IFS
International
Featured Standards

IFS Product and Food Defence Guideline

VERSION 2

ENGLISH

IFS would like to thank all participants who contributed to the review process for the IFS Product and Food Defence Guideline. In particular, IFS would like to thank Prof. John W. Spink (Michigan State University) for his valuable contribution, especially concerning the role of food safety management for cybersecurity. We would like to express our gratitude to Dawid Stępień, Andrzej Cieślak and Barbara Szymańska (Dynacon Sp. z o.o.) for their support on the topic of cybersecurity in the food and non-food industry. Furthermore, we would like to thank Bosch CyberCompare for their helpful advice about cybersecurity strategies for IFS certified companies.

This guideline is a supporting document related to the topic of product defence. It is not a normative document, and its implementation is not mandatory.

Food defence requirements are subject to different regulations in different countries and regions, which must be taken into account.

In case of any queries regarding the interpretation of IFS Standards and Programs, please contact standardmanagement@ifs-certification.com

TABLE OF CONTENTS

1 Introduction

1 INTRODUCTION

Product defence – including food defence – has become a relevant topic for many industries to counteract intentional tampering or malicious actions. The food industry has explicit regulatory and standard compliant requirements. Intentionally contaminated or adulterated products, e.g. as a terrorist act, can be a risk to public health and should therefore be assessed within the food/product safety management system. In addition, a disruption of the supply chain due to malicious acts can result in high costs for the affected company and its clients. The aim of this guideline is to equip companies with the right prevention methods to manage threats regarding intentional product contaminations and provide support for the implementation of the product defence requirements in the IFS Standards.

The guideline addresses suppliers of food and non-food products (non-food products as detailed in the Standards IFS HPC and IFS PACsecure) and contributes to better cooperation within the supply chain when it comes to delivering safe products.

There is currently no comprehensive or explicit regulation of product defence at EU level, but since the manufacturer is responsible for the overall safety of the product, product defence can be considered as part of this overall responsibility and general principles and requirements of food law, regulation (EC) No. 178/2002. Specific regulations are provided by the FDA (U.S. Food and Drug Administration) and implementation required by US manufacturers and those exporting into the US market.

This guideline has been adapted to the product defence requirements of the current version of IFS Food – IFS Food version 8 and IFS HPC version 3. Other IFS Standards such IFS Logistics version 3, IFS Broker version 3.2, IFS Cash & Carry/Wholesale version 2, IFS PACsecure version 3 and IFS Progress Food version 3 also contain product defence requirements, which can be applied in a similar way to food and non-food products. This guideline therefore addresses not only food manufacturers, but also the non-food suppliers.

Furthermore, a chapter on cybersecurity has been added, as all external threats related to product defence should be addressed and the number and impact of cyberattacks have increased significantly in recent years. According to Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the EU, the food industry belongs to "other critical sectors" for cybersecurity issues (Directive (EU) 2022/2555, Annex II, 4).

2 Definitions and general aspects

2 DEFINITIONS AND GENERAL ASPECTS

Product and food defence does not have an international harmonised definition but you can find some descriptions and definitions below.

Product defence in this document comprises all measures by which a product can be protected against tampering or other intentional, malicious, criminal, or terrorist actions.

The aim should be to "prevent food products from intentional adulteration from acts intended to cause wide-scale harm to public health, including acts of terrorism targeting the food supply". (FSMA Final Rule for Mitigation Strategies to Protect Food Against Intentional Adulteration, 11/2022)

IFS Definition of product and food defence
Procedures implemented to assure the protection of food and non-food products and their supply chain from malicious and ideologically motivated threats. (IFS Food version 8, Glossary)

The purpose of a product defence procedure and plan is to identify, prevent or mitigate and monitor possible sources of **intentional** contamination of food or non-food products. The HACCP system runs in parallel and its purpose is to identify **unintentional** physical, chemical and biological hazards which are significant to food safety (see Figure 1, which is also applicable to other products). While food safety and product defence programs exist independently, there are common elements (e.g. the sealing of transportation vessels).

FIGURE 1
Food protection risk matrix

<table>
<tr><td>Product
Quality</td><td>Product
Fraud (1)</td><td>Gain:
Economic</td><td rowspan="2">Motivation</td></tr>
<tr><td>Product
Safety</td><td>Product
Defence</td><td>Harm:
Public health, economic, warfare or terror</td></tr>
<tr><td>unintentional</td><td>intentional</td><td colspan="2" rowspan="2"></td></tr>
<tr><td colspan="2">Action</td></tr>
</table>

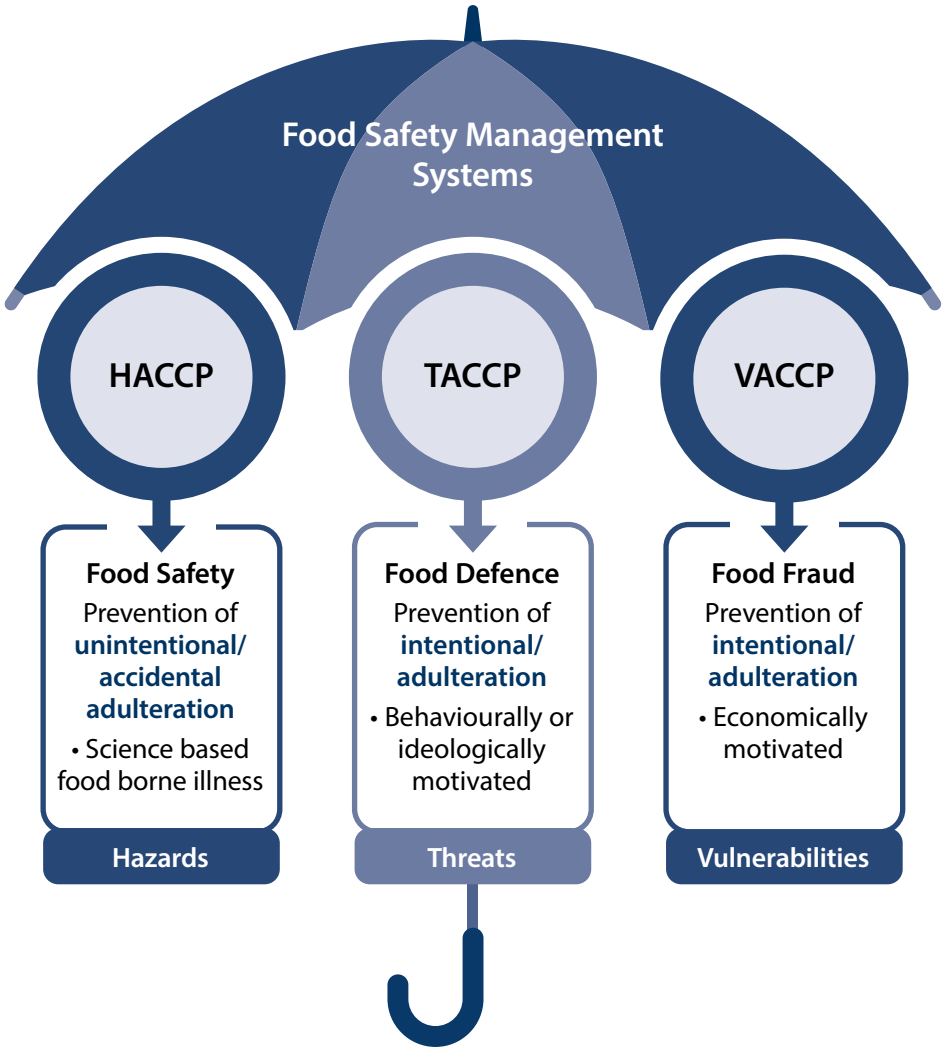
(1) Includes the subcategory of economically motivated adulteration and food counterfeiting
Source: (Spink, J. and Moyer, D. C., 2011), adapted for food and non-food products

2.1 General aspects

As specified in the IFS Product Fraud Mitigation Guideline, product fraud mitigation and product defence have the same basic objective: the prevention of intentional adulteration. Nevertheless, separate risk assessments are recommended since the likelihood, impact and consequence may be quite different (see Figure 2). For example, food fraud does not necessarily result in a health risk to the consumer. Moreover, the root cause (motivation) and resulting preventative measures are quite different.

