
<td>chemicals used on site such as cleaning or engineering chemicals (inks and solvents)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Physical including:</th>
</tr>
</thead>
<tbody>
<tr>
<td>needles</td>
</tr>
<tr>
<td>razor blades</td>
</tr>
<tr>
<td>glass</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Allergenic / immune response agents including:</th>
</tr>
</thead>
<tbody>
<tr>
<td>milk</td>
</tr>
<tr>
<td>gluten (Wheat, Rye, Barley, Oats)</td>
</tr>
<tr>
<td>celery</td>
</tr>
<tr>
<td>egg</td>
</tr>
<tr>
<td>fish</td>
</tr>
<tr>
<td>crustacean</td>
</tr>
<tr>
<td>molluscs</td>
</tr>
<tr>
<td>sesame</td>
</tr>
<tr>
<td>soya</td>
</tr>
<tr>
<td>lupin</td>
</tr>
<tr>
<td>mustard</td>
</tr>
<tr>
<td>nuts</td>
</tr>
<tr>
<td>peanuts</td>
</tr>
<tr>
<td>sulphites</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Radiological including:</th>
</tr>
</thead>
<tbody>
<tr>
<td>radioactive material</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Not of the:</th>
</tr>
</thead>
<tbody>
<tr>
<td>nature</td>
</tr>
<tr>
<td>substance</td>
</tr>
<tr>
<td>quality</td>
</tr>
</tbody>
</table>
## Team

<table>
<thead>
<tr>
<th>Name</th>
<th>Job Role</th>
<th>Number of years with the company/experience in the industry</th>
<th>Joined team</th>
<th>Training</th>
<th>Team Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Julia Brown</td>
<td>Technical Manager</td>
<td>3 years with company as Technical Manager. 15 years experience in technical management in food industry</td>
<td>Jan 2014</td>
<td>One day threat &amp; vulnerability course November 2014</td>
<td>Core member Team Leader</td>
</tr>
<tr>
<td>David White</td>
<td>Production Manager</td>
<td>2 years with the company as Production Manager. 12 years experience in a variety of manufacturing roles</td>
<td>Jan 2014</td>
<td>One day threat &amp; vulnerability course November 2014</td>
<td>Core member</td>
</tr>
<tr>
<td>Simon Green</td>
<td>Engineering Manager</td>
<td>10 years with the company. 12 years experience in food engineering</td>
<td>Jan 2014</td>
<td>One day threat &amp; vulnerability course November 2014</td>
<td>Core member</td>
</tr>
<tr>
<td>Steve Smith</td>
<td>Goods in Supervisor</td>
<td>1 year with the company. 6 years experience in various warehouse roles</td>
<td>Dec 2014</td>
<td>In-house briefing from team leader December 14</td>
<td>Core member</td>
</tr>
<tr>
<td>Helen Davies</td>
<td>Head Buyer</td>
<td>4 years with the company. 8 years experience in food procurement</td>
<td>Jan 2014</td>
<td>One day threat &amp; vulnerability course November 2014</td>
<td>Core member</td>
</tr>
<tr>
<td>Fred Greaves</td>
<td>Logistics Manager</td>
<td>15 years with the company. 20 years experience in logistics management</td>
<td>Jan 2014</td>
<td>One day threat &amp; vulnerability course November 2014</td>
<td>Core member</td>
</tr>
<tr>
<td>Katherine Holmes</td>
<td>Human Resources Administrator</td>
<td>6 months with the company. 3 years experience in HR roles</td>
<td>Jan 2015</td>
<td>In-house briefing from team leader January 2015</td>
<td>Core member</td>
</tr>
</tbody>
</table>
Prerequisite programmes

The prerequisites that support this system include:

- Site security
- Human resources
- Training and competency of staff
- Supervision and management
- Internal auditing
- Supplier approval
- GMP
- Chemical control
- Foreign body control
- Cleaning

Further details of each prerequisite system can be found in the relevant Quality Management System documentation.
Process Flow - Sausage Manufacturing & Utilities

1. Raw material intake
2. Storage
   Chilled <5°C or ambient
3. De-bag/de-box
   3a. Packaging
4. Weigh up
5. Transfer to mixer
6. Mixing
7. Forming
8. Transfer to fryer
9. Flash frying
   9a. Oil intake
   9b. Oil storage
   9c. Filtration 3mm
10. Transfer to freezer
11. Blast freezing
12. Transfer to packing
13. Packing into cartons
   13a. Cartons
14. Glue
15. Date coding
16. Weighing
17. Pack into boxes
   17a. Boxes & tape
18. Palletise
   18a. Pallets
19. Shrink wrapping
   19a. Shrink wrap
20. Metal detection
21. Frozen storage ≤ -18°C
22. Vehicle loading
23. Vehicle sealing
24. Transport to depot
25. Delivery at depot

Utilities Process
U1. Mains water infeed
U2. Water storage

Product Process
9. Flash frying
   9b. Oil storage
   9c. Filtration 3mm
21. Frozen storage ≤ -18°C
22. Vehicle loading
23. Vehicle sealing
24. Transport to depot
25. Delivery at depot

