IFS Food

IFS Guideline for Food and Product Defence

VERSION 1.1

JANUARY 2023

ENGLISH

Content

IFS Guideline for Food and Product Defence

Acknowledgements

IFS would like to thank all participants who contributed to the review process for the IFS Food and Product Defence Guideline. In particular, IFS would like to thank Andrzej Cieślak, Barbara Szymańska and Dawid Stępień (Dynacon Sp. z o.o.) for their support on the topic of cybersecurity in the food industry.

IFS Guideline for Food and Product Defence

1 Background

The first version of the IFS Guideline for implementing food and product defence has been written by the North American IFS Working Group in order for IFS Food certified suppliers around the world to understand the intent of the food/product defence requirements, and to gain an understanding of implementation practices and considerations.

This update of the guideline has been adapted to the current IFS Food Version 7 and product defence requirements and further expanded to include aspects of cybersecurity, which is playing an increasingly important role in the safe production of food.

Food defence strategies were introduced in the regulatory requirements deployed by the US Food and Drug Administration (FDA) and the United States Department of Agriculture (USDA) with the Food Safety Modernization Act (FSMA) in 2010. This resulted in 13 optional requirements in previous IFS Food Standard versions, tailored to companies exporting or operating within the United States. However, in the latest version of the standard, the number of requirements was reduced to four (4) which are now applicable to all certified companies globally.

Due to the fact that besides the US no other market has introduced similar legislation, some stakeholders of the supply chain still do not feel comfortable with the implementation of defence plans. The IFS Guideline for Food and Product Defence is meant to provide support in this area and answer the following frequently asked questions:

- Who is responsible within an organisation for the implementation of the requirements?
- What should be considered during the development of a food/product defence plan?
- How can threats and their occurrence probability be defined and appropriate measures implemented?
- Which requirements should be considered at which part of the production site?
- When should the requirements be implemented and corresponding checks of the implementation be carried out?

- Why each requirement is important to the production site and/or organisation implementing the criteria?
- How the requirement can be implemented in a practical, effective way?
- What IFS expects concerning cybersecurity?

The aim of this guideline is to equip companies with the right prevention methods to manage threats resulting in food and product contaminations. Furthermore, employees can use this guideline to prepare themselves and consequently reduce the risk of occurrence of intentional actions to contaminate food products.

2 Definitions of Food and Product Defence

Food/product defence does not have an international and unique definition but below are two definitions offered by United States authorities that describe their intent behind a food/product defence strategy.

Food defence is the collective term used by the US Food and Drug Administration (FDA), United States Department of Agriculture (USDA), Department of Homeland Security (DHS), etc. to encompass activities associated with protecting the nation's food supply from deliberate or intentional acts of contamination or tampering. This term encompasses other similar verbiage (i.e., bioterrorism (BT), counter-terrorism (CT), etc.)

The USDA Food Safety and Inspection Service define food defence as "the protection of food products from intentional adulteration by biological, chemical, physical or radiological agents.

A misconception of food/product defence is to consider it a synonym of food security. Food security is defined below.

Food Security – When all people at all times have both physical and economic access to enough food for an active, healthy life. Food security includes both physical and economic access to food that meets people's dietary needs and food preferences.

The purpose of a food and product defence plan is to identify, mitigate and monitor possible sources of intentional contamination of food or products. It is the purpose of a HACCP system to identify unintentional physical, chemical and biological hazards which are significant to food safety. While food safety and food/product defence programs exist independently, there are common elements (e.g. the sealing of transportation vessels).

IFS definition of food/product defence: Procedures implemented to assure the protection of food and non-food products and their supply chain from malicious and ideologically motivated threats.