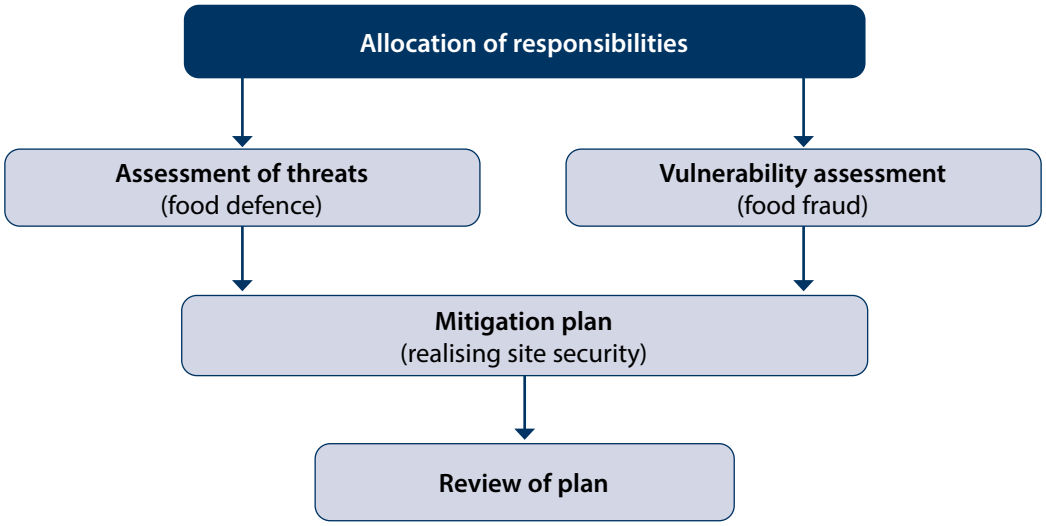
Nonetheless, similarities can be seen within the approach to address product/food defence and fraud (see Figure 3).

FIGURE 2
Food safety, food defence and food fraud – differences and common assessment method



Source: TQCS International

FIGURE 3
Similarities within the approach of food fraud and food defence



IFS recommends the TACCP method for product and food defence (while VACCP applies to food fraud mitigation). This approach includes a threat assessment and critical control points. "Weak points" are analysed and critical control points in the supply chain and processing activities are identified. TACCP is structured analogous to the classic HACCP; however, its focal point is the comprehensive site security.

Detailed explanations concerning IFS Food Fraud Requirements can be found in the IFS Product Fraud Mitigation Guideline.

TACCP: "Threat Assessment and Critical Control Points" analyses threats such as deliberate contamination of food, sabotage of the supply chain or the use of food or for terrorist or criminal purposes.

VACCP: "Vulnerability Assessment and Critical Control Points" to identify vulnerabilities for a food business due to food fraud.

3 Example of a product defence assessment

3 EXAMPLE OF A PRODUCT DEFENCE ASSESSMENT

IFS does not define what the product defence procedure and plan should entail. The company is free to develop its own tools. As already mentioned above, it might be helpful to consider the approach of a TACCP method.

Figures 4–8 show the TACCP method **as an example** for a product/food defence assessment. (Adapted from Source: TACCP/VACCP A Guidance Document for the Malting Industry, Maltsters' Association of Great Britain).

FIGURE 4
Approach of TACCP method

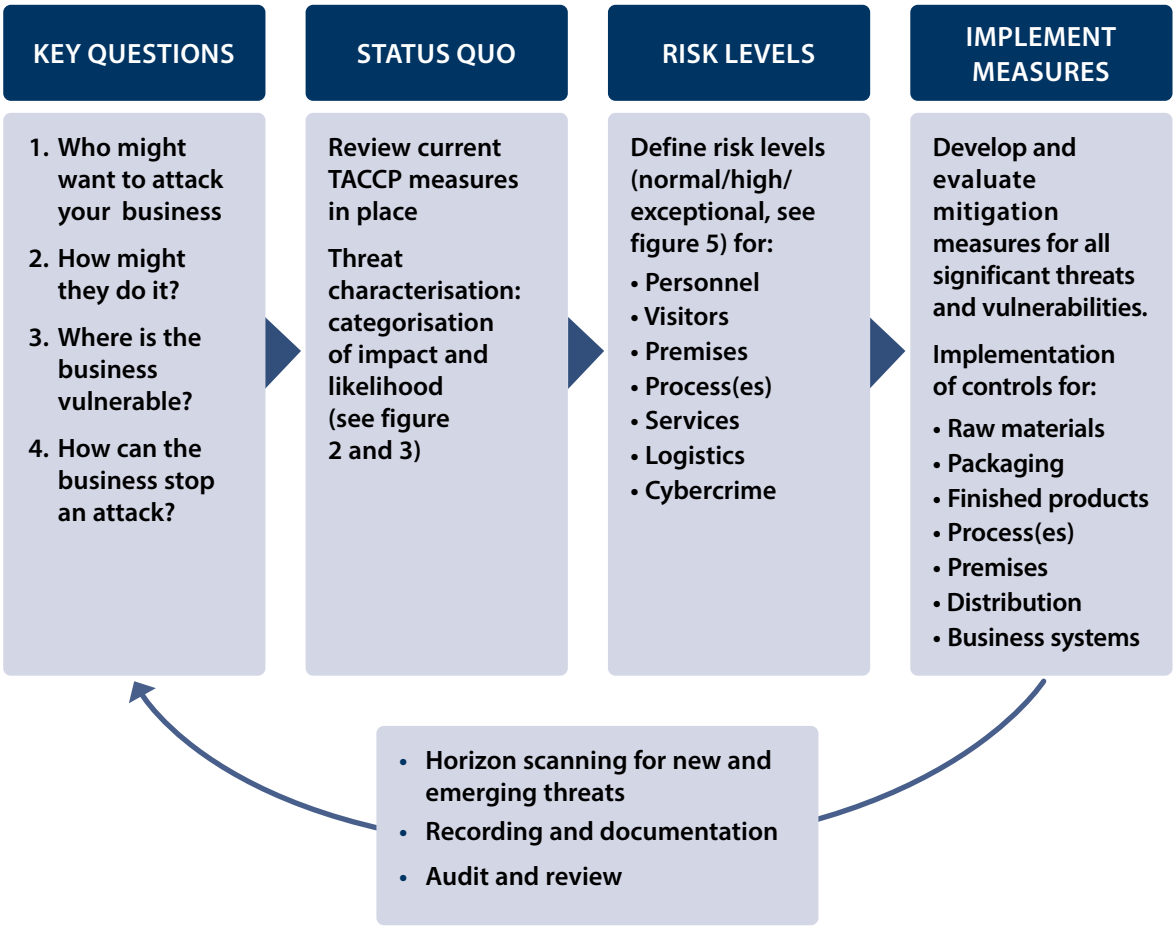


FIGURE 5
Examples for impact assessment criteria

Impact	Safety	Economic
5 – Catastrophic	Death	Site closure
4 – High	Severe symptoms/hospitalisation	Brand damage
3 – Moderate	Generally mild symptoms, but some cases of hospitalisation	Regulatory non-compliance/ recall/withdrawal
2 – Minor	Mild symptoms for a few days	Media activity
1 – Low	Mild symptoms, prompt recovery	No impact

FIGURE 6
Examples for likelihood assessment criteria

Likelihood	Site history
5 – Highly frequent	Incident has occurred during the last 6 months
4 – Frequent	The last incident was recorded between 6 and 12 months ago
3 – Moderate frequent	The last incident was recorded between 1 and 2 years ago
2 – Low frequent	The last incident was recorded between 2 and 3 years ago
1 – Infrequent	The last incident was recorded over 3 years ago