Key
Utilities Process Step
Product Process Step
## Describe the process

<table>
<thead>
<tr>
<th>Process Flow Step</th>
<th>Detail</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>1. Raw material intake</strong></td>
<td>The ingredients for the sausages are bought in from approved suppliers</td>
</tr>
<tr>
<td><strong>2. Storage chilled or ambient</strong></td>
<td>Ingredients are stored within a secure goods in warehouse. Access to the warehouse is controlled by swipe card. Delivery drivers ring a bell to alert the warehouse staff of their arrival. At times staff in the warehouse may be ‘lone workers’</td>
</tr>
<tr>
<td><strong>3. De-bag/ de-box</strong></td>
<td>Ingredients are de-boxed or de-bagged and weighed in the weighing-up room. This is the first step at which the product is exposed</td>
</tr>
<tr>
<td><strong>4. Weigh up</strong></td>
<td>Personnel in the weighing-up room often work alone, especially at quieter times</td>
</tr>
<tr>
<td><strong>5. Transfer to mixer</strong></td>
<td>Ingredients are transferred to the production area where they are added to the mixer either in a tote bin via a hoist or manually depending on quantity. Tote bins should be covered during transit. Line 1 has a lidded hopper on the mixer. Line 2 has an open mixer hopper, due to the design it is not possible to fit a lid</td>
</tr>
<tr>
<td><strong>U1. Mains water infeed</strong></td>
<td>The main utility used on site which has contact with the product is water. This is drawn from a mains potable water supply provided by the local water company. Treatment and testing criteria and testing results are available from the local water company and accessed by the company for information</td>
</tr>
<tr>
<td><strong>U2. Water storage</strong></td>
<td>Water is held in short term storage tanks on site before being used. These tanks are external to the factory buildings, but located within the site boundaries and are protected by site security controls and additionally by robust padlocks at access points</td>
</tr>
<tr>
<td><strong>6. Mixing</strong></td>
<td>There are two mixers which feed two different lines. Line 1 is a more modern line with less manual input, line 2 has older equipment which requires more manual input</td>
</tr>
<tr>
<td><strong>7. Forming</strong></td>
<td>The product is enclosed during forming in an area where there are a number of members of staff</td>
</tr>
<tr>
<td><strong>8. Transfer to fryer</strong></td>
<td>Once formed the sausages are transferred to the fryer for flash frying via an open belt</td>
</tr>
<tr>
<td><strong>9. Flash frying</strong></td>
<td>Frying process does not cook the product, just colours the outside. The product is not sold ready to eat, the sausages require thorough cooking as per pack instructions by the consumer before consumption</td>
</tr>
<tr>
<td><strong>10. Transfer to freezer</strong></td>
<td>After frying the sausages are transferred via an open belt to the blast freezer. On line 1 this involves one person to check the orientation and spacing of the sausages before entering the freezer, on line 2 this requires two people. These people rotate at regular intervals due to the nature of the job</td>
</tr>
<tr>
<td><strong>11. Blast freezing</strong></td>
<td>Freezing is the primary preservation method relied upon</td>
</tr>
<tr>
<td><strong>12. Transfer to packing</strong></td>
<td>Transfer is via open conveyor</td>
</tr>
<tr>
<td>Process Flow Step</td>
<td>Detail</td>
</tr>
<tr>
<td>---------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>13. Packaging into cartons</td>
<td>Once frozen the sausages are packed into primary packaging (cardboard cartons). Sausages are placed into packs manually on line 2 and automatically on line 1</td>
</tr>
<tr>
<td>14. Sealing</td>
<td>Cartons are sealed with heated glue. The packaging does not have any specific tamper evident measures</td>
</tr>
<tr>
<td>15. Date coding</td>
<td>Glue, inks and solvents are stored in a locked cabinet near the packing line, the key is kept on a hook in the production office</td>
</tr>
<tr>
<td>16. Weighing</td>
<td>The cartons are date coded and pass over a check weigher</td>
</tr>
<tr>
<td>17. Pack into boxes</td>
<td>The boxes are taped automatically</td>
</tr>
<tr>
<td>18. Palletise</td>
<td>Palletised by hand</td>
</tr>
<tr>
<td>19. Shrink wrapping</td>
<td>Completed pallets are shrink wrapped by hand and transferred to frozen storage</td>
</tr>
<tr>
<td>20. Metal detection</td>
<td>Each pack is metal detected before being placed in an outer carton by hand. This involves 4 people at the end of each line</td>
</tr>
<tr>
<td>21. Frozen storage</td>
<td>External access to freezer is through internally opened only fire exits</td>
</tr>
<tr>
<td>22. Vehicle loading</td>
<td>Once required the pallets are loaded onto vehicles. The company uses its own vehicles most of the time, however a third party haulier is also used during busy times or when the company vehicles are not available</td>
</tr>
<tr>
<td>23. Vehicle sealing</td>
<td>The vehicle is sealed, by the company personnel, even if using a third party, and the vehicle leaves site</td>
</tr>
<tr>
<td>24. Transport to depot</td>
<td>Most customer depots are within approximately 4 hours driving time, however some loads travel further, requiring a stop when the vehicle may be left unattended</td>
</tr>
<tr>
<td>25. Delivery at depot</td>
<td>Seal ID is checked for integrity on arrival</td>
</tr>
</tbody>
</table>
## Impact assessment

