# Vulnerability Management Initiatives

**A comparison of Vulnerability Management Initiatives in agri-food chains on the island of Ireland and in selected OECD countries**

safefood 20 years promoting North/South working

# Vulnerability Management Initiatives

**ISBN: 978-1-905767-90-8**
**Date: June 2019**

# Executive summary

In recent years, food supply chain resilience has emerged as a key challenge for businesses in the context of risks arising from to a range of internal and external forces. High impact but low probability events ("black swan events") are of increasing concern due to the challenges posed by globally-interconnected chains. These conditions give rise to economically motivated adulteration of food products and ingredients as well as ideologically motivated threats. Furthermore, social media and the internet amplify the impact and reputational risks associated with such events.

This research investigated the level of awareness and practice of key food system stakeholders on the Island of Ireland (IoI) vis-a-vis such challenges and considered this in relation to approaches and practices in other selected member countries of the Organisation for Economic Co-operation and Development (OECD). Hence this study considers various food supply chain Vulnerability Management Initiatives (VMIs) and puts forward a summative Vulnerability Management Framework (VMF).

Beginning with a systematic literature review, the methodology employed a survey and in-depth interviews and provides insight into this aspect of supply chain resilience – one which to date has received little attention on the IoI. The literature review provides a summary of definitions and concepts, together with a categorisation of standardisation initiatives and of current practices. The details of these are given in Appendix 1, the first relating to economically motivated hazards, and the second to ideologically motivated ones. The literature review also established a conceptual basis and guidance for the development of two strands of fieldwork: an online survey of industry and in-depth interviews with expert stakeholders. The survey established a baseline regarding industry awareness of, and measures taken to address, these challenges. Data from in-depth interviews with a range of stakeholders was integrated with the quantitative analysis of the industry survey. In-depth interviews with stakeholders from regulatory agencies, industry representative groups and experts in this field from four other OECD countries (Denmark, the UK, the Netherlands and the USA) supported cross-country analysis that led to the development of a VMF.

The study identifies key characteristics of food vulnerabilities arising from economically motivated adulteration and ideologically motivated threats. As such these vulnerabilities are distinguished from those that may arise due to quality control and assurance process failures, because perpetrators set out to act opportunistically in their own self-interest and to the detriment of the buyer/food system.

Survey and interview data from the IoI indicated an awareness of the challenges presented by intentional adulteration of product with different views on the significance of food fraud and food threat. Specifically, results from the online survey of 176 industry respondents indicate that the industry believes that adulteration for economic gain is a bigger concern than adulteration for malicious intent. While respondents are somewhat evenly divided in terms of viewing such concerns as a major or growing risk, seven in 10 respondents report they have an active system in place to deal specifically with adulteration/misrepresentation.

VMIs identified on the IoI, based on reported incidents, were classified as proactive (namely, (i) vulnerability assessment processes and (ii) surveillance and information-sharing databases) and reactive (primarily, (i) delist the supplier, (ii) increase supplier auditing, and (iii) enhance product testing). While very few food threats were reported by respondents, analysis of more general responses and interview data points to the role of employee vetting and site security measures, with particular reference to Publicly Available Standard 96 (PAS 96). The role of measures at governmental level was highlighted for threats arising externally.

VMIs identified in OECD countries studied were classified as initiatives; (i) based on the institutional landscape, including changes in existing institutions and the establishment of new units/structures (ii) based on collective private sector-led action, e.g. data sharing and development of standards and (iii) company practices undertaken to address vulnerabilities, e.g. in-house data collection through testing and monitoring.

A typology of VMIs is presented. The analysis classifies VMIs as those that are firm/agency centric and those that involve different types and levels of collaboration. The roles of both organisational and system-wide initiatives are considered. This points to a role for both and highlights benefits that could be derived from enhanced collaboration at both industry and public-private partnership levels. Mechanisms to ensure confidentiality, such as protocols governing exchange and use of data, are key to building the trust required to support collaboration.

A VMF is used to illustrate the main elements of strategies that aim to detect, deter and prevent economically or ideologically-motivated food product adulteration. In this context a number of underlying themes are identified. Analysis of these informs strategy design and deployment, including vulnerability assessment and preventative countermeasures.

These strategies are set within an institutional landscape in which both public and private organisations play a role in establishing regulations, standards and processes that influence and support organisational behaviour and responses at food supply chain actor and system levels.

# Key project recommendations

1. Establish an industry-based network to share experience and data in the area of food fraud and threat. This could complement or merge with existing industry networks such as FIIN and most likely employ a third-party service provider to manage data collection, analysis and dissemination of results. [Industry-led]

2. Development and delivery of training for industry personnel and auditors of accredited standards in assessing compliance with food fraud and threat requirements [Accreditation and Standards organisations in conjunction with the Food Standards Agency in Northern Ireland (FSA NI) and the Food Safety Authority of Ireland (FSAI)].

3. Develop exemplar template flowcharts for specific products. These flowcharts would include: (i) initial screening and more detailed screening steps, (ii) use of data from open access databases (e.g. Rapid Alert System for Food and Feed (RASFF)) and/or private databases (e.g. Decernis, Foodakai), (iii) specific analytical tests (both rapid and validated) for this product, (iv) design and deployment of countermeasures and controls relevant to this product category, and (v) mechanism for anonymous flow of data into repository held by a 3rd Party. [Agencies and Industry representative bodies]

4. Maintain a review of state-of-the-art analytical techniques and devices and make available to industry [Public-Private Partnership - Industry network in conjunction with research institutions and agencies].

5. Review of horizon scanning databases and service providers and publication of a guide that supports industry use of these [Public-Private Partnership - Industry network in conjunction with research institutions and agencies].

6. Adopt a State-led approach to address potential food threats (of terrorist orientation), including mapping trade flows [relevant justice and enforcement institutions and organisations].

7. Provide online guidance and toolkits together with online training suitable for small and medium-size food companies. [Agencies and Industry representative bodies]

8. Establish a research call to evaluate the potential of digital technologies (including Blockchain and AI applications) in supporting food supply chain integrity [Department of Agriculture Food and the Marine (DAFM), Department of Agriculture, Environment and Rural Affairs (DAERA), ***safe***food, Bord Bia, Industry representative bodies].

9. Review of penalties available to enforcement authorities, including confiscation of illegal gains and publication of penalties imposed on perpetrators [DAERA, DAFM, FSA NI, FSAI].

# Foreword and acknowledgements

All food businesses are exposed to threats and vulnerabilities, which arise from actions by individuals or organisations within the supply chain. The impact of such actions ranges from economic and reputational damage to individual companies, and indeed the wider food industry, to illness and death of food product consumers. This report, based on a research project funded by ***safe*food**, examines the related issues of food fraud (which is economically motivated) and food threats (which are maliciously motivated) which result from intentional action by perpetrators who identify and exploit vulnerabilities in the supply chain. The findings inform a set of recommendations of relevance to a range of stakeholders including industry and regulators.

The principal researcher was Dr Seamus O'Reilly, Department of Food Business and Development, Cork University Business School, University College Cork, in association with Prof. Maeve Henchion, Ashtown Research Centre, Teagasc, Postdoc Researcher Dr Alan Sloane, University College Cork (UCC) and Research Officer Hanna Sheerin, Teagasc.

The researchers are most appreciative for the participation of 22 interviewees and a representative from the Northern Ireland Grain Trade Association (NIGTA) who contributed greatly to this research, as they gave their time freely and engaged in an open and forthright manner. We are also grateful for the excellent response to our survey from food industry on the IoI, and we thank in particular the Northern Ireland Food & Drink Association (NIFDA), Elaine Groom at the Agrifood and Biosciences Institute of Northern Ireland (AFBI), and Invest NI for their assistance in promoting response to the survey in Northern Ireland.

We acknowledge also support and assistance given by IT research services at UCC, in particular Sean O'Mahony and Barry O'Sullivan.

The interest and support shown by Dr James McIntosh throughout the project is greatly appreciated, as is the support offered by Gillian Fox and Tracey Thompson at ***safe*food**.

# Table of Contents

# 1 Introduction & background to project

## Introduction

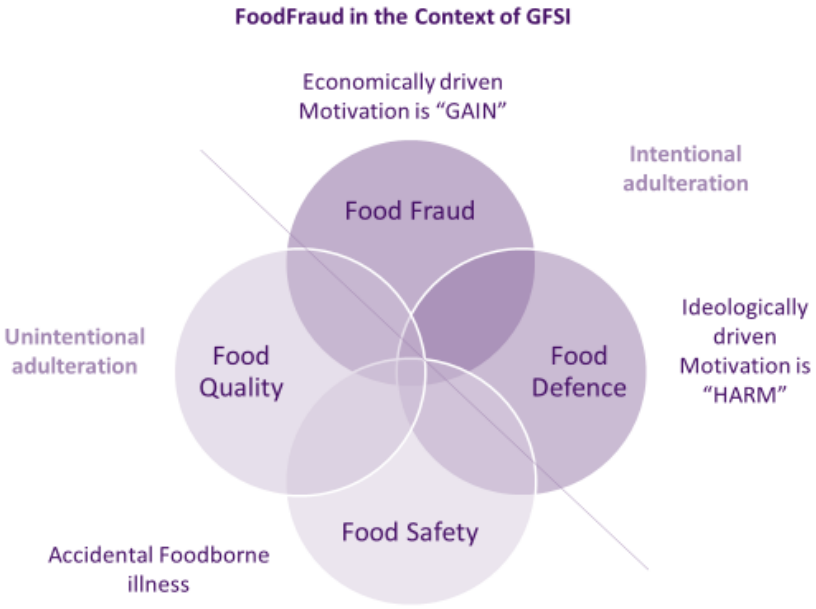
Exports from the Irish agri-food sector (including drink and tobacco) are worth more than €12.5bn on a whole-island basis. Despite its success, however, the sector is exposed to threats and vulnerabilities which, if not prevented or adequately responded to, could result in illness and death as well as economic and reputational damage to food production plants, companies, industries, and national food systems. Although the probability of their occurrence is low, these impacts could be widespread and persistent. Such "black swan" (low probability, but high impact) events are therefore of increasing concern to industry. Furthermore, the fact that supply chain disruptions are increasingly publicly announced and framed as supply chain "failures" in discussion on social media for example, ensures this is an area of interest to industry as well as to regulators and public health agencies.

Increasing globalisation and pressures to reduce costs and improve efficiencies have increased food supply chain complexity. Such complexity is manifest through disaggregation, as evidenced by the development of ingredients industries, and by the dispersal of both suppliers and customers. It results both in new types of supply chain risks and also magnifies their impacts. For example, in the case of (unintentional) dioxin contamination in pork products from Ireland in 2008, products reached 54 countries, and in the 2017 case of Fipronil in eggs in the Netherlands (Askew, 2018), products were traced to 49 countries (including 26 of the 28 current EU member states). These developments have therefore given rise to conditions that increase food firms' vulnerability to adulteration of products through both fraud (for economic gain) and threat (for psychological or ideological reasons) (Moyer et al., 2017; van Ruth et al., 2017). The phenomenon of food fraud and food threats has been an increasing focus of research and policy development as reflected in the UK, for example, in the publication of "the Elliot review" (Elliot, 2014). Protection against food fraud and food threats necessitates policy and processes that extend beyond food safety food quality, which are concerned within unintentional actions that endanger or contaminate the food supply, because food fraud and food threats are the result of intentional action on the part of malevolent or criminal actors.

Because adulteration is the deliberate addition of, or alteration to, an ingredient in a food product for malicious reasons (Moyer et al., 2017), the concept of adulteration implicitly involves the question of the actor's intention and motivations. Fraud and threats are considered to have different motivational drivers: food fraud is carried out for economic gain, and thus is also termed "economically-motivated adulteration" or EMA (Spink et al., 2018), and food threats are made for psychological or ideological reasons, for example revenge by a dissatisfied employee, or politically motivated terrorist activity. While food threats most likely are designed to be directly harmful to consumers, food fraud is often not. But this is not necessarily the case – the use of melamine as a nitrogen-boosting adulterant in milk for baby formula production in China in 2008 (Gossner et al., 2009) originated from economic motives, but resulted in hospitalisations and deaths. In addition to such direct consequences, food fraud results in economic and reputational damage to food production plants, companies, industries, and national food systems, and these can be widespread and persistent.

By contrast, contamination – which is the focus of Food Safety and Food Quality - is accidental and may not involve deliberate actions by any human or organisational actor in the production network or chain (see Figure 1.1). As the conditions leading to Food Fraud and Threat differ from those leading to Food Safety and Food Quality, responses to prevent, deter, detect, or mitigate the effects of these require particular attention.