FIGURE 7

Example for risk scoring matrix for personnel

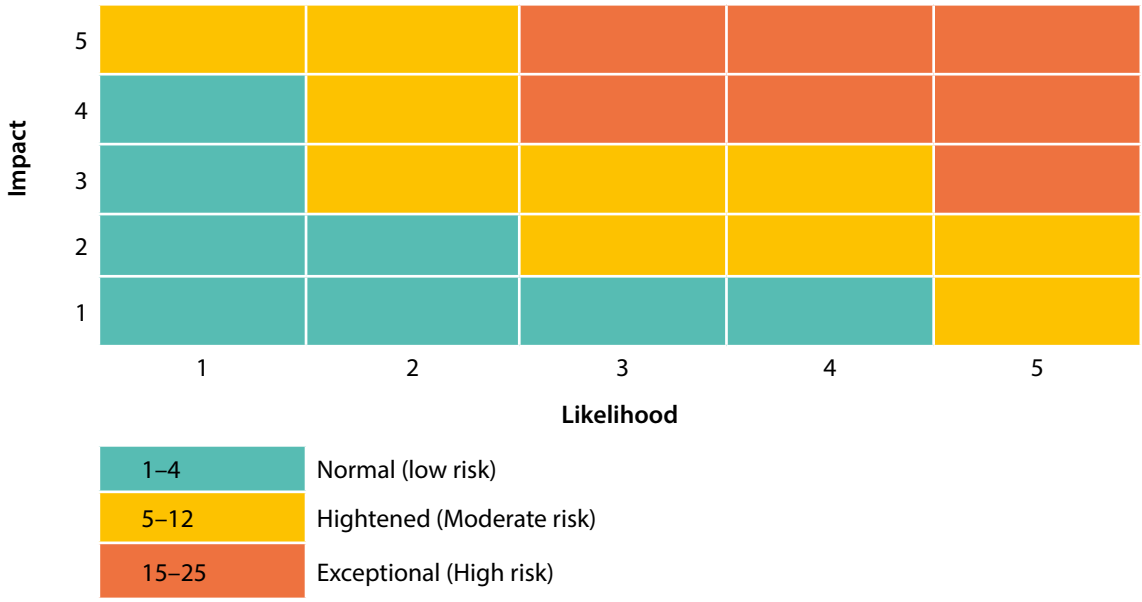


FIGURE 8

Example for development of mitigation measures for potential attackers

Group	Direct opportunity	Means	Mitigation measures
External person	**LOW** **They have no direct access to production facility or supply chain.**	No direct access to supply chain or production site but can gain access by exploiting weak security procedures.	• Controlled site access. • Effective cybersecurity measures. • Control of raw materials or finished product in the supply chain.
Contractors	**MEDIUM** **They have legitimate direct access to the site.**	With trusted status they will have direct access to raw materials and finished products at the site.	• Vetting procedures and full contractor induction prior to gaining site access. • Control/restrictions placed on where they may be allowed to work. Regular review of their suitability.
Employees and temporary staff	**HIGH** **Direct and extensive access to the site.**	With trusted status they will have direct access to raw materials and finished products at the production site.	• Pre-employment vetting • Prior site induction • Restricted areas of work • Regular performance reviews

Once the organisation identifies product/food defence threats and vulnerabilities, appropriate control measures shall be developed and implemented based on the elimination, mitigation, and maintenance of occurrence probability to an acceptable level.

Records are evidence of effective implementation and provide information about the extent to which the product defence procedure and plan is confirmed.

In some cases, a site registration is mandatory in different countries (e. g. Bioterrorism Act and the FDA registration of US exporters).

While conducting the product defence assessment, different factors should be considered. These may include:

- **Accessibility to the production site:**
  - Surroundings and construction/design of the production site
  - Contract and temporary employees may be a major risk
  - Accessibility to Information Technology (IT), Operational Technology (OT), (manipulability of production settings and configurations as well as data logger records, autoclaving, etc.) and database (to specific documents and customer data, e. g. specifications, recipes and contracts).
- **The characteristics of some products and processes may make them more vulnerable to intentional adulteration than others. Characteristics may include:**
  - Production batch size
  - Variety of products and processes
  - Shelf life
  - Accessibility to the product.
- **Situational factors could increase the risk of intentional adulteration. Such factors include:**
  - Disgruntled employees
  - National, political, business, personal, or other differences
  - Changes in organisational culture
  - Economic disruption / financial gain
  - Public fear.

Tests of the effectiveness of the existing product defence measures can be performed internally or with the help of external experts. As part of this test, the product defence team should consider the following checklist (not exhaustive).

Checklist for internal use on site

Exterior

- [ ] Are doors, windows and roof areas kept secure (e. g. security doors or access with chip cards in critical areas)?
- [ ] Is a perimeter fence or wall necessary? If a perimeter fence or wall exists, is it in good condition?
- [ ] Is the access of people and vehicles controlled?
- [ ] Are there backup sources of critical utilities, such as electrical, water, information technology (computer data), and refrigeration systems available, in case of emergency?
- [ ] How are bulk receiving and storage areas secured (a responsible person from the receiving party should be present during unloading and access to storage should be controlled)?

Interior

- [ ] Are surveillance methods utilised — such as cameras, staff supervision, or security services?
- [ ] Are hazardous materials or controlled substances managed (e. g. chemicals like cleaning agents, acids, lye, flammable liquids)?
- [ ] Is staff access limited to appropriate work location, job function and working hours?

Shipping and Receiving

- [ ] Are transportation vessels sealed/locked properly and are seals traceable?
- [ ] Do drivers provide appropriate credentials and documentation (e. g. plot number)?
- [ ] Are transportation service providers part of the supplier approval program?

Raw Materials

- [ ] Are water, ice and steam sources secure and monitored?
- [ ] Are all raw materials secured and monitored when not in use?
- [ ] Are packaging materials and product labels and seals (if applicable) controlled?

Personnel

- [ ] Are personal background checks necessary or performed, if allowed by law?
- [ ] Has the potential for retaliatory actions by terminated/previous employees been assessed?
- [ ] Are personnel supervised? Are cameras allowed?
- [ ] Are employees trained in food/product defence awareness and identifying/reporting unusual or suspicious behaviour?
- [ ] Is there a policy addressing personal items/legal or illegal weapons and drugs?

Cybersecurity

- [ ] Are cyberthreats continously identified?
- [ ] Are these threats effectively controlled?

4 Food and product defence requirements in IFS Standards

4 FOOD AND PRODUCT DEFENCE REQUIREMENTS IN IFS STANDARDS

4.1 Explanation of IFS Food Defence Requirements

This chapter contains background information and suggestions for implementing certain requirements of the IFS Food Standard, as well as examples for auditor questions. These interpretations and explanations also apply to similar product requirements in the following standards and programs: IFS Progress Food 3, IFS Logistics 2, IFS Broker 3.2, IFS PACsecure 3, and IFS Wholesale / Cash & Carry 2. Specific references to these standards and programs can be found in Chapter 4.3 and in the table in the annex.

4.1.1 Responsibilities and training

Requirement 4.21.1, IFS Food version 8

The responsibilities for food defence shall be defined. The responsible person(s) shall have the appropriate specific knowledge.

WHY

It is essential that the product/food defence team has a solid knowledge about potential threats in all areas and how they are constantly evolving.

If applicable (if food defence is legally required in the production and destination countries of products), there should be a designated contact and process for communicating with the local and national authorities.

HOW

"The responsible person(s)" could be a team or one person.

In the case of a team, this team should include cross functional employees from all levels within the organisation. They should possess the knowledge and expertise, e. g. by specific training, to identify program requirements and propose the best course of action. A team leader who is responsible for the coordination, development, implementation, maintenance and improvement of the system should be identified. Relevant product defence knowledge should be included in regular trainings/instructions and be communicated to the members of the company (see requirement 3.3.4).

Requirement 3.3.4, IFS Food Version 8

The contents of training and/or instruction shall be reviewed and updated when necessary. Special consideration shall be given to these specific issues, at a minimum:

- food safety
- product authenticity, including food fraud
- product quality
- food defence
- food related legal requirements
- product/process modifications
- feedback from the previous documented training/instruction programs.

If specific food defence legislation is applicable in the production and destination countries of products, there should be a designated contact and process for communicating with the local and national authorities. That responsible person(s) for food defence shall have the full commitment from and report to the senior management.

Questions that the auditor should ask and the company should be able to provide an answer to:

1 Who is accountable for the food defence procedure and plan?

2 What are the competence and qualifications demonstrated by the person(s) responsible for the food defence procedure and plan?

3 Was this communicated to the members of the company? How?

4 Is food defence included in trainings and instructions?

4.1.2 Food defence procedure and plan

Requirement 4.21.2, IFS Food version 8

A food defence procedure and plan shall be documented, implemented and maintained to identify potential threats and define food defence measures. This shall include, at a minimum:

- legal requirements
- identification of critical areas and/or practices and policy of access by employees
- visitors and contractors
- how to manage external inspections and regulatory visits
- any other appropriate control measures.