<table>
<thead>
<tr>
<th>Process Step</th>
<th>Threat</th>
<th>Consumer</th>
<th>Score</th>
<th>Business</th>
<th>Score</th>
<th>Impact Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>Packaging storage</td>
<td>Harm to the consumer caused by substandard product packed into genuine packaging due to theft of packaging from warehouse by criminals</td>
<td>Substandard product may be harmful as it is unlikely to be produced to legally compliant standards however fraudsters are generally not intending to harm consumers, therefore the harm to the consumer is likely to be minor</td>
<td>7</td>
<td>Negative publicity following an incident of fraudulent product could cause major financial loss to a medium sized business</td>
<td>3</td>
<td>10</td>
</tr>
<tr>
<td>De-bagging ingredients</td>
<td>Harm to the consumer caused by sharp physical contaminant such as glass due to malicious contamination from disgruntled lone worker</td>
<td>Hard or sharp items may lead to hospitalisation in vulnerable groups if chewed or swallowed</td>
<td>8</td>
<td>Civil action following an incident of malicious contamination could cause major financial loss to a medium sized business</td>
<td>3</td>
<td>11</td>
</tr>
<tr>
<td>Open mixing</td>
<td>Upset to the consumer caused by contamination with meat protein at the point of mixing due to malicious contamination from disgruntled lone worker</td>
<td>The presence of meat protein in a vegetarian product is likely to cause repulsion to a vegetarian consumer</td>
<td>6</td>
<td>The negative publicity which may arise from a meat protein contamination incident may cause major financial loss to a medium sized business</td>
<td>3</td>
<td>9</td>
</tr>
<tr>
<td>Closed mixing</td>
<td>Upset to the consumer caused by contamination with meat protein at the point of mixing due to malicious contamination from disgruntled lone worker</td>
<td>The presence of meat protein in a vegetarian product is likely to cause repulsion to a vegetarian consumer</td>
<td>6</td>
<td>The negative publicity which may arise from a meat protein contamination incident may cause major financial loss to a medium sized business</td>
<td>3</td>
<td>9</td>
</tr>
<tr>
<td>Process Step</td>
<td>Threat</td>
<td>Consumer</td>
<td>Business</td>
<td>Score</td>
<td>Score</td>
<td>Impact Score</td>
</tr>
<tr>
<td>----------------------</td>
<td>------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------</td>
<td>-------</td>
<td>-------</td>
<td>-------------</td>
</tr>
<tr>
<td>Hand packing on line 2</td>
<td>Food poisoning of the consumer caused by malicious vegetative pathogenic contamination of product due to spiking by a disgruntled accompanied worker</td>
<td>The contamination will only be on the surface and even insufficient cooking by the consumer will reduce vegetative pathogens to a safe level</td>
<td>The consumer would be unaware of the issue and therefore there would be no impact on the business</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Water storage</td>
<td>Harm to the consumer caused by addition of toxic chemicals to external water supply tanks due to malicious contamination from terrorist or extremist</td>
<td>Toxic chemicals may be fatal for vulnerable groups or general population depending on nature or concentration</td>
<td>Consumer deaths or hospitalisation could lead to serious negative publicity, legal action and possible closure of business</td>
<td>9</td>
<td>4</td>
<td>13</td>
</tr>
</tbody>
</table>
### Vulnerability assessment

<table>
<thead>
<tr>
<th>Step</th>
<th>Threat</th>
<th>Motivation</th>
<th>Score</th>
<th>Opportunity</th>
<th>Score</th>
<th>Vuln. Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>Packaging storage</td>
<td>Harm to the consumer caused by substandard product packed into genuine packaging due to theft of packaging from warehouse by criminals</td>
<td>The motivation to produce and sell substandard product under an established brand is classed as food fraud</td>
<td>3</td>
<td>The opportunity to steal packaging from the warehouse is limited as the warehouse has controlled access. Pedestrian and product access points are covered by CCTV</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>De-bagging ingredients</td>
<td>Harm to the consumer caused by sharp physical contaminant such as glass due to malicious contamination from disgruntled lone worker</td>
<td>A disgruntled employee may hold a personal grievance against the company which may motivate them to carry out a threat</td>
<td>1</td>
<td>De-bagging is often carried out by lone workers. There is no CCTV in this area</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>Open mixing (line 2)</td>
<td>Upset to the consumer caused by contamination with meat protein at the point of mixing due to malicious contamination from disgruntled accompanied worker</td>
<td>A disgruntled employee may hold a personal grievance against the company which may motivate them to carry out a threat</td>
<td>1</td>
<td>The mixing area for both lines in a busy area in the middle of the production floor, it is very unusual for lone workers to be here. Line 2 mixer is open</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>Closed mixing (line 1)</td>
<td>Upset to the consumer caused by contamination with meat protein at the point of mixing due to malicious contamination from disgruntled accompanied worker</td>
<td>A disgruntled employee may hold a personal grievance against the company which may motivate them to carry out a threat</td>
<td>1</td>
<td>The mixing area for both lines in a busy area in the middle of the production floor, it is very unusual for lone workers to be here. Line 1 mixer is enclosed</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>Step</td>
<td>Threat</td>
<td>Motivation</td>
<td>Score</td>
<td>Opportunity</td>
<td>Score</td>
<td>Vuln. Score</td>
</tr>
<tr>
<td>-----------------------</td>
<td>------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------</td>
<td>-------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-------</td>
<td>-------------</td>
</tr>
<tr>
<td><strong>Hand packing on line 2</strong></td>
<td>Food poisoning of the consumer caused by malicious vegetative pathogenic contamination of product due to spiking by a disgruntled accompanied worker</td>
<td>A disgruntled employee may hold a personal grievance against the company which may motivate them to carry out a threat</td>
<td>1</td>
<td>The hand packing line on line 2 usually requires 4 staff who work in close proximity to each other, therefore the opportunity to contaminate the product is lower, unless all 4 staff were involved</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td><strong>Water storage</strong></td>
<td>Harm to the consumer caused by addition of toxic chemicals to external water supply tanks due to malicious contamination from terrorist or extremist</td>
<td>A terrorist or extremist may be motivated by causing mass illness or fatalities. There are no currently known reasons why the business would be a target for a terrorist or extremist attack</td>
<td>4</td>
<td>Water tanks are external to the building but within the site boundary. Access points of external water tanks are locked with robust padlocks. CCTV over external access points, but doesn't cover water tanks</td>
<td>2</td>
<td>6</td>
</tr>
</tbody>
</table>
The overall risk score