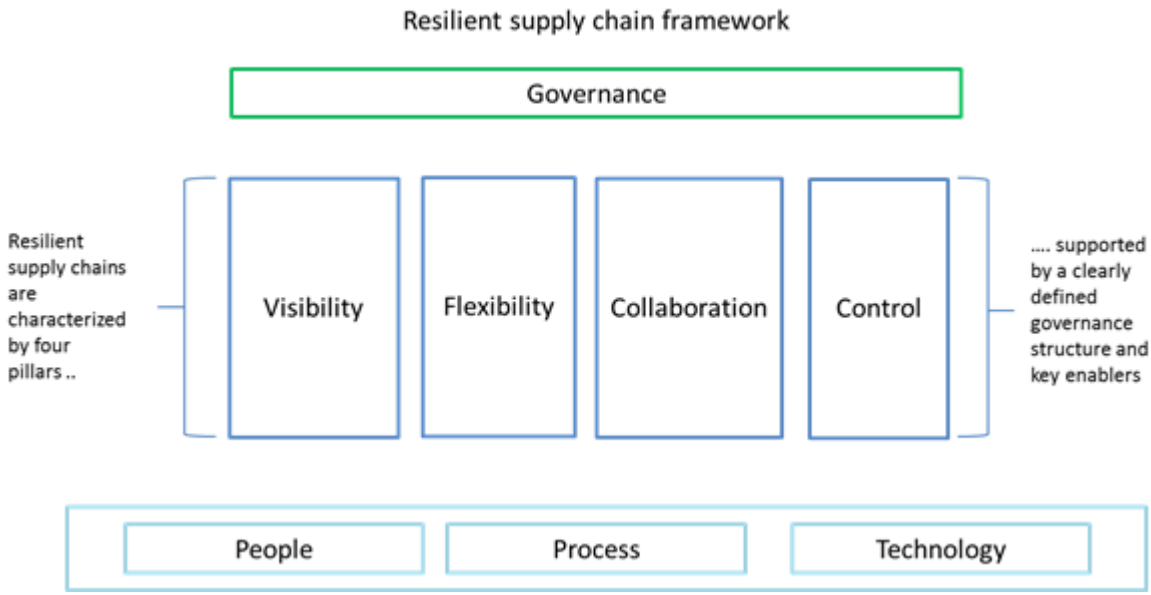
Figure 1.1: Food fraud (adapted from the Global Food Safety Initiative (GFSI), 2014)




By analogy to the successful adoption of hazard identification and control within food safety practice (e.g. Hazard Analysis and Critical Control Points or 'HACCP'), processes to defend against intentional contamination or a threat (e.g. Threat Analysis and Critical Control Points or 'TACCP' (GFSI, 2014)) and dishonest conduct or vulnerability (e.g. Vulnerability Analysis and Critical Control Points or 'VACCP' (Spink, 2014)) have been developed. Furthermore, within the EU and other OECD countries, frameworks have been developed to identify and manage food safety risks and hazards. Within these, some initiatives are designed for rapid alerts (e.g. the Rapid Alert System for Biological and Chemical Attacks and Threats (RAS-BICHAT)), and others to enhance cooperation across jurisdictions to facilitate rapid removal of suspect products from sale (e.g. RASFF) and to improve coordination between actors (e.g. AAC). Such initiatives represent an area of on-going activity, but the approaches, emphases and motivations differ between jurisdictions. For example, the rules adopted by the FDA in the USA emphasise food threats, while EU initiatives are centred more on food fraud. On the other hand, detailed approaches in both jurisdictions focus on training, standardisation of processes, and regulation, together with information sharing. Furthermore, new IT technologies, such as Radio-Frequency identification (RFID) and blockchains offer promise for the development/enhancement of traceability systems.

An overall approach to food integrity increasingly includes the four components of visibility, flexibility, collaboration, and control. These may be viewed as risks of differing natures to Food Integrity (Fassam and Dani, 2017; Kleboth et al., 2016; Manning, 2016a). A supply chain that is designed to preserve integrity is said to be "resilient", capable of preventing many risks to integrity and of responding quickly and effectively to any failures that occur. Figure 1.2 illustrates a framework for analysing resilience in food supply chains (Deloitte, 2013).

**Figure 1.2: Resilient supply chains, adapted from Deloitte (2013)**




It is therefore timely to review practices designed to increase supply chain resilience in response to food fraud and food threat across a variety of countries and to determine the feasibility of incorporating those into agri-food production and supply chains on the IoI based on an understanding of both their originating context and the context in which they will operate. Because such practices are embedded within national and EU-wide supply chain organisation and regulatory environments, and because they reflect differences in cultural contexts, they are unlikely to transpose directly to the IoI. An understanding of the contexts in each jurisdiction therefore needs to be complemented by an understanding of the context within the IoI, to determine the feasibility of adopting new practices and rules here. Such a review can ultimately underpin the development of more resilient supply chains for the agri-food sector.

Based on a systematic review of literature in the field, this study establishes the conditions contributing to the emergence of these challenges, current responses to these threats and the underlying assumptions, principles and processes. The literature review informed subsequent fieldwork, including (i) an industry survey conducted on the IoI, which explores the food industry's awareness and perceived level of exposure to the threat and the actions they are taking to prevent such events, and (ii) in-depth interviews with key stakeholders on the IoI and four selected OECD countries to identify and examine approaches and strategies taken to address such supply chain challenges.

# Background

## Definitions

### Food fraud

Food fraud encompasses a wide variety of intentional actions, motivated in one way or another by the potential for economic gain, or – less frequently perhaps - to avoid economic loss. Thus, most cases of food fraud involve the substitution of a relatively expensive ingredient with a less expensive substitute at some point in the supply chain, and consequent monetary gain for that intermediary supplier. In some cases, an ingredient that is temporarily unavailable or in short supply may be substituted because the processor wishes to satisfy a contract or to maintain an established supply relationship. We may also distinguish between two categories of food fraud, which have been termed "intrinsic" and "extrinsic" (Manning, 2016b), although not all cases can be clearly categorised as one or the other. Intrinsic frauds involve the material substitution of an ingredient – for example "filling" dried oregano herbs with olive or myrtle leaves (Black et al., 2016b). Extrinsic frauds, by contrast, are those that misrepresent "extrinsic" properties of an ingredient, for example claiming an ingredient/product is of organically-certified origin (Megget, 2018), has PGI/PDO certification (Marks and Paravicini, 2017) or is produced in conformance with special rules and conditions, such as being halal when it is not (McElwee et al., 2017). Many extrinsic frauds are also classified as cases of mislabelling – this was the most frequently reported classification in the European Union (EU) Food and Feed Alerts (RASFF) database in 2017 (European Commission, 2018).

Not all cases of fraud are clearly categorizable as either intrinsic or extrinsic. For example, misidentification of fish species, as reported in the recent large-scale FAO report (Reilly, 2018), may be deliberate and thus thought of as intrinsic, but in some cases may be unintentional and more properly considered to be mislabelling, and thus extrinsic. More elaborate extrinsic or mislabelling frauds have also been reported however, for example the fraudulent re-use of bar-codes (Securing Industry, 2018). Thus, EMA (Economically Motivated Adulteration) has emerged as a term to cover not just deliberate adulteration but also misrepresentation of foods for economic gain and so it covers a wide range of fraud activities.

### Food threats (Food Defence)

Food threats – and the response to these, termed "Food Defence"- are cases of adulteration that are motivated by ideological, political, or personal factors. These range from large-scale adulteration for ideological/political reasons – sometimes termed "bio-terrorism" or "agro-terrorism" – to those arising from much more local reasons of personal animus or enmity, most typically actions by a disgruntled employee aimed at damaging the economic or reputational position of their employer. While much attention and research, especially in the USA, has focussed on the first type of food threat (Mitenius et al., 2014), documented incidents of that kind are extremely rare, with the most prominent being the Oregon salad-bar attacks in 1984 which were motivated by political conflicts at the local-government level (Török et al., 1997). By contrast, the second type, arising from personal grievances, has been quite common and widely reported across different industry sectors and geographic regions (Mitenius et al., 2014).

### Comparing fraud and threats

While researchers have made a distinction between "fraud" and "threat", it is clear that in practice such distinctions may be difficult to preserve, since they depend on an assessment of the perpetrator's motives, and thus may not necessarily be objective. Moreover, it is possible that ideological and economic motives might be intermixed – for example in a case where a disaffected employee sought to extort or blackmail a producer for economic gain, but perhaps also motivated by some deeper animosity; or where an ideologically-motivated attacker paid an insider to carry out the

adulteration. As Gregson and Crang (2017) and Lord et al. (2017) point out, “licit” and “Illicit” sub-chains may be found to be intermixed, and likewise ideological and economic motivations may not be easily disentangled or may overlay one another.

Nevertheless, the distinction is useful when developing protocols and methods for responding to such vulnerabilities in the food chain. This is because the greatest risk from ideologically motivated actions - although seemingly also the rarest in occurrence (Dalziel, 2009) - is of adulteration that spreads widely or universally through the food system. The introduction of such adulteration would therefore have to occur in a universal input source, such as water, or in a highly connected node in the food supply chain (e.g. a large retailers’ MDC). Fraud, by contrast, is most likely to occur at a point in the chain where incremental value-add (and economic gain) is highest and the chance of detection is lowest. In addition, the terrorist is not concerned about the duration of their threat, since succeeding once achieves their aim. By contrast, the fraudster hopes to profit from the activity without detection for as long as possible, and several prominent frauds have in fact continued for extended periods of time (Kurtzweil, 1995; Modeland, 1988). Since most protocols for prevention of frauds and threats are based on “thinking like the criminal” and on assessment of the likelihood and location of vulnerabilities in the supply-chain and the production process, the distinction between fraud and threats remains important.

### Conditions – opportunities and motivations

From a motivational perspective food fraud and food threat differ fundamentally from food safety and quality. Most authorities on food fraud/threats, e.g. Spink et al. (2013, 2016, 2017a) in relation to fraud and the WHO (2002) on defence, have argued that these activities differ markedly from the type of issues that are familiar to producers in relation to Food Safety. They argue that in food safety one seeks to control frequently occurring events, that arise from sources such as contamination or processing errors, and that therefore the focus of controls is on identifying the most important (or critical) risks and then initiating responses that reduce the likelihood and consequences of those risks. HACCP (Hazard Analysis and Critical Control Points) is the primary example of such an approach. Risks and likelihoods of this kind are identifiable, enumerable, and quantifiable because they are internal to the processing unit and, being frequently occurring, are amenable to data collection on their context, causes and overall likelihood. By contrast, fraud/threat vulnerabilities may have never occurred before, may never occur again, or may represent a potential opportunity that never leads to an actual event. It is such vulnerabilities – “weakness[es] or flaw[s] that create[s] opportunities for undesirable events” (Spink et al., 2017a, p.216) – that matter when developing countermeasures against fraud or threats, and these vulnerabilities can be assessed only qualitatively in terms of likelihood and consequences, i.e. “the susceptibility of the system” (Spink et al., 2017a, p.216). Some aspects of a vulnerability assessment may of course be aided by quantitative data sources (e.g. commodity price movements) and it is generally recommended that these are incorporated in response strategies (FSA and the National Sanitation Foundation (NSF), 2015).

Spink et al. (2017a, p.216) further argued that the management of fraud (and, by extension, of threats) “necessitates a shift of the focus of countermeasures and control systems from intervention and response [i.e. mitigation] to prevention”. Here, they define (from International Standard Organisation (ISO) standards) “mitigation” as “countermeasures … to reduce the consequence of the event”, where those events arise from “risks that cannot be eliminated” (Spink et al., 2017a, p.217). They define countermeasures as measures “intended to reduce or eliminate the likelihood of the event occurring”, and thus prevention “focuses on identifying and eliminating or reducing vulnerability”. In summary, therefore, the argument is that countermeasures against these risks should be based on prevention of the causes of such events, i.e. by assessing vulnerabilities; whereas countermeasures in the field of Food Safety may be based on mitigating the consequences of risks to safety of the product, by assessing risks especially at critical points in the production process (Spink et al., 2017a, p.217).

## Response strategies

Given this motivation, response strategies focus attention on the conditions that lead to fraud/threats, with assessment tools designed to address motivations and opportunities to commit such offenses on the one hand and the control measures in place on the other hand (Manning and Soon, 2016; van Ruth et al., 2017). Thus, in very broad terms, these responses can be described as strategies based on:

- Deterrence;
- Detection;
- Control Measures.

Of course, all of these operate in conjunction with one another, so that, for example, improvements in measures for detection increase the deterrent effect, since there is an increased likelihood that the fraudster will be discovered. Alternatively, countermeasures may be based on information gleaned from previously detected incidents. Increasing legal penalties (Elliott, 2015; Pagnattaro and Peirce, 2010; Roberts, 2011) may improve deterrence even without improvements in the rate of detection, since the consequences for the fraudster, when detected, are now greater.

These strategies seek to shift the balance from low risk of detection and good opportunity to profit illegally to high risk of detection and strongly negative consequences of such for the perpetrator. The food fraudster's attention is focused on market signals such as price-spikes or increasing demand for a commodity and the potential opportunity to act which is dependent on issues such as the complexity of the supply chain or the availability of technology and knowledge to adulterate. Thus, they seek to identify areas where the chances of detection and/or consequences if detected are low.

## Deterrence

Jack (2018) observed that food fraud is an economic crime, requires "comprehensive pre-planning", and is likely to be based on "a rational cost-benefit analysis", so that Becker's (1968) rational choice theory on deterrence is "very likely" to apply:

> "... when potential offenders conclude that the expected penalty associated with being caught committing a crime outweighs the monetary gain they will receive through committing that crime" (Jack, 2018, p.152).