WHY

It is essential to gain a broad overview of all applicable threats to develop an effective food defence procedure and plan. A detailed assessment of the legislation in the production and destination country is particularly important to avoid legal complications. Applicable threats can be derived, for example, from the company environment, the number and type of visitors/contractors or IT related sources (cyberthreats). It is important to ensure that only authorised personnel have access to manufacturing, storage areas, and carry out the sample collection. There should be a way to track and monitor visitors and contractors. Also, the management of external inspections and regulatory visits are to be considered according to the relevant legislation.

All measures should aim to control the identified threats to minimise the probability of adverse effects to the product(s). In any case, the likelihood of occurrence should be considered to cover all significant threats and eliminate those which are unlikely and would just drain additional resources.

HOW/WHAT THREATS?

The following four step approach can be considered the backbone of a structured threat analysis:

1. threat identification,
2. threat characterisation,
3. exposure assessment, and
4. characterisation of occurrence probability.

All threats should be compared with historical and anticipated events, to evaluate the forementioned four iterative steps. It may also help to determine acceptable levels of occurrence and when to take measures. Please find an example of the detailed approach in chapter 3 of this document.

It is recommended to use checklists and/or software to map the threats and determine the level of risk for each threat. The following examples might help to identify potential threats:

- People who oversee processes, packaging, transportation and warehousing, and therefore **gain access to critical information**. For example, where contaminants may be introduced at the most convenient and less controlled stages.
- People who have access to the premises and are able to **adulterate the product without being discovered**. If there is a greater likelihood of being discovered, the probability of this occurring is greatly decreased.

Questions that the auditor should ask and the company should be able to provide an answer to:

1. What legal/customer food defence requirements are applicable to the company?
2. How can the company demonstrate compliance with such requirements?
3. How are external visits managed?
4. Which details were recorded during the last official visit?

4.1.3 Site security

There are many ways to manage threats and many types of situations that create a risk of unauthorised access. Examples of methods used to control unauthorised access can include fencing, guards, security alarms, electronic pass keys, locked doors, windows that do not open, cameras. In general, such measures should protect food and non-food products that are stored both inside and outside of the production site. Storage bins/silos are included. Measures such as sign-in procedures, keeping doors locked, etc. can supplement or substitute physical barriers.

Specific attention should be paid to easily accessible raw materials, intermediate and finished products, chemicals (cleaning agents, acids, lye, flammable liquids, etc.) as well as to equipment and materials that are stored outside, which must be protected from unauthorised access and possible threats of manipulation.

Controls for incoming and outgoing goods such as seals and labels can provide additional security. The seals should be traceable. A proper usage of seals increases security (e. g. that there are no opening gaps allowed).

According to requirement 4.21.2 the **identification of critical areas/practices, access policies for employees, visitors or contractors as well as the management of external visits**, and other appropriate control measures are to be included in the food defence plan and procedure.

Questions that the auditor should ask and the company should be able to provide an answer to:

1 Based on the food defence procedure and plan, what areas have been identified as critical?

2 What control measures are in place in order to control access to those areas and other premises?

3 Does the policy of access include the following people?
- Temporary employees
- Contractors
- Visitors
- Employees
- Carrier drivers

4 Are records available which provide evidence that all visitors and contractors have received the necessary introduction to facility requirements related to product defence before they have been permitted onsite?

4.1.4 Review and test of effectiveness

Requirement 4.21.3, IFS Food Version 8

The food defence plan shall be tested for effectiveness and reviewed at least once within a 12-month period or whenever significant changes occur.

WHY

Due to the nature of products and the high volatility of potential threats, it is essential to review the food defence plan regularly and at least once within a 12-month period.

A food defence plan for the implementation of the identified control measures will help the organisation in defining the schedule and resources necessary to maintain the plan. Threats with a high probability of occurrence should be prioritised. With the help of regular tests and exercises, weak points can be identified and existing defence measures can be complemented.

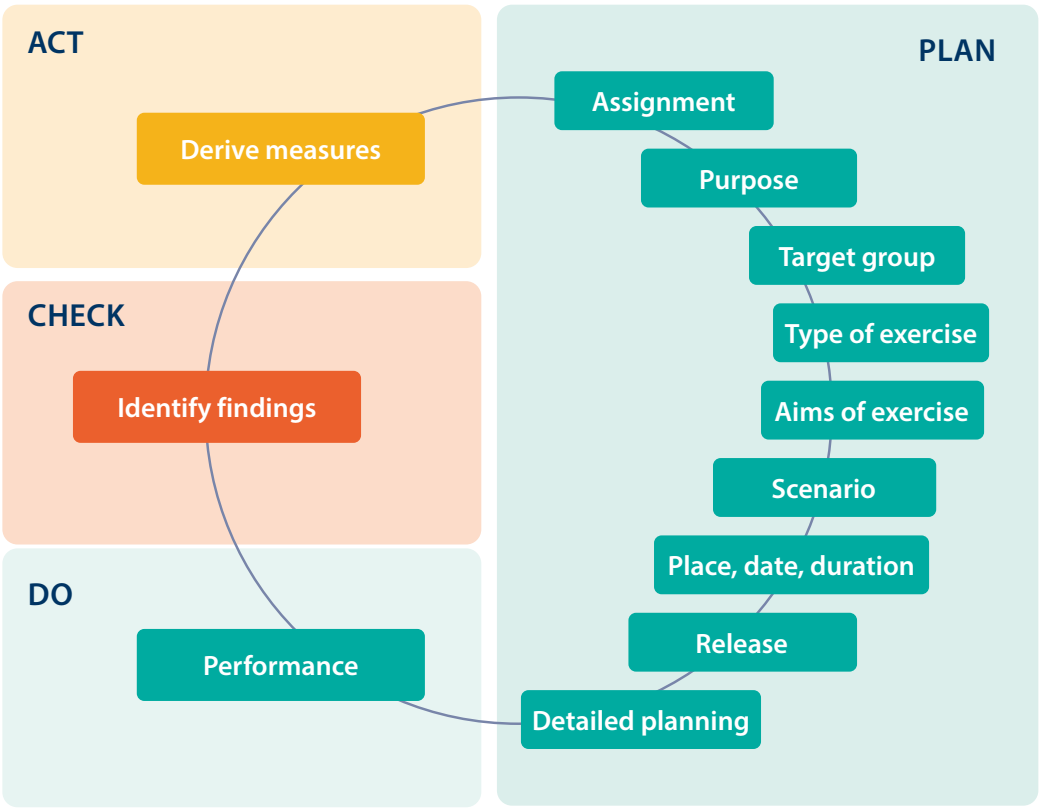
HOW

The food defence plan should be an established part of the internal audit process.

Once the plan is implemented, identified vulnerabilities controlled and deficiencies rectified, it is time for the review and tests of effectiveness. The regular review of the plan ensures that it remains current and relevant. Threats and their likelihood should be reassessed annually or following a significant change. The checklist in chapter 3 can be used for the review.

Tests of effectiveness can be performed internally or with an external service provider. FDA provides the Food Related Emergency Exercise Bundle (FREE-B), which is a compilation of scenarios based on both intentional and unintentional food contamination events (*https://www.fda.gov/food/food-defense-tools/food-related-emergency-exercise-bundle-free-b*). However, it is also possible to use scenarios that have been created independently. In this case the scheme which is shown in figure 9 could be considered.

FIGURE 9
The exercise process as a P-D-C-A cycle (plan – do – check – act)



Questions that the auditor should ask and the company should be able to provide an answer to:

1. How often is a review of the food defence plan performed?
2. What criteria does the company consider when determining the frequency of the assessment of threats and their likelihood of occurrence within the food defence plan?
3. When was the last test of effectiveness carried out? Internally or externally?
4. Has any incident or attack taken place since the last audit? How was it managed?
5. How is recurrence prevented?

4.1.5 Commitment of the senior management

Requirement 1.2.5, IFS Food Version 8

The senior management shall maintain a system to ensure that the company is kept informed of all relevant legislation, scientific and technical developments, industry codes of practice, food safety and product quality issues and that they are aware of factors that can influence food defence and food fraud risks.

Requirement 1.3.1, IFS Food Version 8

The senior management shall ensure that the food safety and quality management system is reviewed. This activity shall be planned within a 12-month period and its execution shall not exceed 15 months. Such reviews shall include, at a minimum:

- a review of objectives and policies including elements of food safety culture
- results of audits and site inspections
- positive and negative customer feedback
- process compliance
- food fraud assessment outcome
- food defence assessment outcome
- compliance issues
- status of corrections and corrective actions
- notifications from authorities.