<table>
<thead>
<tr>
<th>Step</th>
<th>Threat</th>
<th>Consumer</th>
<th>Business</th>
<th>Impact Score</th>
<th>Motivation</th>
<th>Opp. Score</th>
<th>Vuln. Score</th>
<th>Risk Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>Packaging storage</td>
<td>Harm to the consumer caused by substandard product packed into genuine packaging due to theft of packaging from warehouse by criminals</td>
<td>7</td>
<td>3</td>
<td>10</td>
<td>3</td>
<td>1</td>
<td>4</td>
<td>40</td>
</tr>
<tr>
<td>De-bagging ingredients</td>
<td>Harm to the consumer caused by sharp physical contaminant such as glass due to malicious contamination from disgruntled lone worker</td>
<td>8</td>
<td>3</td>
<td>11</td>
<td>1</td>
<td>4</td>
<td>5</td>
<td>55</td>
</tr>
<tr>
<td>Open mixing (line 2)</td>
<td>Upset to the consumer caused by contamination with meat protein at the point of mixing due to malicious contamination from disgruntled accompanied worker</td>
<td>6</td>
<td>3</td>
<td>9</td>
<td>1</td>
<td>3</td>
<td>4</td>
<td>36</td>
</tr>
<tr>
<td>Closed mixing (line 1)</td>
<td>Upset to the consumer caused by contamination with meat protein at the point of mixing due to malicious contamination from disgruntled accompanied worker</td>
<td>6</td>
<td>3</td>
<td>9</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>18</td>
</tr>
<tr>
<td>Step</td>
<td>Threat</td>
<td>Consumer</td>
<td>Business</td>
<td>Impact Score</td>
<td>Motivation</td>
<td>Opp. Score</td>
<td>Vuln. Score</td>
<td>Risk Score</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------------------------------------------------------------------</td>
<td>----------</td>
<td>----------</td>
<td>--------------</td>
<td>------------</td>
<td>------------</td>
<td>-------------</td>
<td>------------</td>
</tr>
<tr>
<td>Hand packing on line 2</td>
<td>Food poisoning of the consumer caused by malicious vegetative pathogenic contamination of product due to spiking by a disgruntled accompanied worker</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>3</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>Water storage</td>
<td>Harm to the consumer caused by addition of toxic chemicals to external water supply tanks due to malicious contamination from terrorist or extremist</td>
<td>9</td>
<td>4</td>
<td>13</td>
<td>4</td>
<td>2</td>
<td>6</td>
<td>78</td>
</tr>
</tbody>
</table>
Protection measures and PRPs

<table>
<thead>
<tr>
<th>Step</th>
<th>Threat</th>
<th>Protection Measures</th>
<th>PRP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Packaging storage</td>
<td>Harm to the consumer caused by substandard product packed into genuine packaging due to theft of packaging from warehouse by criminals</td>
<td>Controlled access points CCTV over pedestrian and bulk access points</td>
<td>Site security</td>
</tr>
<tr>
<td>De-bagging ingredients</td>
<td>Harm to the consumer caused by sharp physical contaminant such as glass due to malicious contamination from disgruntled lone worker</td>
<td>No protection measure as lone worker and no CCTV</td>
<td></td>
</tr>
<tr>
<td>Open mixing (line 2)</td>
<td>Upset to the consumer caused by contamination with meat protein at the point of mixing due to malicious contamination from disgruntled accompanied worker</td>
<td>Team working</td>
<td>Supervision &amp; management</td>
</tr>
<tr>
<td>Closed mixing (line 1)</td>
<td>Upset to the consumer caused by contamination with meat protein at the point of mixing due to malicious contamination from disgruntled accompanied worker</td>
<td>Team working Enclosed equipment</td>
<td>Supervision Equipment design</td>
</tr>
<tr>
<td>Hand packing on line 2</td>
<td>Food poisoning of the consumer caused by malicious vegetative pathogenic contamination of product due to spiking by a disgruntled accompanied worker</td>
<td>Team working</td>
<td>Supervision &amp; management</td>
</tr>
<tr>
<td>Water storage</td>
<td>Harm to the consumer caused by addition of toxic chemicals to external water supply tanks due to malicious contamination from terrorist or extremist</td>
<td>Locked tank access points</td>
<td>Site security</td>
</tr>
</tbody>
</table>
### Decision tree