This contrasts with the observation that much crime is committed on impulse and is therefore influenced by the immediate ease of opportunity. Note also that food threats from the terrorist or ideological activist are not so strongly constrained by rational calculation (although they are unlikely to be impulsive), and so may not be so well controlled by strategies based on deterrence. Nevertheless, the regulation adopted by the EU (European Parliament, 2017) in the aftermath of the "horse-meat" fraud reflects this perspective by specifying that the penalties should "at least offset the economic advantage that those criminals had sought to gain" (Jack, 2018).

In this regard, note that deterrence as a strategy to control fraud and threat relies primarily on the state, by relying on it for "enforcing policies and regulations" (A. T. Kearney and GMA, 2010, p. 19). What van der Meulen (2011a, p.30) calls "private laws" can act as secondary deterrents by requiring participants in the supply chain to meet standards, and by withholding or withdrawing certification (see below), impose economic and reputational penalties on firms that do not meet the criteria of the standard:

> "In case the audit shows non-compliance, no certification is provided and/or the right to use the mark representing the certification is withdrawn. By consequence the company can no longer do business with customers that demand certification" (van der Meulen, 2011b, p.80)

## Detection: analytical protocols

Although food fraud and food threats have a long history, their detection is relatively new (Ellis et al., 2015). While, the first line of defence against food adulteration is full transparency within the supply chain and assessment of the likelihood of penetration at any point by opportunistic perpetrators, in the case of a more vulnerable supply chain, where raw materials are purchased through traders and other sources, a higher degree of sampling, testing and surveillance is necessary. In such circumstances access to carefully selected, continuously developing and appropriate techniques to analyse and verify the absence or presence of any potential adulterants is vital (Stadler et al., 2016). Because the perpetrators of food adulteration employ methods of misrepresentation that are increasingly difficult to detect, the use of highly sophisticated and ever-evolving analytical techniques is essential in order to definitively authenticate food and thus prevent incidences of food adulteration (Black et al., 2016a). It is clear that those associated with the food industry are seeking rapid, user-friendly methods to detect food adulteration in order to gain assurance in their compliance to both branding and labelling (Danezis et al., 2016). In order to be practicable, these methods must move from laboratories to food supply chains by being both robust and reproducible and provide reliable results at vulnerable points in the supply chain daily while being handheld or remote sensor devices to allow operation at-line or in-line (Ellis et al., 2015; Ellis and Goodacre, 2016). There has been a lot of research carried out in this area to pinpoint the most advantageous testing methods.

Several studies have indicated that the current 'targeted' testing methods utilised by the food supply chain can be blind to foreign and novel adulterants similar to those that could be used to adulterate food produce. These studies suggest that current food testing (targeted) needs to be combined with non-specific methods (untargeted), preferably with in-line or at-line detection capabilities to increase consumer protection (Ordoudi et al., 2017; Pedersen et al., 2016). López et al., 2014) explain that a combination of both methods is most effective, as untargeted sampling is best for detecting an unknown adulterant, while targeted sampling when used for a known substance gives more information about that specific adulterant.

According to Danezis (2016), chromatographic and molecular methods are the two main approaches taken to food authentication solutions; where chromatographic, molecular, vibrational and fluorescence spectroscopy techniques have increased in popularity for their use in food authentication, as evidenced by the time-series charted in Figure 1.3.

Figure 1.3: Temporal evolution per technique (Danezis et al., 2016, p. 7)

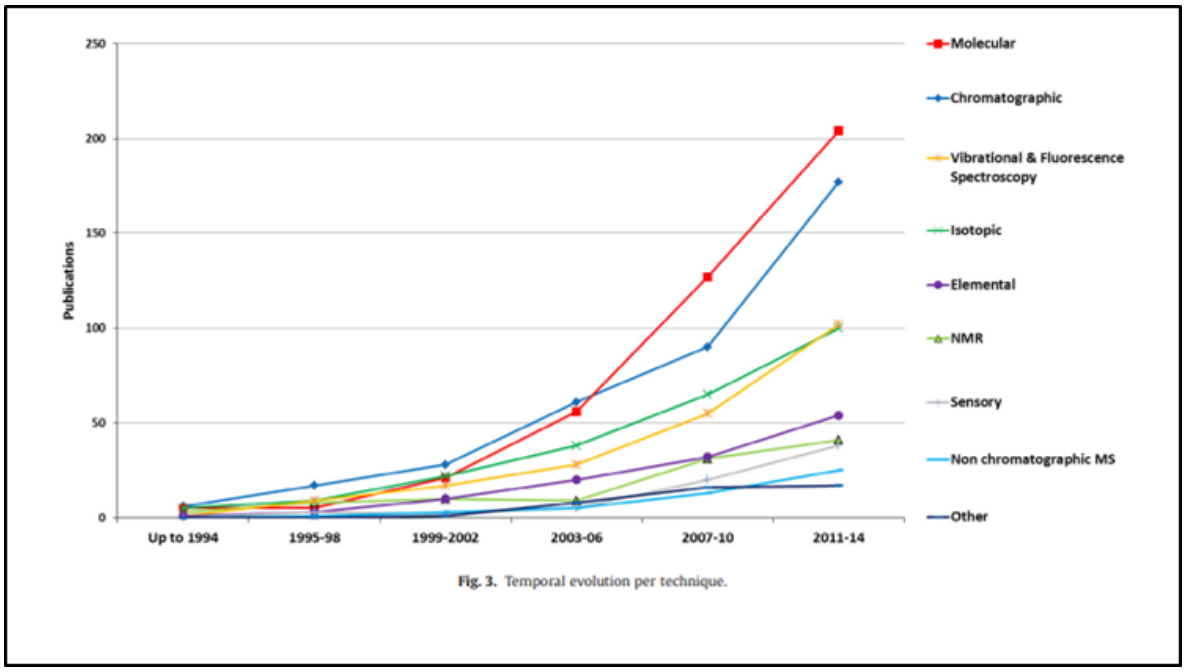



Fig. 3. Temporal evolution per technique.

With regard to meat products, there is no perfect analytical tool capable of providing an answer for all the possible problems that can be encountered at one time (Sentandreu and Sentandreu, 2014). There have been significant developments in DNA typing (Corrado, 2016; FSAI, 2019) and, similar to many other fields of food science, mass spectrometry (MS) has become a frontline technology replacing other methods in food authentication testing (Georgiou and Danezis, 2015). MS (considered to be the gold standard within many industries) is advantageous as a method because it has high sensitivity, selectivity, throughput and multi-analytical capabilities (providing more descriptors and thus facilitating better classification within food adulteration) (Callao and Ruisánchez, 2018; Georgiou and Danezis, 2015). MS is usually coupled with chromatographic techniques because the chromatography column chemistry, when chosen both appropriately and carefully, separates out the complex components of food adequately. However, the disadvantage of MS has been that this analysis is generally expensive and time-consuming to carry out. As a result, there has been significant progress made towards the development of portable 'point-and-shoot' technologies using MS so that utilising MS is becoming a more viable option in the food industry (Stadler et al., 2016). Developments in the miniaturisation of MS (e.g. handheld or portable devices) continue to evolve and are advantageous as they can be used both at-line, in-line or out at different points in the food supply chain (Ellis et al., 2015; Karunathilaka et al., 2018).

While there has been a great deal of research into the development of new analytical techniques to authenticate food, because the perpetrators involved in food adulteration are continually developing ways to outwit accepted techniques for food authentication, this research must continue to innovate ever-evolving techniques, and increase sophistication in identifying chemical markers (Wielogorska et al., 2018), data acquisition and modelling while also establishing standardised global reference methods and databases that contain comprehensive information about foods and production methods (Danezis et al., 2016; Reid et al., 2006; Stadler et al., 2016). In addition to this continued research, it is important to note that any technique that is found to be effective must also be challenged at industry level to ensure that it includes appropriate sensitivity and specificity parameters and that it is practicable at industry level in terms of both usage cost and efficiency with a minimum risk of failure (Hong et al., 2017; Reid et al., 2006; Stadler et al., 2016).

### Control measures

Spink et al. (2016) consider control or counter-measures within an overall context of detection, deterrence and prevention. Detection measures, in addition to the analytical protocols described above, include assessment of food supply chain vulnerabilities to identify fraud opportunities and mapping trade points to focus surveillance activity. Deterrence measures seek to both reduce the opportunity and ensure penalties are dissuasive. While preventative measures attempt to disrupt the perpetrators, such measures are of particular importance where prosecution is unlikely. Hence, Spink et al. argue that active vulnerability assessment mapping acts as a counter-measure in itself as it is evident to potential perpetrators and as such also acts as a deterrent.

Thus, in combating perpetrators these strategies seek to enhance horizon scanning to detect candidate products/ingredients and to simultaneously improve visibility and information sharing. Such strategies can work with food threat as well as food fraud as terrorists are attracted to opportunities to act where they will have maximum impact. While they may be less concerned with detection after the event, they are still likely to be concerned about surveillance while planning.

All of the standards, processes and methods that have been developed and that will be detailed below, are consequently based on a general "prevention and vulnerability reduction approach" (van Ruth at al., 2017). The following sections will describe the structure of the various approaches to vulnerability reduction in terms of the framework presented in Figure 1.4 below. This framework draws on the analyses of van der Meulen (Corini and van der Meulen, 2018; van der Meulen, 2011a) and Appelhof & van den Heuvel (2011), and in particular on van der Meulen's (2011a, p.30) concepts of "public law" and "private law". In this categorisation, laws, rules, and regulations relating to food that are enacted and enforced by states or inter-state bodies are considered "public". "Private food laws" are then:

> "*... the elaborate structures of rules known as, self-regulation, private (voluntary) standards, codes of conduct, or certification schemes. These structures have been created by private actors using private law instruments to regulate conduct of food businesses*" (Van der Meulen 2011a, p.30)

In Van der Meulen's categorisation these laws, rules, and regulations are organised into hierarchies, with public above private, and with further hierarchies within those categories, for example international/regional/national within public laws (van der Meulen 2011a, p.33), as shown in Figure 1.4 and Figure 1.5.

**Figure 1.4: The pyramid of food law (from Van der Meulen, 2011a, p.33)**

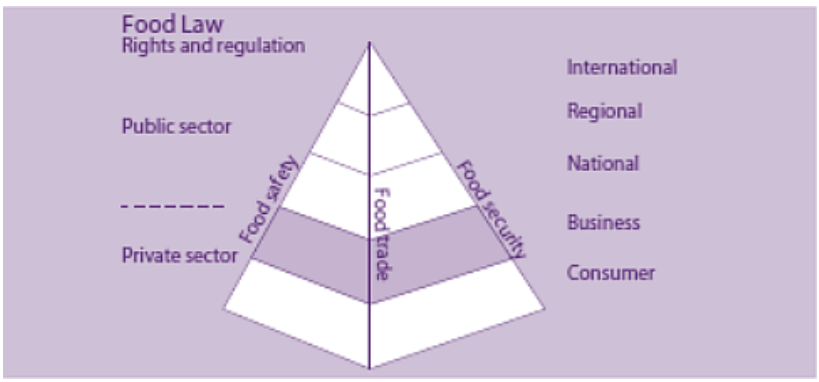
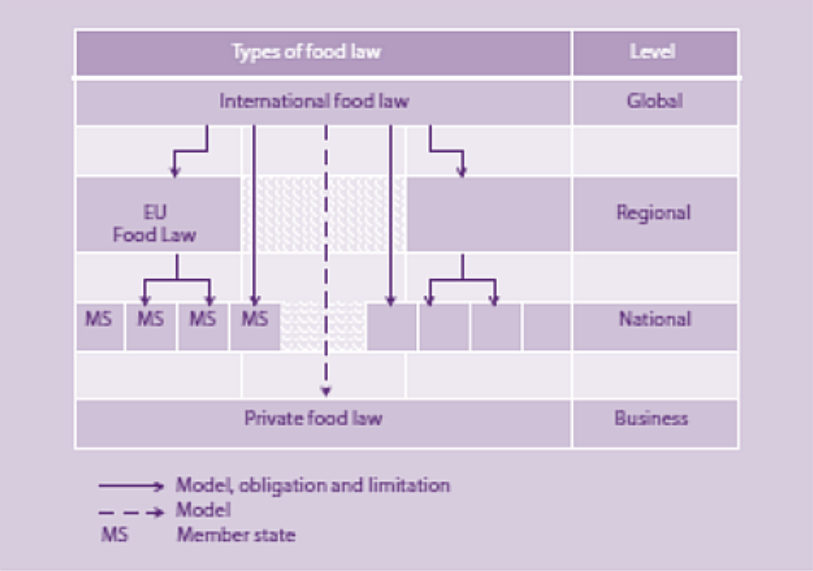


**Figure 1.5: Multi-layered food law (from Van der Meulen, 2011a, p.35)**




Spink et al. (2016, p. 71) have argued that the development and application of these laws as they relate to fraud should be through what they term "public-private partnerships", i.e. collaboration between government and business interests. A principal reason for this is that no one business has a complete view of, or control over, the supply-chain and what they term its "exchange points"

> "Governments have the most control of the food supply chain at border crossings and in regulating the point of consumer purchase. Industry has the most control at the ownership exchange when receiving materials and at the sale to consumers. For these reasons, Food Fraud prevention is most efficiently achieved for the country, market, and world at these exchange points through a public–private-partnership." (Spink et al., 2016, p. 71)

Van der Meulen (2011b, p.85-86) similarly described the existence of what he termed "public-private interconnections" in which there was complex inter-dependencies not only among various systems of private food law, but also between private and public food law:

> "Private schemes are not only interconnected among themselves, but also with public law. The vast majority of private certification schemes refer to public law requirements that have to be complied with. Less common but also existing is the inverse where public law provisions require compliance with private schemes".