WHY

The senior management is committed to include product defence into the existing management system because product defence can only be carried out effectively with the full support of the senior management.

HOW

The company should be kept up to date with the current risks in the area of product defence at all times. Furthermore, the results of the regular product defence assessment are to be considered within the management review.

Questions that the auditor should ask and the company should be able to provide an answer to:

1 How is the company kept up to date with regard to product defence risks?

2 Did the last management review identify a need for investment in product defence?

4.2 Explanations of the IFS HPC Product Defence Requirements

In this chapter the IFS HPC Product Defence Requirements are explained. The interpretation is exemplarily and can be transferred to other IFS Standards covering non-food products, such as IFS PACsecure, IFS Broker and IFS Logistics.

4.2.1 Responsibilities

Requirement 4.18.2, IFS HPC version 3

The responsibilities for product defence shall be defined. The responsible person(s) shall have full commitment from the senior management.

A product defence team (it could be a person or a team) shall be established, which is accountable to the facility management team. This team shall have defined roles and responsibilities which are reviewed on a regular basis.

The team should be interdisciplinary within the organisation (if applicable). The members/person should have appropriate knowledge and expertise about product defence and shall be able to propose the best course of action. In case of a team, a team leader should be responsible for the coordination, development, implementation, maintenance and improvement of the product defence procedures and mitigation measures.

It is recommended to include the review of the product defence plan in the annual senior management review.

Questions that the auditor should ask and the company should be able to provide an answer to:

1. Who is accountable for the product defence procedure and plan?
2. What competences and qualifications are demonstrated by the person(s) responsible for product defence?
3. What is the position of the person(s) responsible for product defence with respect to the senior management team?
4. How does senior management support the person(s) responsible for product defence?
5. Where are the responsibilities clearly defined?
6. Was this communicated to the members of the company? How?

4.2.2 Product defence procedure and plan and review

Requirement 4.18.1, IFS HPC version 3

A product defence procedure and plan shall be implemented in relation to assessed threats. This shall encompass a minimum of the following:

- identification of critical areas and/or practices and policy of access by employees, visitors and contractors,
- transport vehicles,
- IT
- legal requirements, if applicable,
- any other appropriate control measure.

The product defence plan shall be well known and established in the company and shall be reviewed annually and upon changes.

The company shall perform an assessment of the relevant threats and implement a product defence procedure and plan, with appropriate measures, based on the probability of the related threats.

IFS does not define what kind of assessment/procedure should be chosen. The company is free to develop its own tools/programs.

Regardless of the applied procedure and plan, all relevant security aspects of the location shall be taken into account. Records of the assessment are important evidence of effective implementation and provide information about the extent to which the product defence plan is confirmed.

As a result of this product defence assessment with regard to threats and their likelihood, the conditions under which there is a risk of intentional actions to adulterate and/or manipulate processes, materials and products should be identified.

Furthermore, it is important that the senior management has identified which personnel have access to certain areas and which do not.

Reviewing and verifying, at least annually or upon changes is necessary to ensure the effectiveness of the site security measures (for example, using knowledgeable in-house or third party staff to conduct tampering or other malicious, criminal, or terrorist action exercises and mock recalls and to challenge computer security systems).

The procedure and plan should be revised accordingly and detailed information should be kept confidential.

Questions that the auditor should ask and the company should be able to provide an answer to:

1 Based on the product defence assessment of threats and their likelihood, what areas have been identified as critical?

2 What control measures are in place to control access to those areas?

3 How does the company maintain control over who enters the premises and critical areas?

4 What access controls are applicable to the following groups of people?

- Temporary employees
- Contractors
- Visitors
- Employees
- Carrier drivers

5 Are visitors and contractors informed of the product defence rules and their scope while on company premises?

6 Does the company have the defined means to ensure that contractors who will spend a long time inside the plant are properly identified, supervised and escorted inside critical areas? Are there arrangements to have designated guides at all shifts?

7 Are there controls to ensure that truck drivers who load or unload products/materials are restricted to defined areas inside and outside the building and company premises? Are there means to watch the movements of non-employees once they enter company premises (e. g. cameras or guards at defined areas, other procedures)?

8 If contractors and visitors are provided with access keys, are those keys programmed to limit access to specified and selected areas?

9 Are access controls updated at the time of termination of an employee or when work is finished on the part of a contractor? Is access to the company's computer still possible for an employee once they are no longer associated with the company?

10 What legal/customer product defence requirements are applicable to the company?

11 When was the last review, what was checked and what had to be adapted?

4.3 Overview on product defence in further IFS Standards and Programs

The requirements for product defence are most comprehensively addressed in IFS Food due to the handling of open products and the direct impact on food safety. Depending on the scope of other IFS Standards and Programs, the requirements are similar or adapted to the respective area of application. The basic principles described in this guideline apply to all companies and the interpretation of individual requirements can be transferred accordingly.

IFS Logistics
The requirements for product defence in IFS Logistics are similar to those of IFS Food version 8. The focus of product defence in IFS Logistics version 3 is on transportation, shipping, receiving and dispatch of goods. Also, IT security is explicitly addressed. Furthermore, an appropriate alert system for product defence is required (4.5.4, IFS Logistics version 3).

IFS Broker
The IFS Broker Standard has very basic requirements related to product defence since there is no physical handling of the product under this IFS Standard. Nevertheless, a product defence assessment and plan of the suppliers (6.1) is required in IFS Broker version 3.2, as well as defined supplier responsibilities for product defence (6.2).

IFS Wholesale/Cash & Carry
The IFS Wholesale/Cash & Carry version 2 also relates to food processing and handling.
The requirements are therefore similar to those in the IFS Food Standard and the interpretation can be transferred.

// Overview on product defence in further IFS Standards and Programs

IFS PACsecure

The requirements for product defence in IFS PACsecure version 3 are similar to IFS HPC and the interpretation can be transferred. Detailed explanations can also be found in the guidance within the standard.

IFS Progress Food

The IFS Progress Food Program helps food suppliers to gradually establish comprehensive processes for food safety and quality. This program is divided into two levels, and IFS Food certification is usually the next objective. The basic level does not include any product defence requirements. The interpretation of the intermediate level of food defence requirements can be adopted from its respective requirement guidance in the IFS Progress Food Program. Also, IFS Food interpretation is an appropriate reference, while keeping in mind that variations may be considered as it is a developing program.

Please find an overview of the detailed product defence requirements of IFS Standards in annex.

5 Cybersecurity and product defence

5 CYBERSECURITY AND PRODUCT DEFENCE

5.1 Introduction

Given the tendency of food companies to introduce digital technologies throughout the food supply chain and the importance attached to the safety and reliability of these systems in Industry 4.0 applications, the risk that cyber incidents can impact food safety can no longer be entirely ruled out. (Susan E. Duncan et. Al.: Cyberbiosecurity – A New Perspective on Protecting U.S. Food and Agricultural System)

In the EU, Directive (EU) 2022/2555, also called NIS2 Directive, takes account of the fact that a common cybersecurity regulatory framework will enhance the level of cybersecurity across the European Union. The food industry is considered as a critical sector for cybersecurity in this directive.

Also, ISO 22000 gives cybersecurity relevance within the food/product safety management system. According to this generally accepted food safety norm, it is important to consider "(…) external and internal issues including but not limited to legal, technological, competitive, market, cultural, social, economic environments, cybersecurity, and food fraud, food defence and intentional contamination (…)". (ISO 22000, Section 4.1, Note 1, 2018)

Industry 4.0 refers to the intelligent networking of machines and processes for industry with the help of information and communication technology.
(*Federal Ministry for Economic Affairs and Climate Action Germany: www.plattform-i40.de*)

Due to the ever-increasing importance of IT/ICT solutions and the complicated geopolitical situation that increases the likelihood of cyberattacks, IFS wants to contribute to the awareness of companies with this chapter, which addresses the following points:

- Definitions (5.2)
- What should be protected? (5.3)
- What are the dangers and possible risks? (5.4)
- Implementation of Incident Response Management (5.5)
- Role of the product safety management (5.6)
- Conclusions (5.7)

The chapter "Cybersecurity and product defence" is intended to provide basic knowledge on the topic and is aimed both at companies that are implementing cybersecurity measures in their company for the first time and at those that want to work on existing cybersecurity measures. IFS would particularly like to address the role of product safety management in this context.