<table>
<thead>
<tr>
<th>Step</th>
<th>Q1</th>
<th>Q2</th>
<th>Q2a</th>
<th>Q3</th>
<th>Q4</th>
<th>Q5</th>
<th>Threat Management Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>De-bagging ingredients</td>
<td>No</td>
<td>No</td>
<td>No, stop</td>
<td></td>
<td></td>
<td></td>
<td>Risk register</td>
</tr>
<tr>
<td>Water storage</td>
<td>No</td>
<td>Yes</td>
<td>N/A</td>
<td>Yes, stop</td>
<td></td>
<td></td>
<td>PRP</td>
</tr>
</tbody>
</table>

### Risk register

<table>
<thead>
<tr>
<th>Process step</th>
<th>Threat</th>
<th>Rationale</th>
<th>Mitigation - Short Term</th>
<th>Mitigation - Medium Term</th>
<th>Mitigation - Longer Term</th>
</tr>
</thead>
<tbody>
<tr>
<td>De-bagging ingredients</td>
<td>Harm to the consumer caused by sharp physical contaminant such as glass due to malicious contamination from disgruntled lone worker</td>
<td>Currently there is no internal CCTV on site. Installing CCTV within lone working areas would involve capital expenditure. There are no known instances of malicious contamination by employees to date</td>
<td>Action: Monitor changes in staff morale and factors potentially affecting staff morale  &lt;br&gt; Responsibility: Senior management team and human resources team  &lt;br&gt; Timescale: Immediately  &lt;br&gt; Review: Monthly</td>
<td>Action: Increase the level of supervision  &lt;br&gt; Responsibility: Production supervisors and human resources team  &lt;br&gt; Timescale: Within 2 months  &lt;br&gt; Review: Monthly</td>
<td>Action: Install full CCTV system covering lone worker areas  &lt;br&gt; Responsibility: Senior Management Team  &lt;br&gt; Timescale: Within 12 months  &lt;br&gt; Review: Quarterly</td>
</tr>
</tbody>
</table>

### VTP summary

None for this extract example.
Process Flow - People

1. Job advertising
2. Application form
3. Short listing
4. Interview
5. Recruit
6. Induction
7. Probationary review
8. Make permanent
9. Annual performance reviews
10. Continued employment
11. Disciplinary action
12. Final warning
13. Dismissal
5a. Agency
7a. Do not make permanent

Key
People Process Step
Describe the process

<table>
<thead>
<tr>
<th>Process flow step</th>
<th>Detail</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Job advertising</td>
<td>Staff are generally recruited via the local job centre. Agency staff are used only when absolutely necessary due to the increased costs</td>
</tr>
<tr>
<td>2. Application form</td>
<td>All potential staff are required to complete an application form</td>
</tr>
<tr>
<td>3. Short listing</td>
<td>Application forms are assessed against set criteria to filter them down to a short list</td>
</tr>
<tr>
<td>4. Interview</td>
<td>Short-listed staff are interviewed by a member of the HR team and a representative from the department they will be working in</td>
</tr>
<tr>
<td>5. Recruit</td>
<td>Staff are informed of the results of the interview by telephone or letter</td>
</tr>
<tr>
<td>6. Induction</td>
<td>All new starters, regardless of position, are required to complete an induction day before starting work. This includes a site tour and information on company procedures, health and safety, and food safety</td>
</tr>
<tr>
<td>7. Probationary review</td>
<td>New starters are subject to a 3 month probationary period, within which it is the responsibility of their supervisor, with support from HR, to perform regular reviews. A performance review is carried out before awarding a permanent contract or extending a temporary contract</td>
</tr>
<tr>
<td>8. Make permanent</td>
<td>Confirmation letters for permanent employment is sent to all successful employees</td>
</tr>
<tr>
<td>9. Annual performance reviews</td>
<td>All staff undergo annual performance reviews, the results of which are documented</td>
</tr>
<tr>
<td>10. Continued employment</td>
<td>Verbal communication through line management</td>
</tr>
<tr>
<td>11. Disciplinary action</td>
<td>The company has a formal grievance and disciplinary procedure in place</td>
</tr>
<tr>
<td>12. Final warning</td>
<td>Formal letters are sent to employees</td>
</tr>
<tr>
<td>13. Dismissal</td>
<td>In the event of dismissal, the individual is accompanied whilst they collect their possessions and escorted off site by a manager</td>
</tr>
</tbody>
</table>
**Risk assessment - People Flow**

### Impact assessment

<table>
<thead>
<tr>
<th>Step</th>
<th>Threat</th>
<th>Consumer Score</th>
<th>Business Score</th>
<th>Impact Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dismissal of employee</td>
<td>Harm to the consumer caused by sharp physical contaminant such as metal blade or glass due to malicious contamination from upset dismissed employee not being escorted off site</td>
<td>8</td>
<td>Civil action following an incident of malicious contamination could cause major financial loss to a medium sized business</td>
<td>3</td>
</tr>
</tbody>
</table>