Private food law itself is a complex structure with many inter-dependencies, and is policed and enforced by a variety of mechanisms, in particular through audits:

> "Private food law revolves around private standards holding requirements with which businesses must comply to achieve directly or indirectly certain product characteristics as defined in the standard. ... The standards are embedded in structures ... that ensure their development and fulfilment such as audits and third-party certification". (van der Meulen 2011a, p.37)

Enforcement of private food laws and penalties for violation of them rest in two distinct mechanisms. First, conformance to standards may be written into supplier-buyer contracts so that non-conformance by the supplier can result in recourse to (civil) contract law, and the imposition of financial penalties, enforced once again by the state. As van der Meulen (2011b, p. 79) describes: "In case of noncompliance liability for damages arises, contractual relations may be ended, and all kinds

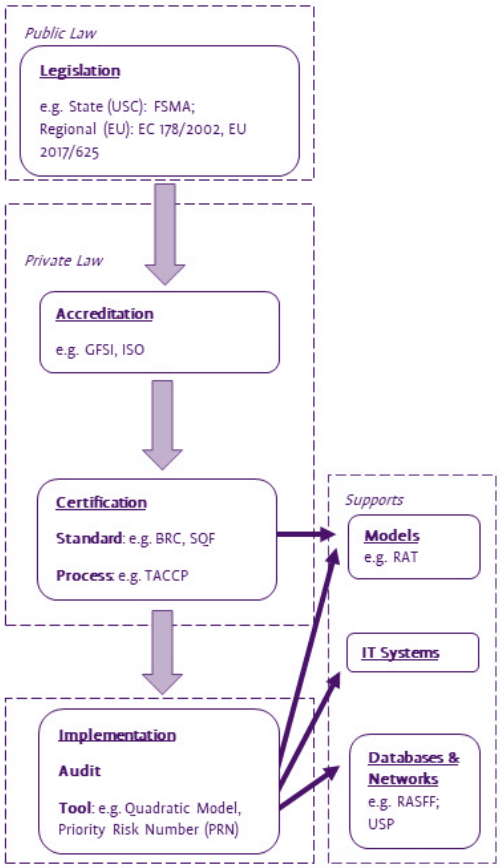
of consequences may arise that have been agreed upon in the contract (like contractual fines)". Beyond such financial penalties, publicity about the proceedings, is likely to result in reputational damage to the supplier both with potential customers, and with the certification authority. The second mechanism, rests similarly in reputational costs, because non-conformance to the standard, if detected through audit (or as above), can result in suspension or withdrawal of certification:

> "In case the audit shows non-compliance, no certification is provided and/or the right to use the mark representing the certification is withdrawn. By consequence the company can no longer do business with customers that demand certification" (van der Meulen, 2011b, p. 80)

Since certification is a requirement for doing business in many contracts the non-conformant business is effectively excluded from such business relationships and may be forced to accept lower prices or more disadvantageous conditions. Moreover, as van der Meulen (2011b, p.78) argues "the impact of the private scheme can go beyond the immediate contractual relation" because "by demanding that in [one] relation a certain standard applies, a purchaser can exercise considerable influence on contractual relations upstream". Thus, large businesses, for example the large multi-national food processors or retail chains that are the sponsors or members of the GMA or GFSI, can, by specifying conformance to their standards, exert an influence that extends far beyond their immediate supply contracts. Private laws thus become "instrument[s] for what is called 'chain orchestration'" (van der Meulen 2011b, p.78), because the requirement of conformance to the standard is propagated onwards through the tiers and the network of suppliers and sub-suppliers. A non-conformant business consequently is positioned outside of, and excluded from doing business with, the whole group of conformant businesses.

In Figure 1.6 below we suggest a detailed framework that incorporates van der Meulen's concepts of Public and Private law, and develops it by adding further detail on the processes and methods that food business operators and auditors can use in practice to identify and resolve fraud- or threat-related vulnerabilities in their production systems.

**Figure 1.6: Legislation, accreditation, certification, and implementation**




The lower layers of the diagram – Implementation and Certification – are influenced by the context of the upper layers – Accreditation and Legislation. As mentioned earlier of course, the direction of control is not only downwards through the layers, but also upwards because knowledge and practice from the lower layers influences the rules and regulations that are codified in the upper layers. Probably the most notable example of such upward influence was the inclusion of HACCP, a process at the Certification layer, in the original European food safety legislation, Regulation (EC) 178/2002 (European Parliament, 2002).

## Legislation

Although other states and regions are developing law in relation to fraud and threat (Mol, 2014; Walker, 2017; Zhang and Xue, 2016), the scope of this study is confined to the EU and the USA. In the USA, the overarching piece of law concerning fraud and threat is the Food Safety Modernization Act (FSMA), signed into law in 2011. This is considered to be the most significant reform of food law in the USA since 1938 (Layton, 2009). In particular, in its provisions on "Preventive Controls", it addresses "preventing intentional adulteration from acts intended to cause wide-scale harm to public health, including acts of terrorism targeting the food supply". While the main focus of the law is on food threats, it now incorporates requirements for similar preventive strategies against economically-motivated adulteration (food fraud). Specifically, it requires vulnerability assessments against food fraud: events that could lead to a "hazard that requires a preventive control" from an act that is "economically motivated" (Spink and Moyer, 2017b, p.58).

In the EU the central law is Regulation (EU) 2017/625, which updates the earlier Regulation (EC) 178/2002. The 2002 regulation established the European Food Safety Authority (EFSA) and placed the HACCP process at the centre of food safety practice. The 2017 regulation, developed in the wake of the horse meat fraud (Elliott, 2014) added provisions against what it termed "fraudulent or deceptive practices along the agri-food chain" and requires the relevant national authorities to take account of "potential risks and the likelihood" of such events occurring. In addition, it encourages the development of cross-national information sharing, which has subsequently been implemented through mechanisms such as RASFF and European Food Fraud Network (EFFN).

In the US, enforcement of the FSMA legislation is a federal responsibility, and is delegated primarily to the FDA, with a role also for the DHS. In the EU, implementation is delegated to national governments, and enforcement to national (or devolved) regulatory bodies, for example in Ireland to the FSAI, or in Northern Ireland to the FSA in NI. In addition, EU-wide actions may be taken, such as Europol's "Project OPSON" which targets food fraud (Varallo, 2018).

### Accreditation and certification

In response to this and other commercial drivers a range of industry standards have been developed or adapted (given the limitations of established food quality assurance process (e.g. HACCP) to equip food supply chain actors to respond to these challenges). Such standards specify processes and tests that food business operators and auditors can use in practice to identify and resolve fraud or threat-related vulnerabilities in their supply chains. Over the past two decades private organisations (e.g. British Retail Consortium (BRC), Safe Quality Food (SQF) Program) have developed internationally accepted quality assurance standards. These standards, which usually seek accreditation from established global bodies (e.g. ISO, GFSI), require certified food supply chain actors to employ various processes and methods which in turn are audited. In recent years the processes required (e.g. HACCP) have been adapted to include measures that respond to food fraud and food threats. While these measures in turn differ somewhat, they all include a vulnerability assessment tool that assesses level of opportunity and motivation and adequacy of control measures. These tools are largely based on self-assessment with links to databases (e.g. commodity prices, fraud/threat incidents on systems such as Decernis (formerly US Pharmacopeial Convention (USP) and RASFF) to support horizon scanning. Figure 1.6 illustrates the role and relationship between accreditation (e.g. GFSI) and certification (e.g. BRC) within the overall international and national legal context.

In response to the proliferation of schemes at the Certification (Standards) level in relation to food safety, and the consequent burden of regulation and auditing on businesses (Kleboth et al., 2016), efforts were initiated by industry actors to create more encompassing schemes, that would accredit the various "Standards" developed and promoted by the Certification bodies. Most prominent among these initiatives is the GFSI, established in 2000, under the auspices of the Consumer Goods Forum (CGF, then the International Committee of Food Chains (CIES)), a group comprised of major international food manufacturers and retailers. One of this initiative's major goals was to reduce redundancy of audits, so that a producer could be "certified once, accepted everywhere" (Appelhof & van den Heuvel, 2011, p.116). A second accreditation body is the ISO, which developed a food safety standard ISO 22000, supported by the multi-national food producers, i.e. the "big brand holders" (Appelhof & van den Heuvel, 2011, p.132). However, the retailers were slow to accept and adopt ISO 22000, and so a new organisation was established, the Foundation for Food Safety Certification and this organisation developed a broader standard, Food Safety System Certification (FSSC) 22000, issued first in 2009. FSSC 22000 is among the standards accepted by GFSI which has consequently emerged as the dominant accreditation body. In fact, Van der Meulen (2011b, p.103) states that "GFSI is developing into the standard of standards". GFSI "benchmarks" certification schemes and endorses those which meet its "benchmarking requirements", or "key elements" (van der Meulen 2011b, p103). These standards, classified as 'private law' by van der Meulen (2011a), are based on a general "prevention and vulnerability reduction approach" (van Ruth et al., 2017:70) with a vulnerability assessment tool fundamental to their operation.

In Appendix 1 we provide detailed descriptions of the origin and development of the two accreditation bodies/schemes (GFSI and ISO), of the most prominent non-specialised certification bodies/schemes (IFS, BRC, SQF, FSSC, and Primus), of other influential bodies/schemes (SSAFE, PAS-96, USP), and also of several protocols specifically designed for Food Defence applications (ALERT, ORM, CARVER+Shock, FASCAT). Two certifications emerged as most important in the survey responses however, so we give short summaries of them here: BRC and FSSC.

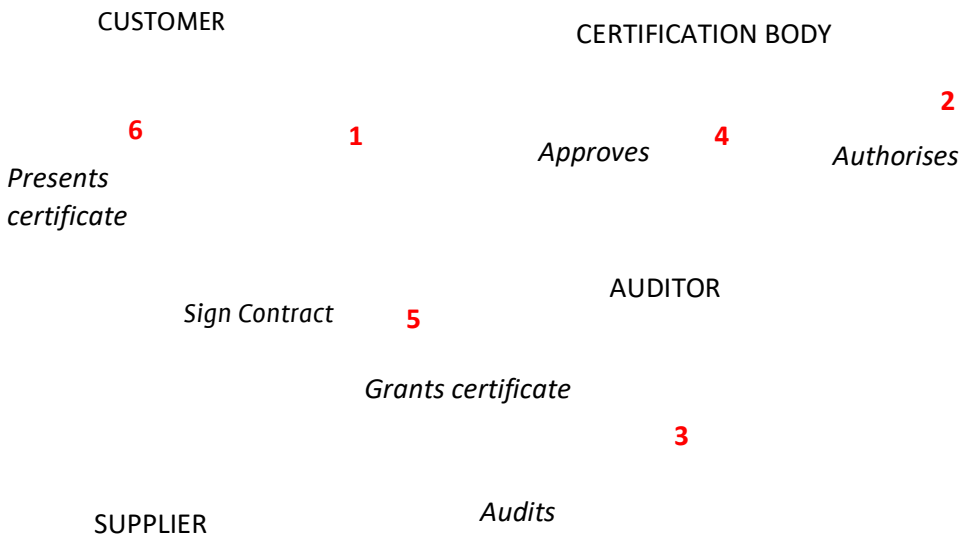
The British Retail Consortium (BRC) was one of the earliest to include requirements relating to food fraud or food defence (pre-dating the inclusion of general requirements in GFSI's benchmarking requirements). The 7th Edition was issued in January 2015, and strengthened requirements in relation to food fraud, in response in particular to the discovery of horsemeat in the beef supply chain in Europe, and that of melanin in milk-powder in China. These requirements are detailed in Section 5.4 of this edition, "Product Authenticity, Claims and Chain of custody". Version 8 (published August 2018), which has now superseded the earlier version, has considered the implications of FSMA and hence food defence with a requirement that the threat assessment includes internal and external threats.

FSSC 22000 was fully recognised by GFSI in 2010. Version 4.1 of the scheme was issued in mid-2017. In relation to food fraud and food defence, just as with BRC, FSSC 22000 requires a vulnerability assessment, the identification of control measures, and the documentation of both of those in a prevention plan.

### Implementation: audit & tools

Where a supplier-customer contract specifies that the supplier will meet a certain standard, such as BRC-7, rather than the customer directly verifying that the conditions of the standard are being met, it is usual that an independent "auditor" verifies compliance, and that the standards body issues a certificate of compliance to the supplier. The certificate can be presented by the supplier to other customers who require the same standard and is taken as evidence of compliance to such contractually agreed standards. This arrangement is called "third-party auditing" (van der Meulen, 2011b, p. 80). The auditor is an organisation or individual who is independent of both customer and supplier. The auditor is also normally independent of the certification body but has been approved by it as a qualified auditor for their standard. Thus, the relationships between the four organisations are somewhat complex, as illustrated in Figure 1.7 but the structure clearly separates responsibilities and has advantages for both customer and supplier in cases where they have multiple supply-chain relationships, and also because they do not themselves have to develop auditing capabilities.