5.2 Definitions

The term cybersecurity is defined in this chapter as follows: "Cybersecurity is the stable environment that ensures and strengthens the exchange of digital data and the business continuity of the organisation. The development and maintenance of these processes must be continuously reviewed and improved. People and their knowledge as well as equipment and software are components of this system." (Andrzej Cieślak, Dynacon Sp. z o.o., 2022)

The aim is to raise awareness and help companies integrate cybersecurity measures, for example through incident response management (IRM, see chapter 5.5). IRM is used to prepare for emergencies and crisis situations so that business disruption is minimised and critical business operations can be restored as quickly as possible in the event of an attack. It can reduce the damage by, for example, quickly clarifying whether a disruption that has occurred is a cyberattack or merely a malfunction. Therefore, it is recommended to implement a cybersecurity system that addresses operational technology and information technology (e. g. Incident response management).

- **Cybersecurity:** Preservation of confidentiality, integrity, and availability of information in the cyberspace. (ISO 27031, 4.20)
  The ISO 27001 defines cybersecurity as the art to protect networks, devices, and data from unauthorised access or criminal use and the practice of ensuring confidentiality, integrity, and availability of information
  (Source: CISA – American Cybersecurity and Infrastructure Security Agency).

- **Information technology (IT)** focuses on data and communication. IT comprises the use of hardware and software to monitor and control physical processes, equipment and infrastructures.
  (Source: GARTNER DEUTSCHLAND GMBH [online]: Operational Technology. 2022).

- **Operational technology (OT)** focuses on the management and control of physical devices existing and operating in the physical world. OT includes the control of real-world devices through operational control systems which are often linked with electronic and digital technologies, such as computerized numerical control machining systems.

- **Information and communication technology (ICT)** is defined as a diverse set of technological tools and resources used to transmit, store, create, share or exchange information. These technological tools and resources include computers, the Internet (websites, blogs and emails), live broadcasting technologies (radio, television and webcasting), recorded broadcasting technologies (podcasting, audio and video players, and storage devices) and telephony (fixed or mobile, satellite, visio/video-conferencing, etc.).
  (Source: (UNESCO's International Institute for Educational Planning, learningportal.iiep.unesco.org, 2009)

5.3 What should be protected?

This question is crucial as the relevance and sensitivity of the data and what it should be protected against must be clear. This can be business secrets or other sensitive data (e. g. personal data) as well as networks and devices, where take-over or modifying operating equipment could possibly lead to a public health hazard.

To have an overview, it is recommended to develop an up-to-date list of all assets, including details on device connections, used protocols, and ports. Are there items in the inventory that are only momentarily linked to the network? It is also helpful to superimpose a dynamic communication map on the industrial processes. All personnel should have full awareness of the connection between assets and processes.

After completing the inventory and identifying the assets, a risk assessment can be performed for specific assets to identify threats and vulnerabilities. Based on the risk assessment, appropriate safeguards, which should be continuously monitored, can be established and implemented. If incidents are identified during the monitoring process, corrective actions should be taken to improve the system.

Applying current standards like ISO 27001, ISO 22301 and IEC 62443 (IEC – International Electrotechnical Commission) helps quality managers set boundaries and indicate a general framework.

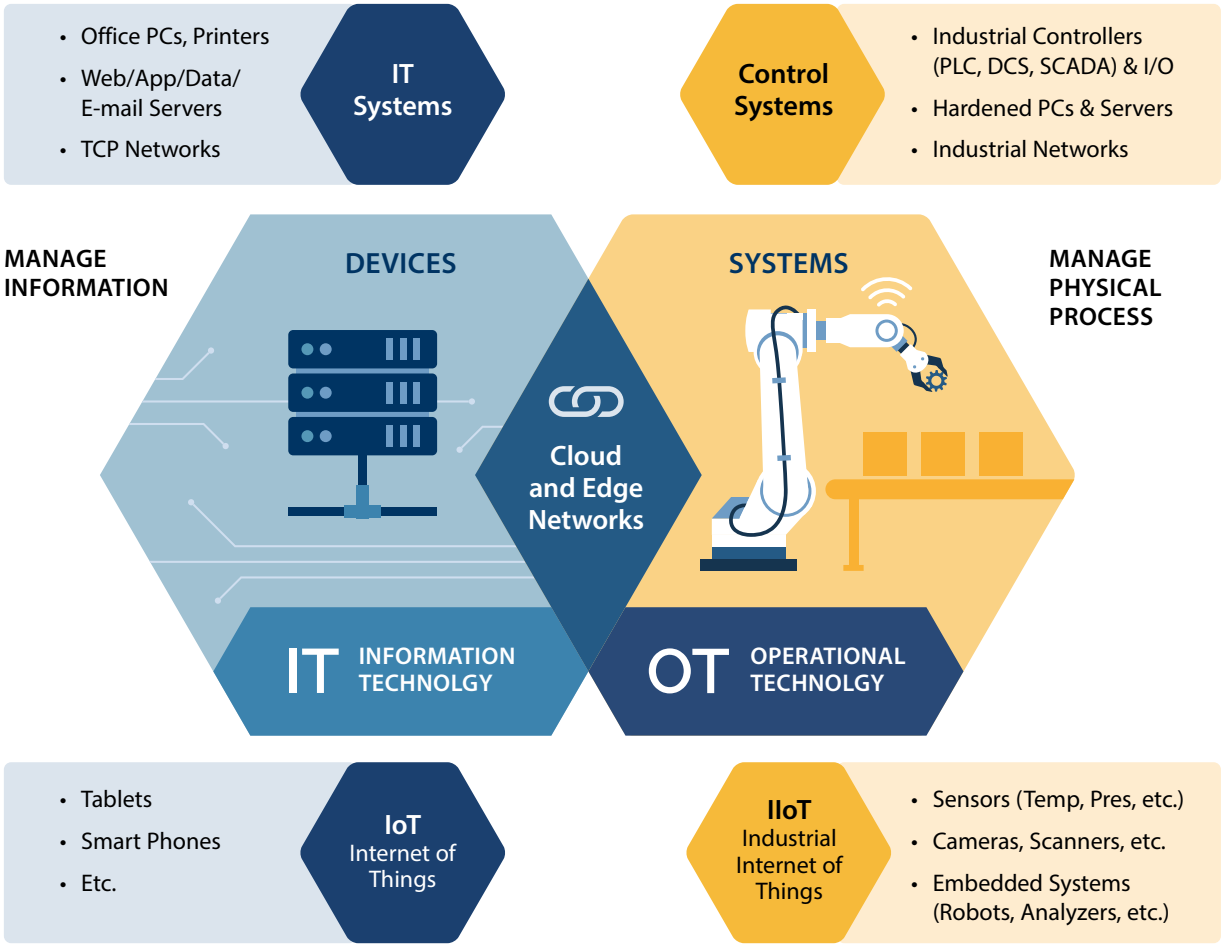
5.4 What are the dangers and possible risks?

With increasing possibilities and growing technical dependency on digital networks, the number of cyberattacks is also rising. Every technology is vulnerable to exploitation by hackers as long as the appropriate protection mechanisms are not implemented. A successful cyberattack can have a severe negative impact on an IT department, production, supply chain (transport, loading, ordering & order processing, etc.), product safety, personnel data and finally, the reputation of the company. These incidents are usually associated with high costs.

Convergence (merging) of IT and OT networks can make it more difficult to control them efficiently and can lead to major security gaps and vulnerabilities in the system. The risk of attacks on the OT, which could also impact product safety, can increase when it is connected to the more "vulnerable component" of IT. Cybercriminals might pretend to belong to a network and infiltrate the system via an Industry Internet of Things (IIoT) infrastructure which can lead to the manipulation of operational assets. But the risk of a cyberattack on OT is unlikely in practice and there is no known case so far where product safety has been directly affected by a hacking attack. However, there are several known cases where cyberattacks have caused major production and delivery failures (CNN: Cyberattack on food giant Dole temporarily shuts down North America production. 2023/02/22; BBC: Meat giant JBS pays $11m in ransom to resolve cyberattack. 2021/06/10).

Although external threats to OT are rare, internal threats should not be neglected. Food and non-food product safety can be threatened through the mistakes of an employee (intentional or unintentional) or a technician. In addition to the operational consequences and impact on the supply chain, the economic consequences can also be severe in the case of an overall production failure. Figure 10 shows which devices are used in the respective area.