### Vulnerability assessment

<table>
<thead>
<tr>
<th>Step</th>
<th>Threat</th>
<th>Motivation Score</th>
<th>Opportunity Score</th>
<th>Vuln. Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dismissal of employee</td>
<td>Harm to the consumer caused by sharp physical contaminant such as metal blade or glass due to malicious contamination from upset dismissed employee not being escorted off site</td>
<td>1</td>
<td>Although procedures are in place to escort dismissed employees from the point of dismissal until leaving site these have not always been complied with. Staff may need to walk past open product to exit the building depending on where their dismissal meeting was held</td>
<td>4</td>
</tr>
</tbody>
</table>

### The overall risk score

<table>
<thead>
<tr>
<th>Step</th>
<th>Threat</th>
<th>Consumer Score</th>
<th>Business Score</th>
<th>Impact Score</th>
<th>Motivation Score</th>
<th>Opp. Score</th>
<th>Vuln. Score</th>
<th>Risk Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dismissal of employee</td>
<td>Harm to the consumer caused by sharp physical contaminant such as metal blade or glass due to malicious contamination from upset dismissed employee not being escorted off site</td>
<td>8</td>
<td>3</td>
<td>11</td>
<td>1</td>
<td>4</td>
<td>5</td>
<td>55</td>
</tr>
</tbody>
</table>
Protection measures and PRPs

<table>
<thead>
<tr>
<th>Step</th>
<th>Threat</th>
<th>Protection Measures</th>
<th>PRP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dismissal of employee</td>
<td>Harm to the consumer caused by sharp physical contaminant such as metal blade or glass due to malicious contamination from upset dismissed employee not being escorted off site</td>
<td>Escorted off site by management</td>
<td>Human resources procedures</td>
</tr>
</tbody>
</table>

Decision tree

<table>
<thead>
<tr>
<th>Step</th>
<th>Q1</th>
<th>Q2</th>
<th>Q2a</th>
<th>Q3</th>
<th>Q4</th>
<th>Q5</th>
<th>Threat Management Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dismissal of employee</td>
<td>No</td>
<td>Yes</td>
<td>N/A</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>VTP</td>
</tr>
</tbody>
</table>

Risk register

None for this extract example.
## VTP summary

<table>
<thead>
<tr>
<th>Process step</th>
<th>Threat</th>
<th>Protection measure</th>
<th>Critical limit/ Criteria</th>
<th>Procedure &amp; Frequency</th>
<th>Corrective Action</th>
<th>Internal Auditing (Verification)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dismissal of employee</td>
<td>Harm to the consumer caused by sharp physical contaminant such as metal blade or glass due to malicious contamination from upset dismissed employee not being escorted off site</td>
<td>Escorted off site by management</td>
<td>Continuous accompaniment from point of dismissal to leaving site</td>
<td>At least one member of the management team to stay with the dismissed employee at all times until they leave the premises</td>
<td>Investigate potential risk to the product</td>
<td>Ensure that the procedure is clear</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Investigate the reason for failure of procedure and implement action as necessary</td>
<td></td>
<td>Assess records for compliance</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Assess CCTV for last dismissed employee to establish if they were escorted up to and past access point</td>
</tr>
</tbody>
</table>
Appendix 2
Case study (raw material driven)

Raw Material Vulnerability Assessment

This case study has been created to give an example of how the methodology for raw material vulnerability assessment described in the guide can be applied in practice.

It does not include all the vulnerability assessment for all ingredients - just egg has been used as an extract.

This example is fictitious and for illustrative purposes only.

Site background information

The case study is based on a vegetarian sausage product produced by a medium sized, independent manufacturer called Veggie Sausages Ltd, supplying branded product to discount retailers. The case study focuses on raw material group driven assessments and considers the assessment of free range egg through the scoring system.
Veggie Sausages Ltd

Raw Material Vulnerability Assessment

Scope

The aim of this study is to identify and manage the potential threats and vulnerabilities to the raw materials, which could have an impact on the consumer and thereby a consequential impact on the business.

This assessment covers the assessment of the following groups of raw materials:

<table>
<thead>
<tr>
<th>Raw material group</th>
<th>Raw materials</th>
<th>Supply chain process</th>
</tr>
</thead>
<tbody>
<tr>
<td>Meat substitute</td>
<td>Branded meat substitute</td>
<td>Manufacturing site &gt; delivery</td>
</tr>
<tr>
<td>Free-range egg</td>
<td>Free-range liquid egg</td>
<td>Farm &gt; processing plant &gt; agent &gt; delivery</td>
</tr>
<tr>
<td>Prepared produce</td>
<td>Fresh onion, herbs (sage)</td>
<td>Farm &gt; processing plant &gt; delivery</td>
</tr>
<tr>
<td>Oils</td>
<td>Olive oil</td>
<td>Producer &gt; processing plant &gt; broker importer &gt; agent &gt; delivery</td>
</tr>
<tr>
<td>Spices</td>
<td>Black pepper</td>
<td>Producer &gt; processing plant &gt; broker importer &gt; agent &gt; delivery</td>
</tr>
<tr>
<td>Salt</td>
<td>Salt (granular)</td>
<td>Harvesting &gt; processing plant &gt; delivery</td>
</tr>
<tr>
<td>Potato Starch</td>
<td>Potato starch</td>
<td>Farm &gt; processing plant &gt; delivery</td>
</tr>
</tbody>
</table>