**Figure 1.7: Third-party auditing**




A major focus of the work of the person or team responsible for food safety or quality within the supplier organisation is then on preparing for and responding to visits from the auditor. In relation to food fraud or food threats, this work is oriented around the development and operation of processes that aim to assess, prevent, or mitigate the effects of vulnerabilities and the documentation of these processes and actions in the form of Vulnerability Assessment plans. While the details of these documents differ from one certification scheme to another, three specific ways of assessing, quantifying, and presenting identified vulnerabilities can be distinguished:

1. Quadratic Models, or Vulnerability Assessment Matrices
2. Priority Risk Numbers (PRN's)
3. Radar Charts, or Spider-web diagrams[1].

Although the details of different certification schemes differ, the concepts involved are generally similar. In some certification schemes these may be quite informally described (e.g. BRC 7), while in others specific forms (e.g. USP) or even software packages have been provided that codify the process of assessment, guide the supplier through it, and present the results in a standardised form (PricewaterhouseCoopers, 2016).

## Conclusions

Some key themes arise from this review: susceptibility, the role of law and standards, and information flow. Food system susceptibility arises due to weakness/gaps that are identified and exploited by perpetrators intent on fraud/threat. Hence response to fraud/threat focusses on weakness or gaps

[1] Computer Scientists favour calling this type of chart a "Kiviat Graph" (Kolence, 1973).

within the system, with an emphasis on prevention rather than mitigation (in contrast to food safety or quality issues). The role of information flow is crucial to response strategies with a fundamental need for collaboration among food system stakeholders, public and private, at various levels. Database development has been facilitated by both public agencies (e.g. EFFN in the EU) and commercial concerns such as Decernis based in the US and FERA (horizon scanning) in the UK. An increased and ongoing effort to develop rapid testing methods (Ellis et al., 2015) has greatly enhanced surveillance of fraud/threat. However, the capacity and willingness of food supply chain actors to use (and contribute to) databases, and to embed fraud/threat defences into their management processes has not been established.

# 2 Project aims, objectives and method

## Aim

The overall aim of this project was to investigate the potential for augmenting the resilience of agri-food supply chains on the IoI, with specific reference to the intentional adulteration of food products. Supply chain transparency and capability to address disruption are essential to long term competitiveness of the agri-food industry. Hence this study sought to establish current levels of awareness and practice on the IoI, identify and assess a range of VMIs in four selected OECD countries and propose a VMF that would benefit the agri-food supply chains on the IoI.

## Objectives

Specifically, the study objectives are as follows:

1. Identify and assess key vulnerabilities in the food chain on the IoI and develop an online survey instrument to capture the perceptions of the food industry with regard to existing and potential vulnerabilities.
2. Describe current VMIs on the IoI and determine rationale behind design of same including key motivating factors (e.g. fraud vs terrorist attack).
3. Identify and evaluate VMIs undertaken in four other OECD countries (the UK, the USA, the Netherlands and Denmark).
4. Determine potential for transferability of practices and processes from VMIs from these other OECD countries to the IoI including the identification of benefits and risks in transposing such approaches to the IoI, develop a framework for assessment based on literature, and apply the framework and test its feasibility and potential benefits in workshop (2) format with stakeholders.

## Method

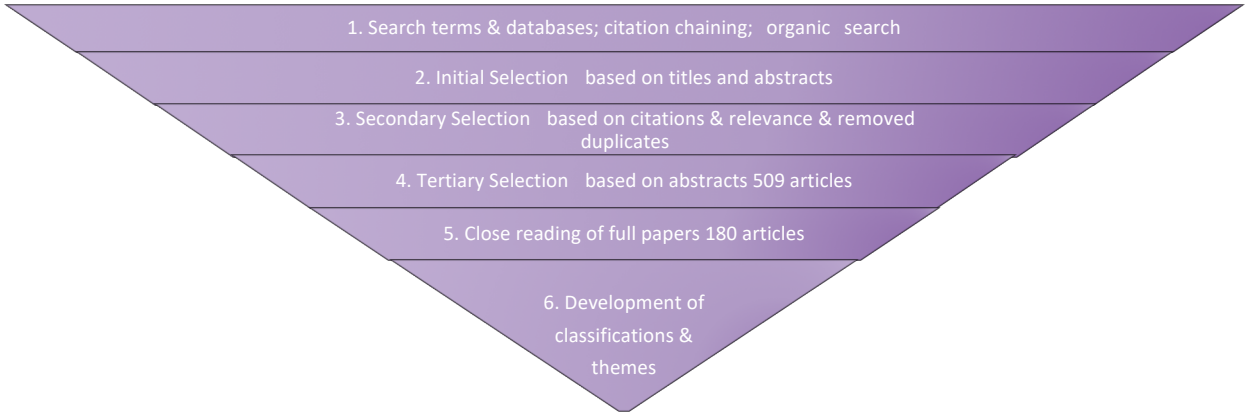
The study consisted of three work streams:

1. a literature review to establish emerging definitions and measures,
2. semi-structured qualitative interviews with stakeholders and experts,
3. an online quantitative survey of food manufacturers in the IoI.

### Systematic review of literature

A systematic review of literature, following the general approach of Briner and Denyer (2012), was conducted to establish the conditions that contribute to the emergence of economically and ideologically motivated adulteration of food, responses to these vulnerabilities and the underlying assumptions, principles and processes. The steps followed are illustrated in Figure 2.1, with search terms, databases searched and number of articles identified initially reported in Table 2.1.

**Figure 2.1: Search & Selection Process**




The search terms were chosen based on initial scanning of the literature and also because they were "statistically unlikely phrases". As this is an emerging area of interest, the "grey" literature was deemed important (Adams et al., 2017). Additional articles were collected through what could be termed "organic search", for example those recommended by experts and colleagues, publicised on social media (Twitter) by a selection of food authorities, and finally by searching the web-sites of organisations known to be actively working on the topic. Articles in the initial selection were screened for relevance, e.g. excluding articles that focused on the details or refinement of analytical techniques. Secondary selection involved first merging references and removing duplicates. The next step involved retaining only those articles with non-zero citation counts, based on Google Scholar data. Finally, the uncited articles were reviewed for quality and those which the authors judged to be authoritative (e.g. published by a competent authority or noted author), topical, or otherwise novel were retained. At the end of this stage 509 items were retained, categorised as follows: 304 cited articles; 118 uncited but relevant; 87 'organic' (incl. grey literature, e.g. industry representative bodies, policy, etc.).

Table 2.1: Search terms & statistics for database searches

| Search Terms | Databases | | | | |
|---|---|---|---|---|---|
| | Science Direct | Scopus | Web of Science | EBSCO | AgEcon Search |
| food AND fraud | 8577 | 6442 | 8542 | 4729 | 18 |
| "food fraud" | 347 | 594 | 179 | 431 | 0 |
| "food defense" | 173 | 352 | 79 | 140 | 8 |
| "food defence" | 42 | | 15 | 11 | 1 |
| "food threat" | 19 | 27 | 4 | 22 | 0 |
| "economically motivated adulteration" | 117 | 377 | 64 | 52 | 0 |
| "supply chain resilience" AND food | 45 | 208 | 8 | 8 | 0 |
| "supply chain vulnerability" AND food | 41 | 177 | 5 | 8 | 0 |
| "vulnerability resolution initiative" | 0 | 0 | 0 | 0 | 0 |
| TOTAL | 784 | 1735 | 354 | 672 | 9 |

Tertiary selection was based on relevance (e.g. consumer studies, and papers on methods for predictive modelling were excluded), timeliness (historic/archival articles), appropriateness (e.g. supply chain risk management excluded), and quality (e.g. short commentaries excluded). These were then divided out among the research team for close reading. The final (close-reading) stage addressed the following areas: (i) review of definitions, (ii) identification of conditions that can give rise to adulteration and (iii) responses pursued and challenges faced. The findings from this provided the initial framing for the study (as presented in the background section above), informed the design of an online survey questionnaire and semi-structured interview guides, and supported the interpretation of empirical findings.

### Survey of food manufacturers on the island of Ireland

A structured questionnaire, developed for an online survey of food manufacturers (ingredient, intermediate and consumer product) on the IoI, was designed to assess awareness of the level of vulnerabilities associated with intentional adulteration (including misrepresentation) of food ingredients and products, and capture their experience of incidents of adulteration, including strategies and actions adopted to prevent/respond to these. The online survey was hosted on the Qualtrics research platform. A total of 176 valid responses were received, from a sample frame of 1,000 firms (750 in the RoI, and 250 in NI), an overall response rate over 17%. The sample frame was based on a database owned by Teagasc, supplemented by additional searches of company websites and personal communications with experts in the area. In addition, in Northern Ireland, personalised emails from relevant agencies to their membership were used to stimulate responses. Details of the questionnaire along with the survey method and demographics of the respondents are given in Appendices 1, 2 and 3 respectively. Data from the survey was analysed using the SPSS software package (Version 24) using standard exploratory and confirmatory statistical methods as appropriate to the data and the research questions.

### Semi-structured interviews of stakeholders

Semi-structured interviews were carried out with 22 stakeholders on the IoI and in the UK, the Netherlands, the USA and Denmark (the four selected OECD countries). The semi-structured interview schedule used for these interviews is presented in Appendix 5. Given industry experience of incidents is a "first hand" experience for industry compared to other stakeholders, an adapted guide was used for industry respondents. The guide was designed to elicit perspectives on definitions and prevalence of adulteration, characteristics of perpetrators and current practices and responses to incidents based on concrete real-life narratives. Selection of respondents ensured representatives from the regulators (food crime units where relevant), industry representative bodies, policy-makers and experts (such as academic, researchers, consultants) were included. In addition, one interview was held with an expert who provided an EU level perspective. A list of all organisations interviewed is presented in Appendix 6. All interviews were recorded (with the permission of the interviewee). The interviews were carried out over the phone or Skype with four exceptions where the participants were met in person. Interviews lasted about 50 minutes on average.

Data analysis was supported by the NVivo™ version 10 computer software package. A thematic approach to analysis was followed. Initial category themes were checked by a second coder who coded a sample of four interview transcripts to establish consistency of application of codes and appropriateness of codes applied to data (Zanoli & Naspetti, 2002, Jung & Kang, 2010; Bieberstein & Roosen, 2015). Cohen's Kappa coefficient for inter-coder reliability was 0.7814, which indicates a good degree of inter-coder reliability. Analysis was carried out at country/regional level at first as this supported subsequent cross-country comparison. The qualitative findings arising from the IoI respondents were integrated with the quantitative analysis of the IoI industry survey to provide a more holistic perspective (addressing objectives 1 and 2). Analysis of qualitative data arising from interviews with respondents from each of the selected OECD countries supported identification of strategies, practices and VMIs in each country (addressing objective 3). This was followed by the cross-country analysis so that the findings were framed within a more comprehensive qualitative account to explore similarities and differences across counties and inform the development of a VMF that supports implementation of Vulnerability Management Initiatives (VMIs) in the IoI (addressing objective 4).

# 3 Project discussion and key findings

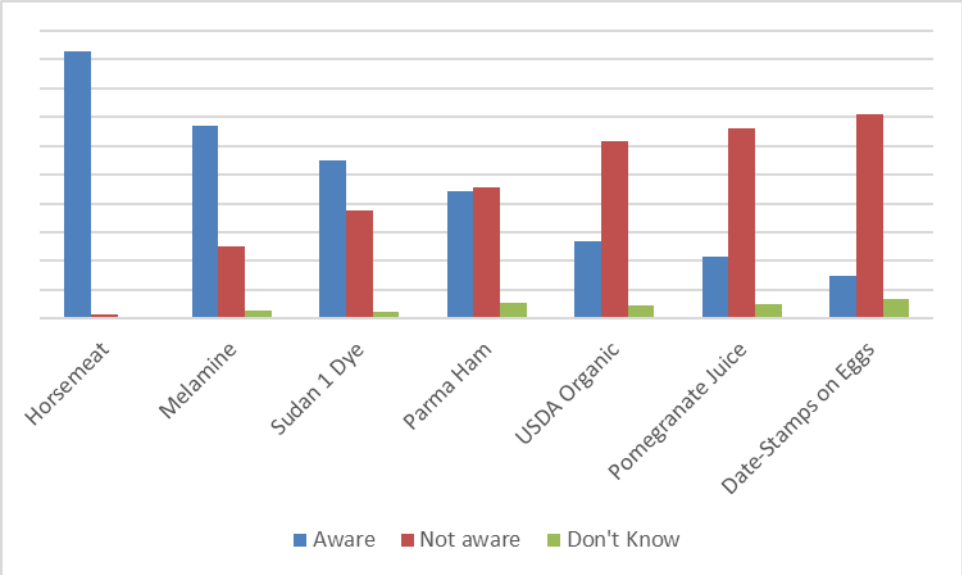
Findings are presented in relation to each of the project objectives. The first two sections address supply chain actors' perception of vulnerabilities arising from economically and ideologically motivated adulteration on the IoI and response strategies, the third section presents findings from other OECD countries studies in relation to their adopted strategies and practices, and the final section draws on the strategies and practices from across these jurisdictions to develop and interrogate a Vulnerability Management Framework (VMF).