FIGURE 10
Connection of IT, OT, IoT, IIoT and the respective devices



Industry-safe and -secure cybersecurity respects the differences between IT and OT environments, and thus the use of protection measures that take into account the specifics of these areas. OT areas should be under the responsibility of people who know and understand the specifics of this environment.

European Union Agency for Cybersecurity (ENISA) has sorted threats into eight groups (Source: ENISA, October 2022). The top cyberthreat reports are of a technical nature, and include findings, major incidents, statistics and more. The threat reports list the following top threats, which should be considered as examples, as the relevance changes quickly:

- Ransomware
- Malware
- Social engineering / Phishing
- Threats against data
- Threats against availability
- Disinformation – misinformation (AI-enabled disinformation, deepfakes and disinformation-as-a-service)
- Supply chain targeting (third-party incidents)

While the company's internal cybersecurity system is crucial for the first 5 threats, the key actions against disinformation and supply chain targeting include, among others: appropriate supervision of suppliers and management of their work and the effects of their work.

To complete the list of possible threats, Paragraph 79 of Directive (EU) 2022/2555 recommends "to protect network and information systems and the physical environment of those systems from events such as theft, fire, flood, telecommunication or power failures (…)". The cybersecurity system should therefore also address *"the physical and environmental security of network and information systems by including measures to protect such systems from system failures, human error, malicious acts or natural phenomena, in line with European and international standards, such as those included in the ISO/IEC 27000 series."*

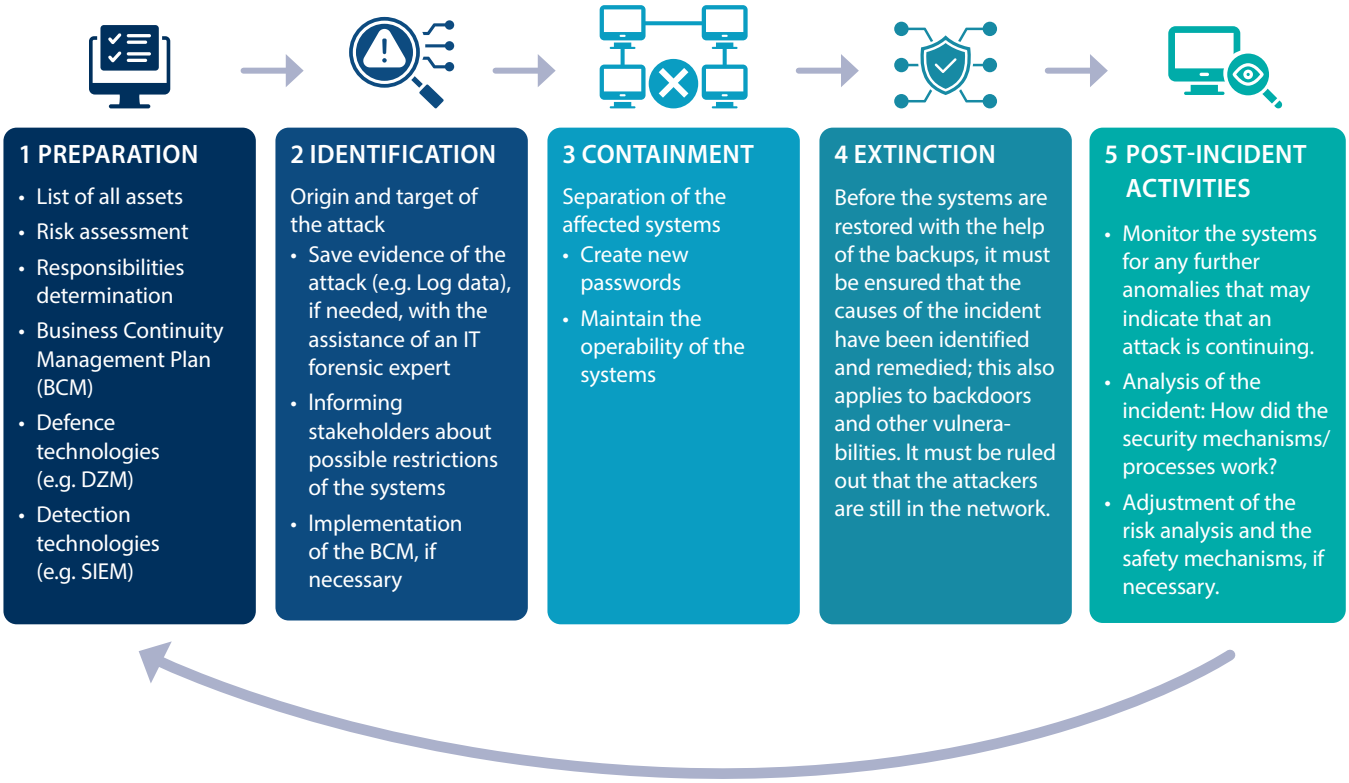
5.5 Implementation of Incident Response Management

Incident Response Management is one of the most effective ways to minimise the damage of a cyberattack. It not only prepares and protects against attacks, but also reduces downtime and the extent of the damage. Thus, processes can be resumed as quickly as possible and the negative impact minimised. Due to the interfaces of crisis management and IT systems, cooperation between the respective responsible persons is essential. It is important that the objectives, scopes, and responsibilities, as well as the framework conditions, are clearly defined. If this is coordinated in advance, a synergy can be recognised and used.

In addition, conducting exercises and tests (e. g. security tests, attack scenarios) is of great importance, as further security measures ("to do's") can be derived from them and thus a good learning effect can be achieved. Exercises could be performed e. g. through self-designed scenarios or scenarios provided by CISA (*https://www.cisa.gov/resources-tools/resources/cybersecurity-scenarios*).

FIGURE 11

Approach of Incident Response Management



Source: based on BOSCH CyberCompare Whitepaper: Schnell und entschieden auf Cyberattacken reagieren: So gelingt das Incident Response Management, 2022

The application of common risk management practices is useful to identify the weakness in product safety related systems when it comes to cybersecurity. (Prof. John W. Spink, Cybersecurity in ISO 22000 Food Safety Management, In Supply Chain Management: Sourcing, Operations & Logistics – including supply chain disruptions, and case studies of food fraud prevention, cybersecurity, and enterprise risk management, York Partners (Publishing) LLC, 2023)

5.6 Role of the product safety management

The responsibility for implementing an effective cybersecurity system does not lie primarily with the product safety management. The **tasks of the product safety management** in this context are to:

1. Identify IT intensive, vulnerable systems
2. Identify possible hazards linked to product safety and communicate them to the IT department.
3. Continuously review the cyberthreats, and the response from the IT department, to assure compliance with the product or food related standards.

Conducting IT/cybersecurity assessments or managing those systems is not the task of the product safety management. Rather, the product safety management (food or non-food) is accountable for sharing the expert, functional-area insight on critical infrastructure protection (what processes are the most vulnerable and why) – and assuring this product safety system is secured.

5.7 Conclusions

Cyberthreats are becoming more of a challenge and may affect all areas of production and food safety. Implementing an IRM can effectively protect against attacks or minimise the damage in the event of a cyber incident. An external (IT) service provider alone cannot solve the problem. This is because cybercrime will continue to exist in the future and with every new technology, new gaps and vulnerabilities will always appear. Thus, it is essential for companies to confront these problems internally. It is crucial to a successful cybersecurity management system that the IT and OT departments cooperate with each other so that the risk of a cyberattack can be reduced. It is also important that IT and management work together so that the problem of cybercrime is integrated into the existing management system. The senior management must effectively deal with problems as they arise, applying the same principles that apply to all management systems. Cybersecurity requires a team that includes a broad range of specialists (not only IT) – comparable with the HACCP team.

The objectives here should be:

- To bring IT security up to a state of the art standard, for which sufficient resources are provided
- Create an inventory of assets to be protected
- Exercises and security tests
- Staff training
- Take into account recommendations from national authorities (e. g. BSI in Germany) on IT-OT separation
- Identify interfaces
- Develop and manage further measures.