Figure 1: Food protection matrix (Spink, J. and Moyer, D. C., 2011)

			Motivation/Effect
	Food Quality	**Food Fraud** (includes EMA and Food Fraud)	*Economic profit*
	Food Safety	**Food Defence**	*Damage: health, economy, terror*
Action	*unintentional*	*intentional*	

2.1 Key Points to consider for the practical implementation

There is no singular defined structure for a food/product defence plan. Therefore, the plan should be developed considering different factors which may include:

- **Surroundings and construction**/design of the production site (geographic location, adjacent facilities, criminal index of the zone …).
- **Accessibility to the production site:**
  - Enclosed production buildings are less vulnerable than facilities where part of the production is done in exterior areas;
  - Use of contract and temporary employees may be a major risk in facilities where the number of employees is low and with low turnover;
  - 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 nature of some products** may make them more vulnerable to intentional adulteration than others. Characteristics may include:
  - Large production batch size;
  - Uniformity;
  - Product categories;
  - 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;
- Harm to others,

- **Cybersecurity system** that addresses operational technology and information technology (e.g. Incident response management).

2.2 Structure of the Food/Product Defence plan

Food/product defence plans typically include the following criteria which may be modified depending on the country, organisation, and regulatory requirements.

- Clear roles and responsibilities, management commitment and employee awareness.
- Assessment of occurrence probability and of threats for the products, facility and facility surroundings.
- Identification of vulnerabilities and the determination of control measures.
- Implementation and suitability of the plan.
- Internal audits of the entire food/product defence plan.
- Continuous improvement of the plan.

3 Explanation of the IFS Food and Product Defence requirements

3.1 Defence Assessment

A food/product defence team or a single person, accountable to the facility management team, shall be established with defined roles and responsibilities. Those responsible person(s) shall have the full commitment from the senior management.

The team shall report to the management and shall have experience in the area of food/product defence. Competence can be gained through training and/or relevant experience in this area.

IFS does not define what the food/product defence plan should look like. The company is free to develop its own tools. It might be helpful to consider the approach of a VACCP method (vulnerability analysis critical control point—"weak points" analysis and identification of critical control points, which is structured analogous to the classic HACCP; however, its focal point is comprehensive site security).

Records are evidence of effective implementation and provide information about the extent to which the food/product defence 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).

Requirement 6.1, IFS Food Version 7

The responsibilities for the food defence plan shall be clearly defined. Those responsible shall have the appropriate specific knowledge and training, and have full commitment from the senior management.

WHY

It is essential that the food/product defence team has a solid knowledge and receives regular training since potential threats are constantly evolving. The senior management committment is crucial since the food/product defence team may take decisions that impact operational and financial aspects of the company.

HOW

"Those responsible" 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 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.

If applicable (if specific food/product 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.

Food/product defence training should be provided to employees appropriate to their duties. The senior management review should include the food/product defence plan (see also requirements 1.2.5 and 3.3.4).

QUESTIONS THAT THE AUDITOR SHOULD ASK AND THE COMPANY SHOULD BE ABLE TO PROVIDE AN ANSWER TO:

1. Who is accountable for the food/product defence plan?
2. What are the competence and qualifications demonstrated by the person(s) responsible for the food/product defence plan?
3. Are training/education records available for the responsible person(s)?
4. How does senior management support the person(s) responsible for the food/product defence plan?
5. Where are the responsibilities defined? Can employees describe their responsibility?
6. Was this communicated to the members of the company? How?

Requirement 6.2, IFS Food Version 7

A food defence plan and procedure shall be developed based on probability and be implemented in relation to assessed threats.

This shall include:

- legal requirements
- identification of critical areas and/or practices and policy of access by employees
- visitors and contractors
- any other appropriate control measure.

The food defence plan shall be reviewed at least annually, and updated when appropriate.

Ideally companies/auditors implement/audit this requirement in three iterative parts: Development of plan, Site security, Review.

The first part requires the development of a food/product defence plan that takes all applicable threats and the likelihood of their occurence into account.

Applicable threats (Part 2 of the requirement) can be derived, for example, from legal requirements, the company environment, the number and type of visitors/ contractors or IT related sources (cyber threats).

The food/product defence plan should be developed, implemented, documented and evaluated (Part 3 of the requirement).

WHY

It is essential to gain a broad overview of all applicable threats to develop an effective food/product defence plan.

A detailed assessment of the legislation in the production and destination country is particularly important to avoid legal complications.