## Key vulnerabilities in the food chain on the island of Ireland: awareness and concerns

### Awareness of vulnerability

Survey and interview data indicated an awareness of the challenges presented by intentional adulteration of product on the IoI. Survey respondents, when asked about specific frauds and threats that had occurred in the past, had a high level of awareness of most economically motivated incidents but lower awareness of threats. The "horsemeat" fraud and the case of adulteration of milk with melanin in China were the best known (Figure 3.1).

Figure 3.1: Awareness




There was a good level of knowledge of the relative likelihood and profitability of these activities. The industry also appears to have a good knowledge of ingredients that have been reported to be susceptible and of the nature of vulnerabilities and possible control measures. These aspects are discussed further below. Building on, or perhaps as a result of, this knowledge, some four out of ten respondents reported they experienced at least one incident of adulteration or misrepresentation in

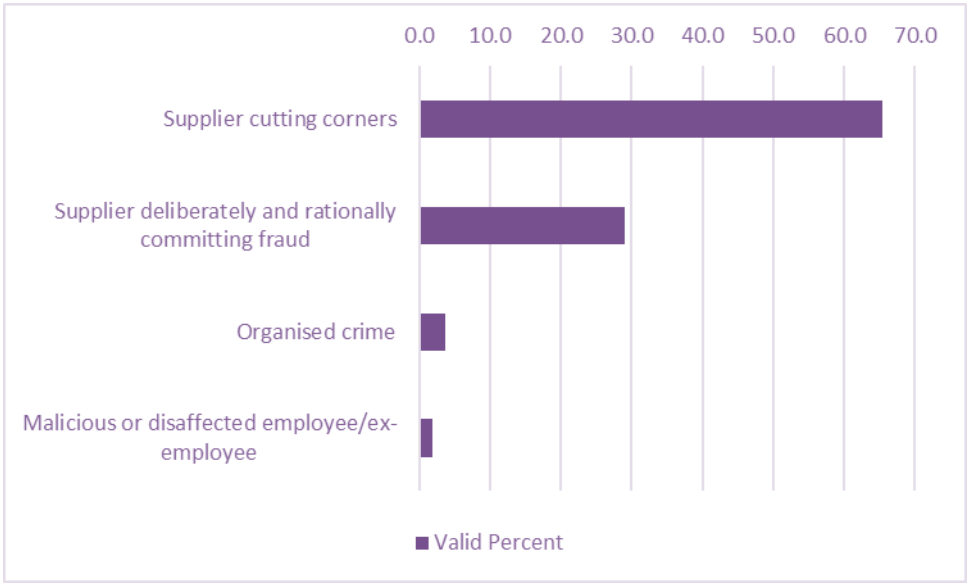
their own business's supply chain within the past 3 years – and about one in ten had incidents of adulteration or misrepresentation "more than once a year". Nevertheless, a majority of the companies who responded stated that they had not experienced any incident in the past 3 years.

There is some evidence that large companies were more likely to have encountered an incident than were small and mid-sized ones. This is attributed to a greater likelihood of detection rather than a higher level of incidence *per se*. No evidence emerged however that the propensity for having an incident, nor the frequency of them, was associated with particular product sectors or with supply chain characteristics (e.g. long versus short).

The overwhelming majority of incidents encountered (the most recent incident, if more than one) were seen as Fraud rather than as Threat (only 2 of the total were seen as Threats). Of the incidents of Fraud, the majority were seen as "cutting corners" rather than as "rational fraud" or "organised crime" (Figure 3.2). While the majority of perpetrators for the reported incidents were believed to be located within the IoI, there is a view that the farther geographically the supply-chain extended, the more likely the business was to encounter fraud. Evidence from interviews with stakeholders supports the 'complex supply chain' argument:

> *"Those things that are most vulnerable tend to be those things that come through complex supply chains, generally coming from outside of the island of Ireland, outside of the United Kingdom, and outside of Europe. So, the more complex the supply chain, the more processing that happens in that supply chain, the more likelihood there is in terms of fraud" (IoI_3)*

**Figure 3.2: Type of perpetrator**




Interviews with wider supply chain stakeholders provide further insight into the type of perpetrator involved; interviewees indicated that offenders are found across a spectrum from food operators 'cutting corners' through rogue actors to organised crime:

> *"It can be those people who are just cutting corners to try to keep in business. Often, they will not think of what they are doing as perpetrating fraud, even though they absolutely are" (IoI_3)*

The role of business culture is evident in characterisations of such activity, offering interesting insight into the motivation and rationalisation of behaviour at the 'cutting corners' end of the spectrum. The view is that such operators "know" they are doing wrong; however they rationalise that this is

acceptable since it is not doing any 'harm'. This can support a notion that quite a lot of fraud arises due to non-compliance; this is still considered to be fraud as there is an assumption that they are conscious of what they are doing.

> *"They probably know that they're doing wrong, but they probably justify to themselves that the product is still safe, and they suspect, or they believe, that the product is okay to pass onto the public" (IoI_4)*

These interviewee perspectives are reflected in the survey responses with almost all of the cases resulting from failures by suppliers, but in only one-third of cases did the buyer consider it to have been deliberately fraudulent or criminal. As explored below, this probably influenced buyer response, sometimes seeing it as a matter requiring contractual renegotiation or education rather than stiff penalties or fines.

### Food industry concerns

As evident from the review of literature above there are various forms of fraud and threat. This complexity is reflected in stakeholder responses:

> *"So, it can be about adulteration of the product, but fraud is a much more complex subject than that" (IoI_5)*

> *"We just did a small team think ourselves and we've listed 50 ways in which fraud can occur with food" (IoI_1)*

Because we find various forms of misrepresentation prevalent in the literature, we assessed industry perception of both adulteration and misrepresentation. While food product adulteration may arise due to economic or ideological motivation, misrepresentation of product is typically pursued for economic gain. Hence, in addition we investigated perception of the prevalence of both fraud and threat and related concerns.

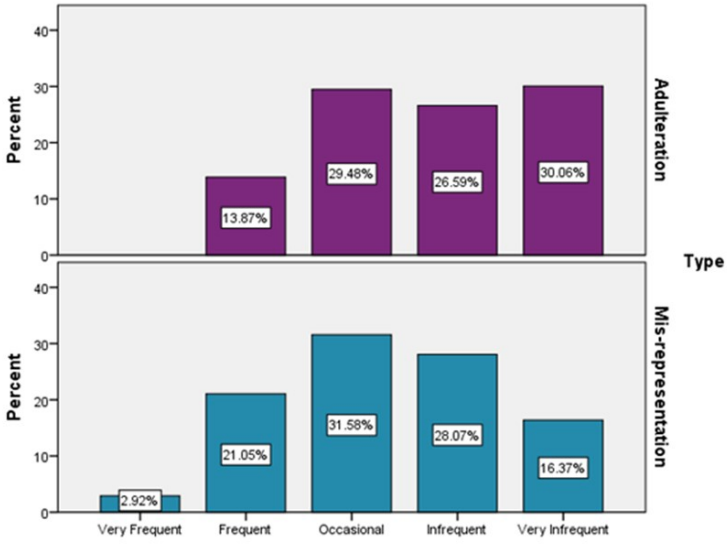
Industry does not, in general, perceive either adulteration or misrepresentation to be widely prevalent in the food supply chain, with only one in seven perceiving adulteration to be more than "occasional", and one in four thinking the same about misrepresentation (Figure 3.3).

While a small number of respondents (3%) thought misrepresentation was "very frequent", no respondents thought adulteration was "very frequent". Perceptions of the two problems were closely associated so that respondents who thought adulteration was infrequent were also likely to think misrepresentation was relatively infrequent, and vice versa. That said, the general perception was that misrepresentation was more frequent than adulteration with respondents usually scoring it the same or higher. Respondents found the level of incidents difficult to quantify due to the challenges of actual reporting. Nonetheless, they indicated that adulteration/misrepresentation is evident across all sectors, despite the varying level of vulnerability across product categories.

> *"It's quite a difficult one. I would say that it's very much under-reported. Any sort of impressions we give is based on the levels of reporting and knowledge we have" (IoI_4)*

> *"I think it's an issue that affects the industry, all of the industry. I think that if people feel that food fraud has not gotten within their industry, they're in denial. It affects every food manufacturer" (IoI_5)*

Figure 3.3: Perception of prevalence of adulteration and misrepresentation



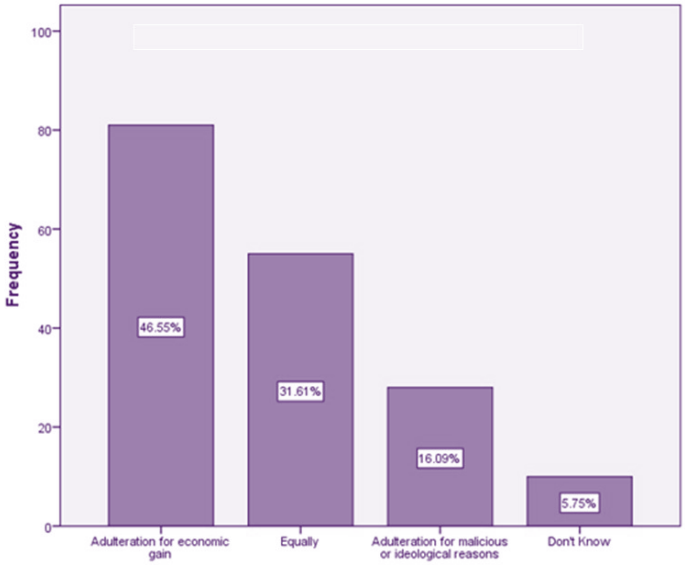

Analysis of respondents who believe adulteration and/or misrepresentation is frequent or very frequent suggested that they were more likely to be involved in the production of meat products, and/or to be smaller companies. Large companies were less likely to have this view about frequency. There was no indication that this group differed from the others in relation to other plausible properties, such as geographic location, actual experience of incidents, or supply chain characteristics, such as upstream or downstream or type and number of customers served.

Industry does not in general perceive these two problems, taken together, to be a growing problem in Ireland, a growing problem in their production sector, nor a major risk to their own business, with at most 13% rating them as a major risk to their business.

There was some evidence that these perceptions of risk/danger differed across broad industry sectors, with a cluster analysis identifying three sectoral groups (meat, dairy, or other), in which the perception of risk was broadly higher in the meat sector and lower in the dairy sector.

With regard to perceptions of the relative seriousness of fraud or threats, there was general sentiment that fraud was the more serious (47%) (Figure 3.4). However, some 32% felt that both issues were equally serious, and 16% felt threats were more serious. Thus, both motivations were widely felt to be important.

**Figure 3.4: Relative seriousness of fraud or threat**




They recognised food threats as distinct from food fraud in that fraud was seen as being more likely to emanate from suppliers (direct or indirect), competitors, and organised criminals while threats were believed to more likely to be carried out by terrorists (ideologically motivated) or by insiders (maliciously motivated). While terrorist threats were considered possible by interviewees, there was little evidence of such events ("*It's not something we'd see much, if any, of at all*" IoI_5). They highlighted the difficulties in addressing threats of a terrorist nature and considered a national/state level response to be more appropriate, notwithstanding a role for industry engagement ("*… as businesses we need to be awake*" IoI_5). This contrasts with sabotage which requires lead action at enterprise level:

> *"Unfortunately, I think the world is becoming more dangerous, and probably more unstable, be it from sourcing, or water sources, economics and so on, and migration, displacement. I think we can't consider that the food chains are isolated from being affected by those things. So, whether that would be intentional or terrorist-related, I think it's a reality. There are sophisticated ways, …. Do we actively consider that? Right now, I would say no, [pause] but we would probably be dependent on a lot of the government agencies, or at a regulatory level, to be assessing risks like that. It's not easy for us alone to do so" (IoI_3)*

The industry's perception of high-risk ingredients and products concurs with evidence from other research, namely that Honey and Olive Oil comprise a high-risk category. In addition, they identified Organic and Special-Claims (i.e. "extrinsic" properties) as also being at high-risk of adulteration or misrepresentation. By contrast relatively unprocessed ingredients, such as (non-organic) Fruits & Vegetables, and Nuts & Nut Products – along with Dairy Products - comprised a low-risk category. In addition to these categories, a stakeholder interviewed highlighted the attractiveness of new products with poorly defined labelling requirements, such as supplements, to fraudsters.

In order to assess industry perception of motivations and opportunities to commit fraud or threat, as well as control measures that could be put in place, respondents were asked to classify various statements as having a positive or negative impact. Analysis of responses indicate a good level of awareness of conditions that give rise to or deter food fraud/threats, in that respondents grouped these statements into two main categories. The first category comprises those that were perceived to increase the likelihood of a risk:

1. Simplicity of adulteration/misrepresentation
2. Availability of knowledge and/or technology to adulterate/misrepresent
3. High value of ingredient or final product (e.g. vanilla, Manuka honey)
4. Differences in pricing of ingredient across countries
5. Differences in business culture and governance across countries
6. Financial difficulties in producer's business
7. High level of demand for product
8. Financial pressure on suppliers.