Questions to be asked:

- Is cybersecurity addressed as a risk in the management system next to product safety, product defence and product fraud?
- Which vulnerable points have been identified in the process flow, where cyberattacks are possible and which could lead to an adverse impact on product safety and quality?
- How is it ensured that cyberthreats, which could lead to compromised product safety or quality, are under control?
- Are staff trained on cyberthreats?
- Is traceability according to legal and, if applicable, customer requirements, ensured at any time, also in case of a cyberattack with IT system breakdown?
- In the event of changes in the process flow; is the risk assessment updated with regard to cybersecurity and product safety?
- What cyber incidents have been registered (recorded) in the organisation recently? How were they dealt with?

6 Annex

6 ANNEX

Product Defence Requirements in IFS Standards

IFS Food 8, IFS HPC 3, IFS Logistics 3, IFS Broker 3.2, IFS Cash & Carry 2, IFS PACsecure 3, IFS Progress Food 3

Nr.	IFS Food version 8	Nr.	IFS HPC version 3	Nr.	IFS Logistics version 3	Nr.
1.2.5	The senior management shall maintain a system to ensure that the company is kept informed of all relevant legislation, scientific and technical developments, industry codes of practice, food safety and product quality issues, and that they are aware of factors that can influence food defence and food fraud risks.			**1.2.3**	The senior management shall maintain a system to ensure that it is kept informed of all relevant legislation, scientific and technical developments, industry codes of practice, product safety and product quality issues, and that they are aware of factors that can influence product defence and product fraud risks. The legal requirements shall be implemented by the respective department(s).	
1.3.1	The senior management shall ensure that the food safety and quality management system is reviewed. This activity shall be planned within a 12-month period and its execution shall not exceed 15 months. Such reviews shall include, at a minimum: • a review of objectives and policies including elements of food safety culture • results of audits and site inspections • positive and negative customer feedback • process compliance • food fraud assessment outcome • food defence assessment outcome • compliance issues • status of corrections and corrective actions • notifications from authorities.			**1.3.1**	The senior management shall ensure that the product safety and quality management system is reviewed. This activity shall be planned within a 12-month period and its execution shall not exceed 15 months. Such reviews shall include, at a minimum: • a review of objectives and policies, including elements of product safety culture • results of audits and site inspections • positive and negative customer feedback • process compliance • product fraud assessment outcome • product defence assessment outcome • compliance issues • status of corrections and corrective actions • notifications from authorities	
3.3.4	The contents of training and/or instruction shall be reviewed and updated when necessary. Special consideration shall be given to these specific issues, at a minimum: food safety • product authenticity, including food fraud • product quality • food defence • food related legal requirements • product/process modifications • feedback from the previous documented training/instruction programs.	**3.5.4**	The contents of training and/or instruction shall be reviewed and updated when necessary. Special considerations shall be given at a minimum to these specific issues: • product safety and quality (e.g. GMPs, risk assessment, etc.), • product safety culture, • product defence, • product related legal requirements, • product/process modifications, • feedback from the previous documented training/ instruction program.			

IFS Broker version 3.2	Nr.	IFS Cash & Carry /Wholesale version 2	Nr.	IFS PACsecure version 3	Nr.	IFS Progress Food version 3
					1.1.7	The senior management shall maintain a process to ensure that the company is kept informed of all relevant legislation, scientific and technical developments, industry codes of practice, food safety and product quality issues, and that they are aware of factors that can influence food defence and food fraud risks.

// Product Defence Requirements in IFS Food 8, IFS HPC 3, IFS Logistics 3, IFS Broker 3.1, IFS Progress Food 3, IFS Cash & Carry 2, IFS PACsecure 2

Nr.	IFS Food version 8	Nr.	IFS HPC version 3	Nr.	IFS Logistics version 3	Nr.
4.21.1	The responsibilities for food defence shall be defined. The responsible person(s) shall have the appropriate specific knowledge.	**4.18.2**	The responsibilities for the product defence shall be defined. The responsible person(s) shall have full commitment from the senior management.	**4.5.1**	The responsibilities shall be defined for the product fraud vulnerability assessment and mitigation plan as well as for the product defence. The responsible person(s) shall have the appropriate and specific knowledge.	
4.21.2	A food defence procedure and plan shall be documented, implemented and maintained to identify potential threats and define food defence measures. This shall include, at a minimum: • legal requirements • identification of critical areas and/ or practices and policy of access by employees • visitors and contractors • how to manage external inspections and regulatory visits • any other appropriate control measures	**4.18.1**	A product defence procedure and plan shall be implemented in relation to assessed threats. This shall encompass at a minimum: • identification of critical areas and/or practices and policy of access by employees, visitors and contractors, • transport vehicles, • IT • legal requirements, if applicable, • any other appropriate control measure. The product defence plan shall be well known and established within the company and shall be reviewed annually and upon changes.	**4.5.4***	A product defence procedure and plan shall be documented, implemented and maintained to identify potential threats (internal and external) and define product defence measures. This shall include, at a minimum: • legal requirements (evidence of registration or on-site inspections necessary • identification of critical areas and/ or practices and policy of access by employees • visitors and contractors • how external inspections and regulatory visits are to be managed • site security conditions • transportation, shipping, receiving and dispatch of goods • IT (cyberattack) • any other appropriate measures The criteria considered in the vulnerability assessment shall be defined. An appropriate alert system shall be defined and periodically tested for effectiveness.	**6.1**
4.21.3	The food defence plan shall be tested for effectiveness and reviewed at least once within a 12-month period or whenever significant changes occur.			**4.5.5**	The product defence plan and product fraud vulnerability assessment shall be reviewed at least once within a 12-month period or whenever significant changes occur. If necessary, the product fraud mitigation plan shall be updated accordingly.	**6.2**

IFS Broker version 3.2	Nr.	IFS Cash & Carry /Wholesale version 2	Nr.	IFS PACsecure version 3	Nr.	IFS Progress Food version 3
			4.21.1	The responsibilities for product defence shall be defined. The responsible person(s) shall have the appropriate specific knowledge.	**4.21.1**	The responsibilities for food defence shall be defined. The responsible person(s) shall have the appropriate specific knowledge and training.
The company shall ensure that suppliers' responsibilities for product defense are clearly defined.	**6.1.1.1**	A product defense hazard analysis and assessment of associated risiks shall have been performed and documented. Based on this assessment and legal requirements, areas critical to security shall be identified and protected. Product defense hazard analysis and assessments of associated risks shall be reviewed anually or upon changes that could effect product integrity. An appropriate system for handling irregularities shall be defined and regularly tested for effectiveness.	**4.21.2**	A product defence assessment, including assessment criteria, shall be documented, implemented and maintained to identify potential threats and define product defence measures. This shall include, at a minimum: • legal requirements • customer requirements • site security conditions • identification of critical areas and/or practices and policy of access by employees • visitors and contractors • how to manage external inspections and regulatory visits • any other appropriate control measures.	**4.21.2**	A food defence procedure and plan shall be developed to identify potential threats and define food defence measures. This shall include a minimum of: • legal and customer requirements • identification of critical areas and/or practices and policy of access by employees • visitors and contractors • any other appropriate control measures.
	6.1.1.2	If legislation makes registration or on-site inspections necessary, evidence shall be provided	**4.21.3**	A product defence plan shall be documented, implemented and maintained, with reference to the product defence assessment, and shall include the testing and monitoring methods.		
The company shall ensure that suppliers and logistics service providers have performed and documented a product defense hazard analysis and assessment of associated risks. Based on this assessment and legal requirements the supplier/service provider shall implement a product defense plan to mitigate identified risks.	**6.1.1.3**	All employees shall be instructed activity-related in reference to defense of products or in case of significant changes of the program for product defense by evidence.	**4.21.4**	The product defence plan shall be tested for effectiveness and reviewed at least once within a 12-month period or whenever significant changes occur. If necessary, the product defence plan shall be revised/updated accordingly.	**4.21.3**	The food defence plan shall be tested for effectiveness.

The IFS publishes information, opinions and bulletins to its best knowledge, but cannot take any responsibility for any mistakes, omissions or possibly misleading information in its publications, especially in this document.

The owner of the present document is:

IFS Management GmbH
Am Weidendamm 1 A
10117 Berlin
Germany

Managing Director: Stephan Tromp
AG Charlottenburg
HRB 136333 B
VAT-N°: DE278799213

Bank: Berliner Sparkasse
IBAN number: DE96 1005 0000 0190 0297 65
BIC-/Swift-Code: BE LA DE BE

The English version is the original and reference document.

The IFS Documents are available online via:
www.ifs-certification.com

ifs-certification.com

Follow IFS on Social Media

Published: July 2024