In any case, the likelihood of occurence should be considered to cover all necessary 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:

I) threat identification,

II) threat characterisation,

III) exposure assessment, and

IV) characterisation of occurrence probability.

All threats should be compared with historical and anticipated events, to evaluate the aforementioned four iterative steps. It may also help to determine acceptable levels of occurence and when to take corrective actions.

The company should use checklists and/or software to map the threats and determine the level of risk for each threat.

While only examples, the following may help with identifying 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 convenience and less controlled stages.
- People who have access to the premises and are able to **adulterate the product without being discovered.** If people fear being discovered, the likelihood and severity of occurrence is greatly decreased.
- People gaining access to critical IT infrastructure, because little or no cyber security is established on-site. **Cyber threats** are becoming more of a challenge and may affect all areas of production and food safety.

QUESTIONS THAT THE AUDITOR SHOULD ASK AND THE COMPANY SHOULD BE ABLE TO PROVIDE AN ANSWER TO:

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

2 How can the company demonstrate compliance with such requirements?

3 What is the process/procedure used to perform the food/product defence plan including assessment of threats and their occurence probability?

4 Is the food/product defence plan in line with legal and/or customer needs and/or expectations?

5 Does the food/product defence plan acknowledge cybersecurity?
Is traceability according to legal and, if applicable, customer requirements, ensured at any time, also in case of a cyber attack with IT system break down?

3.2 Site Security

The second part of requirement 6.2 includes the identification of critical areas/practices, access policies for employees, visitors or contractors and other appropriate control measures. It also includes methods and responsibility for managing inspections and regulatory visits.

Requirements for site security can also be found in Chapter **4.9 Production and storage premises** of the IFS Food version 7. These requirements are supplemented with additional requirements relevant to food/product defence.

WHY

The implementation of control measures defined in the food/product defence plan should result in control of threats and reduction of occurrence probability, through preventing unauthorised access to products, ingredients and services that could adversely affect the content or safety of the food/product.

HOW

Through a combination of effective and concrete food/product defence measures (physical barriers, procedures and systems), that work together to prevent uncontrolled access to:

- areas external of the production site,
- all areas of processing and storage,
- areas internal of the site, besides production and storage (e.g. laboratories handling chemicals and reagents),
- waste disposal areas where potentially hazardous materials are disposed,
- service areas such as water, gas, electric, refrigeration systems,
- information technology and operational technology, etc.

Such barriers and procedures should, applied properly, provide adequate protection of food and non-food products and the systems used to manufacture and store it.

Measures established should be appropriate to effectively manage possible food/product defence threats.

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 would be included. Computer systems should be fire-walled and password protected. 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 in case of 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 (e.g. that there are no opening gaps allowed) increases security.

It is recommended to implement adequate measures to prevent unauthorised access to information technology and operational technology. Cyber threats should be controlled with the aid of an effective cybersecurity system that also takes employee awareness of identified threats into account. The risk of adverse impact of cyber attacks on food safety, product legality, quality and authenticity should be minimised.

QUESTIONS THAT THE AUDITOR SHOULD ASK AND THE COMPANY SHOULD BE ABLE TO PROVIDE AN ANSWER TO:

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

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

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

4 Does the policy of access include the following people?

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

5 Are records available providing evidence that all visitors and contractors receive the necessary introduction to facility requirements related to food/product defence before they have been permitted on-site?

6 Which cyber threats have been identified and how are they prevented and monitored? Are staff trained on cyber threats?

3.3 Review and test of effectiveness

The third step regarding requirement 6.2 is the annual review of the product defence plan, which includes the occurrence probability of threats.

WHY

Due to the nature of food/product threats and the high volatility of potential threats, it is essential to review the food/product defence plan regularly and at least on an annual basis.

HOW

In order to identify vulnerabilities, the food/product defence team should consider the following (not an exhaustive list) during the annual review of the food/product defence plan:

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 there adequate lighting?
- Is the access of people and vehicles controlled?
- Are there back-up sources of critical utilities, such as electrical, water, information technology (computer data), and refrigeration systems available, in case of emergency?
- Are parking areas controlled and monitored?
- Are ventilation systems adequately protected?
- How are bulk receiving and storage areas secured (a responsible of the receiving party should be present during unloading, access to storage should be controlled)?