The second category comprises those that were perceived to decrease risk:

1. Easy availability and low cost of test/detection methods
2. High security on access to materials during production
3. Steady pricing of ingredient or final product (i.e. no price spikes)
4. Transparency of supply chain and security of audit trail
5. Short or Local Supply chain.

## Current Vulnerability Management Initiatives

We define the term "Vulnerability Management Initiatives" (VMIs), as "strategies or actions which can be undertaken by stakeholders in the food supply chain to resolve (i.e. eliminate or reduce) their own or others' vulnerability to the risk of food fraud or threat". Stakeholders in this framework are individual firms, regulatory, investigative, and enforcement agencies, as well as policy-making bodies, both private and public, at the national and supra-national level. In this section, however, we concentrate on VMIs that are within the "span of control" (van Ruth et al., 2017, p. 71) of an individual firm, since that is the evidence available from the survey, with some additional commentary based on the stakeholder interviews.

We also distinguish between proactive and reactive initiatives. Proactive initiatives are focused on preventative activities, such as vulnerability assessment or deployment of detection technologies to facilitate information sharing. Reactive initiatives are those that take place in response to an incident, such as product recalls, legal recourses, and regulatory or criminal enforcement.

In terms of existing VMIs we identified two major categories of proactive initiative that have been undertaken:

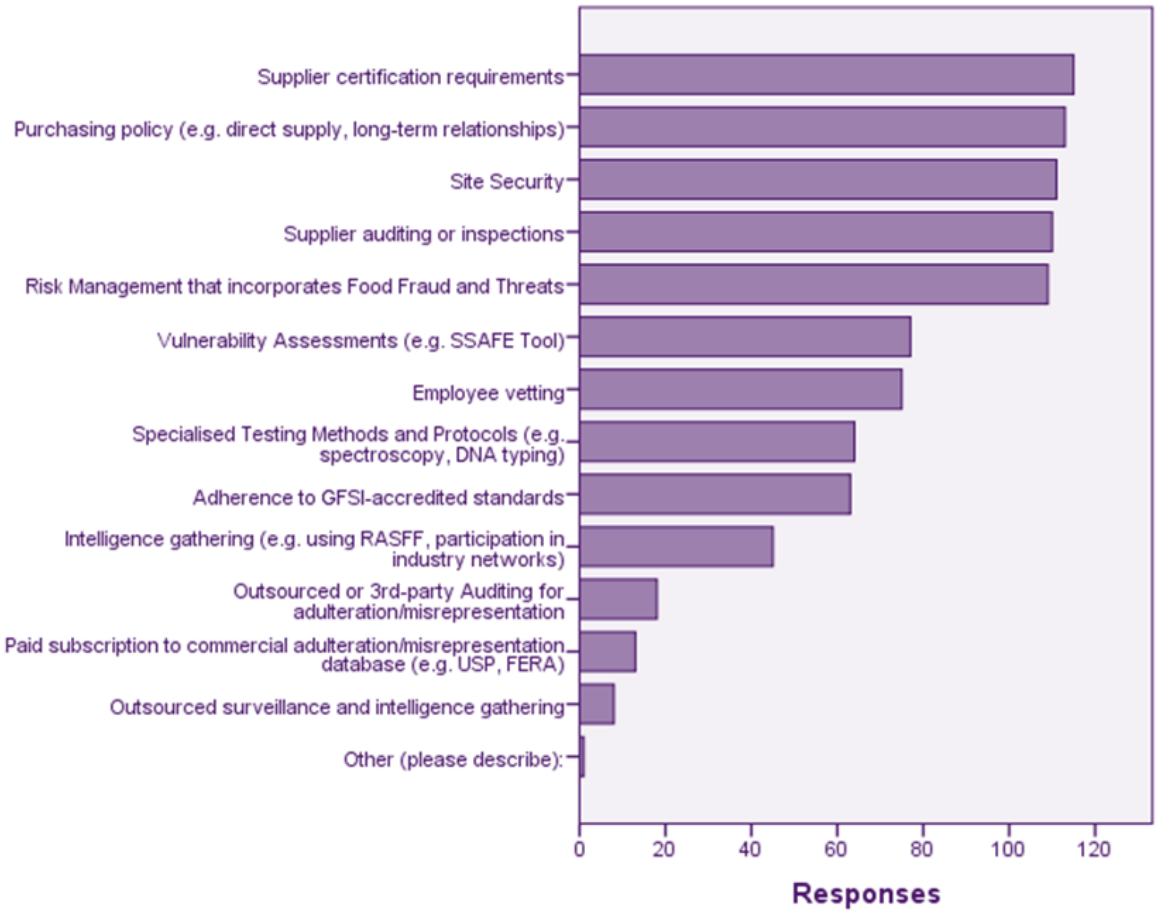
- Vulnerability Assessment Processes
- Surveillance and Information-Sharing Databases

### Proactive initiatives

#### Vulnerability assessment processes

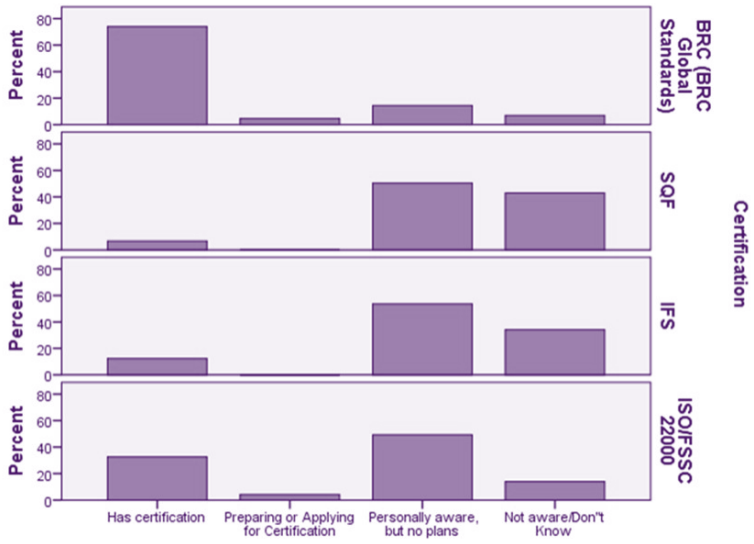
Three quarters of respondents reported that they had systems or processes in place to deal specifically with adulteration and/or misrepresentation, as distinct from general food safety or quality processes. A further 13% were either currently putting a system in place or were actively considering doing so. Only 13% had neither an operating process nor current plans for. With regard to specific processes (see Figure 3.5), by far the most frequently implemented were control measures applied to the inbound supply chain: Supplier certification requirements; Purchasing policy; Supplier auditing or inspections (all above 80% of respondents).

Figure 3.5: Vulnerability management - systems and processes




Formal Vulnerability Assessments, such as that advocated by Safe Supply of Affordable Food Everywhere (SSAFE), were implemented by 59% of respondents, 49% adhered to GFSI-accredited standards (which incorporate Vulnerability Assessments), and more general Risk Management for fraud/threats were implemented by 84%. Among the GFSI-accredited standards, BRC is by far the most widely adopted in the IoI, with some 74% of respondents holding that certification, and another 5% preparing for it. The second most popular certification was ISO/FSSC, with 32% holding it, and 86% being aware (Figure 3.6). Levels of awareness of all four certifications were quite high, with all being above 50%. Moreover, quite a few respondents held multiple certifications, in some cases all being certified in four named schemes (as illustrated in in Figure 3.6). Strictly local firm or site-level initiatives such as site security (85%) and employee vetting (58%), were also widely adopted.

**Figure 3.6: Awareness and usage of main certified standards by survey respondents (IoI)**




As highlighted by the review of literature, pressure from the dominant buyers, i.e. the large multinational processors and the multiple retailers, has driven many of the initiatives for accreditation and certification, and contractual requirements for such certification has pushed its adoption upwards along the supply chain. In that regard it is interesting that among the respondents to a question regarding which companies were considered to be "leaders" in responding to food fraud and threats, those most mentioned were multiple retailers (25%), and multinational Irish and foreign processors (33%). In other words, these efforts were seen to be strongest in and to emanate from large firms.

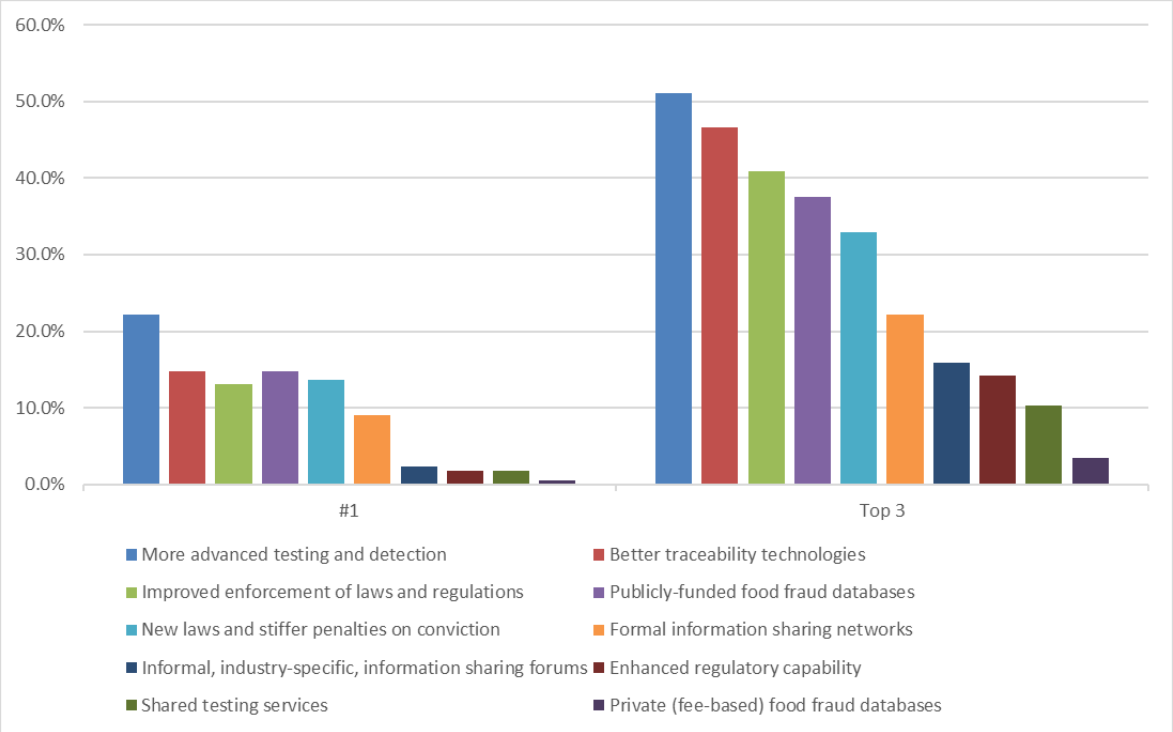
### Surveillance and information-sharing databases

By contrast with the above, outsourcing of either intelligence-gathering or auditing were infrequent (6% and 14%) practices, as was the use of commercial intelligence-sharing databases (14%). Use of any form of intelligence-gathering and sharing, whether private industry networks or public initiatives such as RASFF was not widespread (35%), but specialised testing methods, such as DNA typing, were used by some 50% of respondents.

Despite their limited usage across the sample, all four information-sharing databases we inquired about in the survey were used by some companies. Of those that were used, RASFF was by far the most often used, with half of users of such databases consulting it at least occasionally. FERA was similarly consulted by 22% of those using such databases, and Decernis and Commodities were consulted by about one in ten. When asked to identify any other databases that they used the respondents gave prominence to alerts from the public food safety authorities such as the FSAI, FSA in NI, FSA (UK), OPSON (Europol) and the FDA (USA). Several mentioned UN bodies, such as the FAO and WHO. Three mentioned the commercial database maintained by Campden BRI.

Just over one fifth (22%) of industry respondents listed 'formal information sharing networks' in their top three most promising developments for tackling food fraud and threats. In addition, almost four in ten (38%) listed 'publicly funded food fraud databases in in their top three most promising developments. (Neither of these however scored anywhere near as highly as 'more advanced testing and detection' (51%), or 'better traceability technologies' (47%)). (See Figure 3.7).

**Figure 3.7: Most promising new practices**




The value of such systems was highlighted by the other interviewees also.

> *"The best forum we have developed is FIIN, and the reason FIIN works well is that it is anonymised. It's retailers, manufacturers, and the FSAI now as well. You're putting in there all your test data, anonymised, so we can look onto there and see – there is a whole load of people do – and your negative results as well as your positive results are in there" (IoI_5)*

> *"[T]he FIIN network is probably one of the best things that's happening right across the world. That's lots of different food businesses coming together to share information, share intelligence. I think that's the best example. For individual companies to try to deal with it, it's really difficult" (IoI_3)*

FIIN is supported by Campden BRI through database management (including assurances of anonymity), analysis of data and the provision of reports.

### Reactive initiatives

The information gained from the industry survey on VMIs which are more reactive in nature relates only to responses from firms which had experienced an incident of fraud or threat within the past three years. As detailed above, these comprised 39% of the total sample, or 59 firms.