Types of threat

The types of raw material threats covered by this study are fraudulent and intentional, prior to delivery.
### Types of manifestation of threats

This study considers the following categories, although this is not an exhaustive list:

<table>
<thead>
<tr>
<th>Biological including:</th>
<th>Chemical including:</th>
</tr>
</thead>
<tbody>
<tr>
<td>- pathogenic organisms</td>
<td>- excess additives</td>
</tr>
<tr>
<td>- biological disease causing agents</td>
<td>- use of non-permitted additives</td>
</tr>
<tr>
<td>- parasites</td>
<td>- chemicals used on site such as cleaning or engineering chemicals (inks and solvents)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Physical including:</th>
<th>Allergenic / immune response agents including:</th>
</tr>
</thead>
<tbody>
<tr>
<td>- needles</td>
<td>- milk</td>
</tr>
<tr>
<td>- razor blades</td>
<td>- gluten (Wheat, Rye, Barley, Oats)</td>
</tr>
<tr>
<td>- glass</td>
<td>- celery</td>
</tr>
<tr>
<td>- stones (ceramics)</td>
<td>- egg</td>
</tr>
<tr>
<td>- engineering metals</td>
<td>- fish</td>
</tr>
<tr>
<td>- brittle plastics</td>
<td>- crustacean</td>
</tr>
<tr>
<td>- personal items (phones, jewellery, etc.)</td>
<td>- molluscs</td>
</tr>
<tr>
<td>- personnel related (fingernails, teeth, etc.)</td>
<td>- sesame</td>
</tr>
<tr>
<td></td>
<td>- soya</td>
</tr>
<tr>
<td></td>
<td>- lupin</td>
</tr>
<tr>
<td></td>
<td>- mustard</td>
</tr>
<tr>
<td></td>
<td>- nuts</td>
</tr>
<tr>
<td></td>
<td>- peanuts</td>
</tr>
<tr>
<td></td>
<td>- sulphites</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Radiological including:</th>
<th>Not of the:</th>
</tr>
</thead>
<tbody>
<tr>
<td>- radioactive material</td>
<td>- nature</td>
</tr>
<tr>
<td></td>
<td>- substance</td>
</tr>
<tr>
<td></td>
<td>- quality</td>
</tr>
<tr>
<td>Name</td>
<td>Job Role</td>
</tr>
<tr>
<td>-------------</td>
<td>---------------------</td>
</tr>
<tr>
<td><strong>Julia Brown</strong></td>
<td>Technical Manager</td>
</tr>
<tr>
<td><strong>David White</strong></td>
<td>Production Manager</td>
</tr>
<tr>
<td><strong>Steve Smith</strong></td>
<td>Goods in Supervisor</td>
</tr>
<tr>
<td><strong>Helen Davies</strong></td>
<td>Head Buyer</td>
</tr>
<tr>
<td><strong>Ruth Allen</strong></td>
<td>Purchasing</td>
</tr>
<tr>
<td><strong>Fred Greaves</strong></td>
<td>Logistics Manager</td>
</tr>
</tbody>
</table>
## Risk assessment

### Impact assessment

<table>
<thead>
<tr>
<th>Raw Material Group</th>
<th>Threat</th>
<th>Consumer</th>
<th>Score</th>
<th>Business Score</th>
<th>Impact Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>Free-range egg</td>
<td>Upset to the consumer caused by non-free-range egg being delivered and used due to fraudulent activity in the supply chain caused by insufficient monitoring of the processor</td>
<td>Purchasing a product which contains non-free-range egg when the product is labelled as containing free range egg would upset the consumer</td>
<td>5</td>
<td>3</td>
<td>8</td>
</tr>
</tbody>
</table>

### Vulnerability assessment

<table>
<thead>
<tr>
<th>Raw Material Group</th>
<th>Threat</th>
<th>Motivation</th>
<th>Score</th>
<th>Opportunity</th>
<th>Score</th>
<th>Vuln. Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>Free range egg</td>
<td>Upset to the consumer caused by non-free-range egg being delivered and used due to fraudulent activity in the supply chain caused by insufficient monitoring of the processor</td>
<td>The motivation to produce and sell non-free-range egg for financial gain is classed as food fraud</td>
<td>3</td>
<td>The opportunity to produce fraudulent product could go undetected if not sufficiently monitored</td>
<td>4</td>
<td>7</td>
</tr>
</tbody>
</table>

### The overall risk score

<table>
<thead>
<tr>
<th>Raw Material Group</th>
<th>Threat</th>
<th>Consumer</th>
<th>Business</th>
<th>Impact Score</th>
<th>Motivation</th>
<th>Opp. Score</th>
<th>Vuln. Score</th>
<th>Risk Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>Free range egg</td>
<td>Upset to the consumer caused by non-free-range egg being delivered and used due to fraudulent activity in the supply chain caused by insufficient monitoring of the processor</td>
<td>5</td>
<td>3</td>
<td>8</td>
<td>3</td>
<td>4</td>
<td>7</td>
<td>56</td>
</tr>
</tbody>
</table>
### Protection measures and PRPs