Interior

- Are surveillance methods utilised—such as cameras, staff supervision, or security services?
- Are all intermediate and finished products secured and monitored?
- Is access controlled?
- Are hazardous materials or controlled substances managed (e.g. chemicals like cleaning agents, acids, lye, flammable liquids)?
- Is access of staff 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 deliveries and shipments scheduled?
- Are transportation vendors part of the vendor approval program?
- Are any missed or delayed deliveries investigated?
- Are returned goods permitted? If so, are they managed?

Raw Materials

- Are water, ice and steam sources secure and monitored?
- Are all raw materials secured and monitored when not in use?
- Are there means to verify integrity and the chain of custody?
- Are packaging materials and product labels and seals (if applicable) controlled?

Personnel

- Are personal background checks necessary or performed, if allowed by law?
- Is the potential for retaliatory actions by terminated employees assessed?
- Are the reasons for an employee's departure reviewed?
- Are personnel supervised? Are cameras allowed?
- Are employees trained in food/product defence awareness and identifying/ reporting unusual or suspicious behavior?
- Are lockers inspected?
- Are personal items restricted in processing areas?
- Is there a policy addressing legal or illegal weapons and drugs?

Cybersecurity

- Are identified cyber threats up to date?
- Are these threats effectively controlled?

Once the organisation identifies food/product 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.

The individual steps of IFS Food/Product Defence requirement 6.2, IFS Food Version 7, in the context of further IFS Requirements