<table>
<thead>
<tr>
<th>Raw Material Group</th>
<th>Threat</th>
<th>Protection Measures</th>
</tr>
</thead>
<tbody>
<tr>
<td>Free-range egg</td>
<td>Upset to the consumer caused by non-free-range egg being delivered and used due to fraudulent activity in the supply chain caused by insufficient monitoring of the processor</td>
<td>Specific origin mass balance audit</td>
</tr>
</tbody>
</table>

### Decision tree

<table>
<thead>
<tr>
<th>Raw Material Group</th>
<th>Q1</th>
<th>Q2</th>
<th>Q2a</th>
<th>Q3</th>
<th>Q4</th>
<th>Threat Management Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Free range egg</td>
<td>No</td>
<td>Yes</td>
<td>N/A</td>
<td>Yes</td>
<td>No</td>
<td>VTP</td>
</tr>
</tbody>
</table>

### Risk register

None for the example extract.

### VTP summary

<table>
<thead>
<tr>
<th>Raw Material Group</th>
<th>Threat</th>
<th>Protection measure</th>
<th>Critical limit/ Criteria</th>
<th>Procedure &amp; Frequency</th>
<th>Corrective Action</th>
<th>Internal Auditing (Verification)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Free range egg</td>
<td>Upset to the consumer caused by non-free-range egg being delivered and used due to fraudulent activity in the supply chain caused by insufficient monitoring of the processor</td>
<td>Specific origin mass balance audit</td>
<td>Pass rate of 99% on mass balance</td>
<td>Attended audit to be carried out unannounced annually. Quarterly off site paperwork audit to be carried out</td>
<td>Where non conformance is suspected to be fraudulent stop supply and move to approved contingency supplier. Where non conformance is not suspected to be fraudulent non compliance must be corrected with evidence within 4 weeks</td>
<td>Review mass balance procedure. Assess training and question relevant personnel against understanding of procedure. Assess records for compliance</td>
</tr>
</tbody>
</table>
Appendix 3
Information sources on emerging issues

The following is a list, which is not exhaustive, of resources for information on emerging issues.

The Institute of Food Safety Integrity & Protection
www.ifsip.org

U.S. Food & Drug Administration – Sign up for Food Defence alerts
www.fda.gov/Food/FoodDefense

U.S. Food & Drug Administration – Recall, Market Withdrawals & Safety Alerts Database
www.fda.gov/Safety/Recalls

FSA guidance
www.food.gov.uk/enforcement/foodfraud

U.S. Pharmacopeial Convention
www.foodfraud.org

MI5 Security Service
www.mi5.gov.uk

Michigan State University – Food Fraud Initiative
www.foodfraud.msu.edu
References

**British Retail Consortium** (2015) *Global Standard Food Safety Issue 7*


**Elliot, C.** (2014) *Elliot Review into the Integrity and Assurance of Food Supply Networks – Final Report*

**GFSI** (2014) *Position on Mitigating the Public Health Risk of Food Fraud*

**Leathers, R** (2014) *TACCP Threat Assessment and Critical Control Point, Guideline 72*, UK, Campden BRI

**U.K. Food and Drink Federation** (ca. 2014) *Guide on Food authenticity: Five steps to help protect your business from food fraud*

**U.S. Food and Drug Administration** (2009) *CARVER + Shock Primer*
About the Authors

Adele Adams

After gaining a degree in Food Science from Nottingham University in 1993, Adele started her career in technical management within the meat industry. She then moved into consultancy and training and began to specialise in HACCP and food safety management, achieving the role of Managing Director of a consultancy firm in 2000. As a Senior Lecturer at the University of Salford Adele helped to establish their MSc in Food Safety Management. In 2003, Adele set up her own company to provide practical training and advice on how to get the best out of the HACCP principles. Adele regularly delivers a wide range of HACCP and food safety programmes, specialising in higher-level courses, to help teams become competent in HACCP techniques. She has also helped many large companies to remodel their HACCP systems in line with best practice, as well as being involved with several projects for the Food Standards Agency. With over 20 years of HACCP experience, Adele is well known for her engaging training and practical approach.

Kassy Marsh

Kassy started her career in the food manufacturing industry in 1998 and has an exceptional ability to implement simple and practical solutions, which can be effectively implemented into the factory environment. With a background of NPD, process and quality control, compliance, auditing and technical management, she has a wealth of experience in meeting the required standards effectively. During her time within compliance she became well known for her pioneering risk assessments which Marks & Spencer used as examples of best practice. Since starting her own consultancy business in 2012 she now specialises in the practical application of HACCP and validation techniques.
The issue of food defence is becoming increasingly important within the food industry. Well publicised incidents such as the horsemeat contamination in 2013 have focused the attention of manufacturers, retailers, enforcers and consumers on the defence of our food supply. As a consequence, the need for a systematic approach to the task of identifying and managing threats and vulnerabilities is accelerating and becoming incorporated into industry standards.

This publication provides new methodology for threat and vulnerability assessment which has been pioneered by two experienced industry professionals, Adele Adams and Kassy Marsh. This methodology details a number of new concepts for assessing threats and vulnerabilities, which will enable manufacturers to carry out and implement robust and structured assessments and management systems.