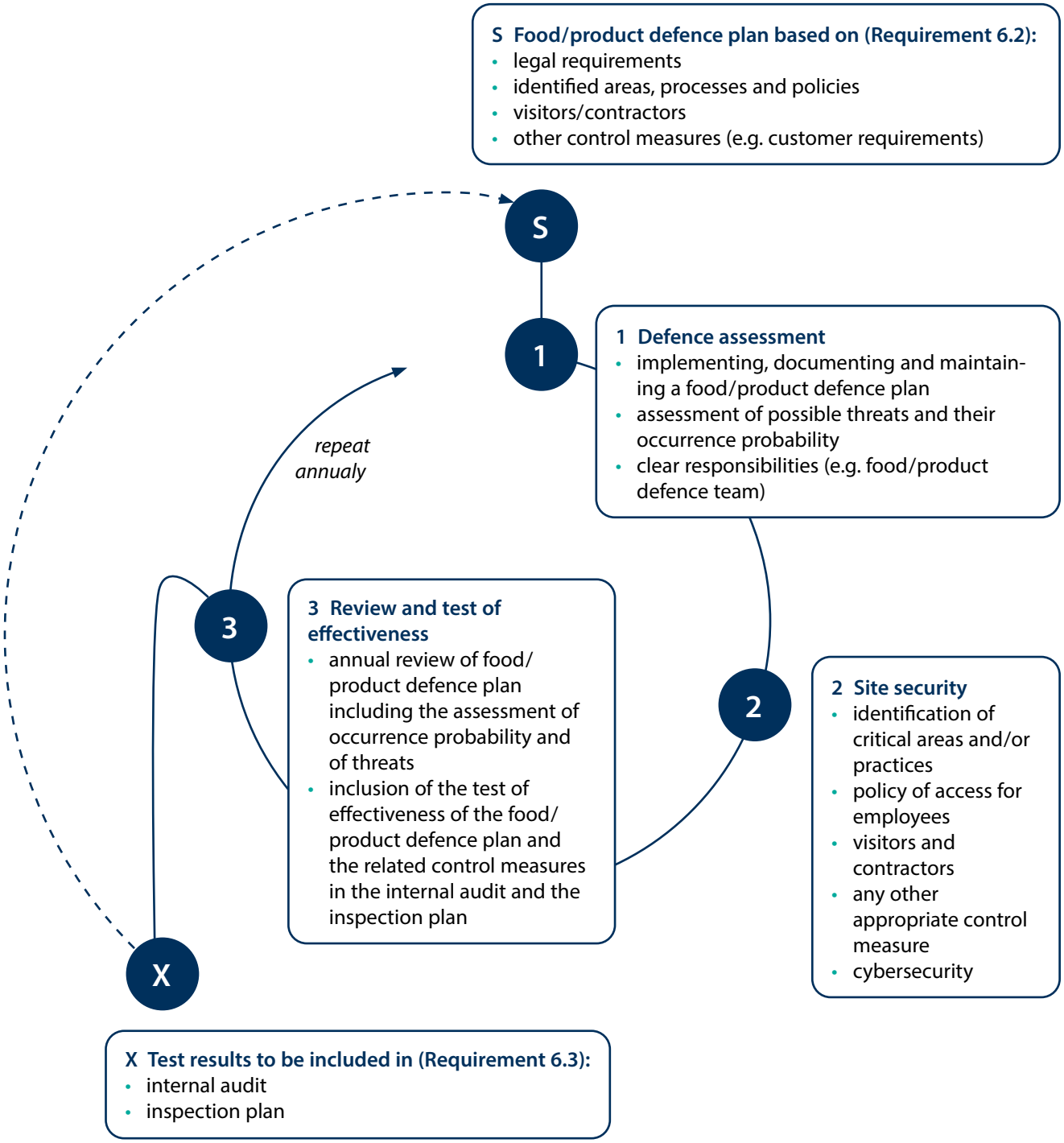

Figure 2: Schematic presentation of conducted steps by a company to fulfil the IFS Food/ Product Defence requirement 6.2 and prerequisite for requirement 6.3.

Requirement 6.3, IFS Food Version 7

The test of effectiveness of the food defence plan and the related control measures shall be included in the internal audit and the inspection plan.

WHY

A food/product defence plan to implement the identified control measures will help the organisation in defining the schedule and resources necessary to maintain the plan. Threats with high probability of occurrence should be prioritised.

HOW

The food/product 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.

The regular review of the plan ensures that it remains current and relevant. Threats and their probability of occurrence should be reassessed annually or following a significant change.

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/product 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/product defence plan?
3. Does the internal audit and inspection plan include the test on the effectiveness of the food/product defence plan?
4. Has any incident concerning food/product defence occurred since the last review? If yes, which measures have been subsequently taken?
5. Has a cyber incident taken place since the last audit? How was it managed?
6. How is recurrence prevented?

3.4 External Inspections

The inspection procedure should describe the methods and responsibility for managing inspections and regulatory visits. This requirement is not applicable (N/A):

- in countries where no legislation exists and/or
- external inspections regulatory visits are not requested or
- the company doesn't export to the US (no FDA inspection possible).

Requirement 6.4, IFS Food Version 7

A documented procedure shall exist for managing external inspections and regulatory visits. Relevant personnel shall be trained to execute the procedure.

WHY

As a part of the food/product defence program, this procedure ensures that sufficient resources are devoted to regulatory compliance and customer inspections. It also ensures that only authorised personnel have access to manufacturing, storage areas, and the sample collection.

HOW

This procedure should describe the methods and responsibility for managing inspections and regulatory visits.

This procedure should be utilised any time an external inspection or regulatory visit is conducted and reviewed on an annual basis or more frequently if necessary.

QUESTIONS THAT THE AUDITOR SHOULD ASK AND THE COMPANY SHOULD BE ABLE TO PROVIDE AN ANSWER TO:

1. Is there a documented procedure defining the criteria to follow in case an external organisation requires access to the company's premises?
2. Are there clearly defined levels of authorities providing external organisations access at all times?
3. Are relevant functions aware of their responsibilities under such conditions?
4. Are levels of authority/responsibilities defined for different information that may be made available?
5. Are there means to ensure a complete record of activities carried out and details of the visit?
6. Are training records available?

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 Standard owner of the present document is:

IFS Management GmbH
Am Weidendamm 1A
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

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

ifs-certification.com