Most of the incidents reported in the survey were detected by the firm's own testing (61%), although some were detected by supplier testing (20%) or by 3rd party testing or auditing (11%). One fifth was detected as a result of an alert from public authorities or regulators. Very few resulted from information from consumers (5%) or whistle-blowers (2%, i.e. 1 case).

By far the most common action undertaken by companies in response experienced incidents of fraud or threat was to delist the supplier (54% of cases). The next most common actions were to increase supplier auditing (36%) or to enhance product testing (28%). Only 10% alerted the authorities and in only 1 case did the firm register the incident (and supplier) in an information-sharing system. Some

20% of cases resulted in product-recalls, but in no case did the firm undertake a public-relations or reputation-management campaign. Thus, it appears from our data that affected firms tend to delist or manage an offending supplier and tend not to share information about the incident with the regulatory authority, or with a wider audience, such as customers, consumers or the media.

### Company rationale for use of Vulnerability Management Initiatives

While the survey could not inquire explicitly into the respondents' or firms' reasons for adopting their particular mix of VMIs, it seems that certification requirements (of customers, primarily retailers) are a strong driver. Some 79% of respondents held certification to a standard that is GFSI-accredited (BRC, SQF, International Featured Standards (IFS), or FSSC), which requires the holder to carry out Vulnerability Assessments for fraud or threats. Overall some 84% reported having a Risk Management process that incorporated fraud and threats.

Most of the respondents believed that organisational units at company level have the primary role in developing and implementing processes for preventing fraud and threats. Of those, Management is seen as the most important organisational unit, followed in order by the Food Safety & Quality team, the business as a whole, and finally the employees. Indeed, ensuring the integrity of the management team, developing processes and controls to protect against food chain vulnerabilities and ensuring staff at all levels are involved was seen as critically important by one of the interviewees. Having shared objectives at management level and a structure that supports shared objectives was seen as good practice for companies:

> *"Because if you have a structure that is working in silos, as that last company that I referred to was, you end up with gaps between the functions for things to fall through" (IoI_6)*

Structuring one's supply chain to have a closed loop was another useful initiative:

> *"We were the only [-] manufacturer, I'd say, in Europe, not to get tainted with the horse-gate issue. That was because we had a closed loop supply chain" (IoI_6)*

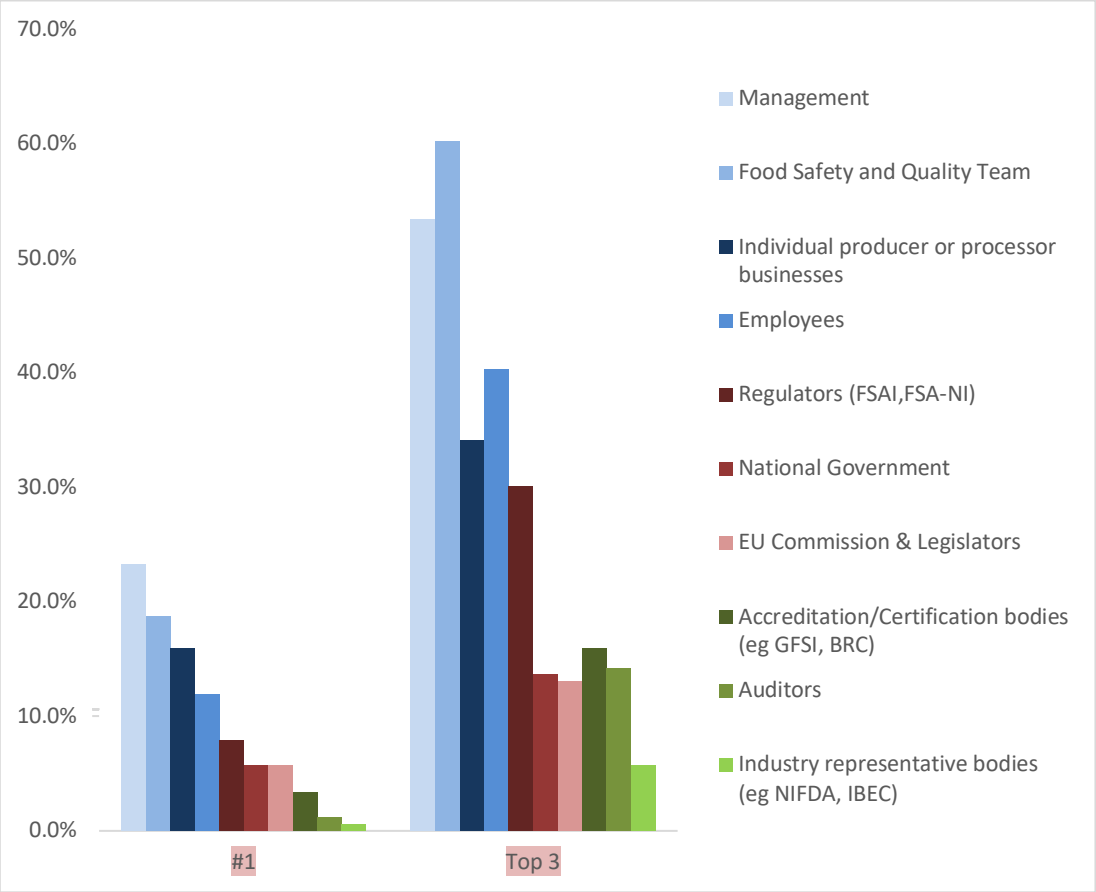
External bodies, such as governmental (Regulators, National, EU) stakeholders or intermediary stakeholders (certification bodies, auditors, or industry representative bodies) were seen to have lower levels of responsibility according to the survey results (Figure 3.8). While many in industry recognise primary responsibility, the role played by the broader stakeholder network is highlighted by interviewees, for example the view of a company interviewee that:

> *"[W]e would probably be dependent on a lot of the government agencies, or at a regulatory level, to be assessing risks like that. It's not easy for us alone to do so" (IoI_5)*

Indeed, there is a view amongst the wider stakeholder network that a coordinated approach is required, with high levels of trust between public and private actors:

> *"Food business cannot think that they should rely on government to prevent and detect fraud. There is a massive obligation on food businesses to do something. But equally so, my argument to those people in the regulatory authorities who say, 'It's up to businesses to do that', I see that the government's responsibility is security. Food security is a big part of security, and fraud is a big part of food security…[..] It has to be around working together in partnerships between those two big players, the regulators and the industry, and not to have it as an adversarial relationship, which is often the case" (IoI_3)*

### Figure 3.8: Responsibility for prevention



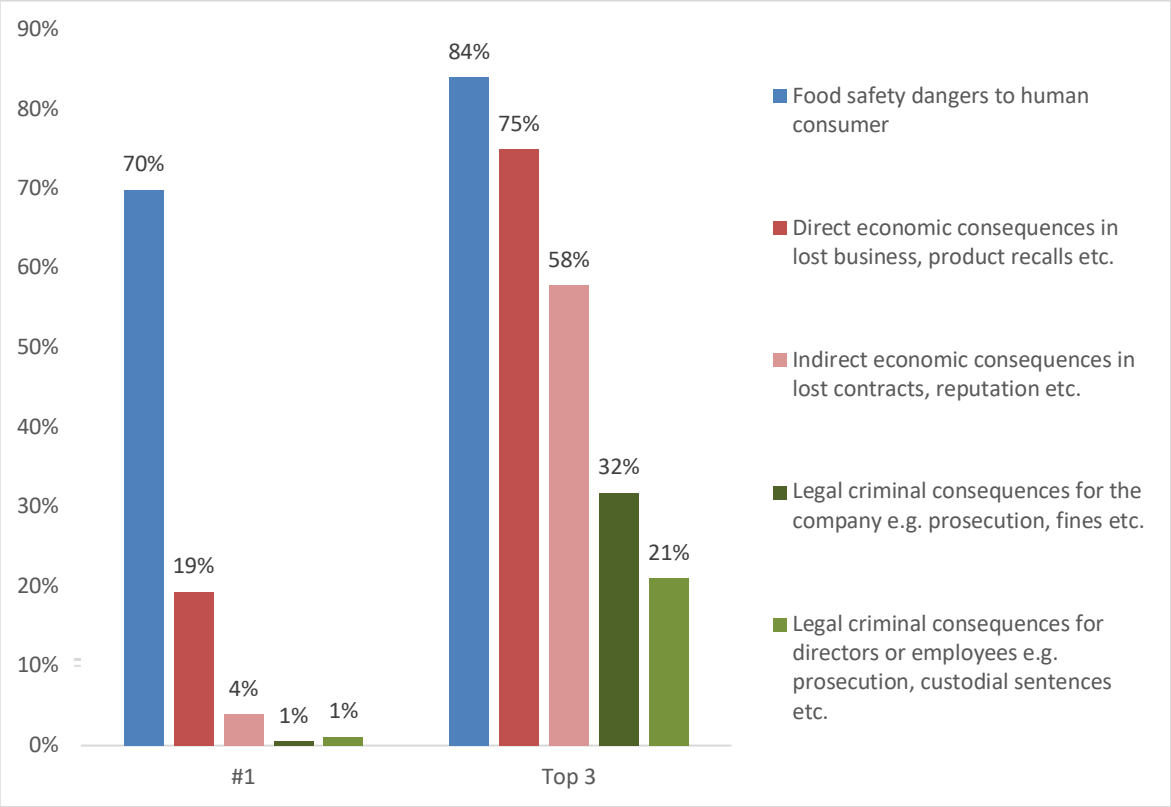

Looking also at responses to the question of how the firm's response to any future incident could be improved in light of their experience, eight in ten respondents proposed improvements in testing or auditing, a further one in ten suggested restricting their inputs to those from "short" supply-chains while the remainder suggested improved coordination ("more communication to supply base" or "knowledge sharing across the food industry and regulators". These responses reinforce the view that industry sees itself as primarily responsible for addressing such issues. While it is important that companies take such responsibility, such a firm-level focus may limit the potential for broader system improvements that could arise if for example companies shared information on testing results (both positive and negative), thus enhancing knowledge, and strengthening future VMIs.

### Industry perceived consequences of food fraud and threat

Danger to the health of consumers was identified by seven out of ten respondents as their primary concern when applying strategies to prevent or respond to fraud and threats (illustrated in Figure 3.9). Economic consequences (direct or indirect) were also important (24% ranked it number 1, and most included those items at number 2 or 3). Legal consequences were much lower, with only 2% ranking those items number 1. Of course, health, economic, and legal dangers and costs are not independent but are strongly inter-linked. Respondents were also aware that an incident at one company can impact on reputation and consumer trust in a much wider sector of the industry:

> *"It only takes one serious incident in any size of company anywhere to start a scandal on the back of a very active "story hungry media" to destroy any industry" (Survey respondent)*

**Figure 3.9: Industry perceived most important consequences posed by food fraud and threat**




This was supported by stakeholder interview responses that emphasised the importance of reputation and brand protection. This included both food fraud and threat:

> *"[Y]ou have a responsibility around brand protection …. to put into place procedures to protect ourselves and [customers] from staff who may want to harm the company or harm the brand" (IoI_6)*

> *"It can destroy reputations of food companies. Once your reputation is damaged, it's long-term, and your businesses have gone out of business because of it. That's reputation piece" (IoI_3)*

As detailed earlier, the vast majority of incidents that were experienced by respondents were perceived as cases of fraud. Moreover, most of these were seen as a "supplier cutting corners" (65%), rather than as "deliberately and rationally committing fraud" (29%). Taken together therefore 94% of the incidents originated from suppliers, with 2% being ascribed to malicious employees (i.e. insiders), and the final 4% being "organised crime" (i.e. outsiders). This predominance of origin in the inward supply-chain likely explains why the firms focus their VMIs on input-controls, such as supplier-audits, certification back through the supply chain, and ingredient testing. Malicious actions by insiders are harder to predict and control, but internal auditing and employee vetting provides assistance. Actions by outsiders, such as organised crime, are harder to anticipate or to control. The case of threats by terrorists (not reported in this data, nor much in evidence in the literature), are by their nature even more difficult to deal with. One respondent described their greatest worry as arising from the "*apparent randomness of ideology motivated threats*". Another described the concern arising from "*not being aware of a particular threat, and not monitoring an unknown risk.*"

With regard to new VMI-related processes and practices there was again an emphasis on testing and traceability, with 22% ranking testing at number 1, and 15% ranking traceability at number 1 (see

Figure 3.7). Notwithstanding some interest in the potential of information-sharing networks, as evidenced by respondents ranking them in their overall top 3 new practices (38% for public networks, and 22% for private ones), only 15% placed public networks as their number 1 rank, while 11% rated private networks at number 1. Moreover, enhanced regulatory capability was rated number 1 by a mere 2% of respondents (and only 14% placed it in the top 3 new practices). Overall however, no practice scored more than 22% as a top-ranked one, so we would judge that respondents do not have a clear direction in terms of new developments in this area. Turning to new technologies, test (e.g. handheld rapid testing devices) and traceability (DNA barcoding, RFID) again came top, but most technologies were rated as middling (somewhat or slightly promising) – with only "edible tags" registering some potential. Thus again here we see a focus on firm-level VMIs when the respondents look forward towards new developments in the field.

## Practice in selected OECD countries

While the fundamental goals of stakeholders are similar across jurisdictions, how these goals are addressed can vary with the result that different initiatives are undertaken thus providing an opportunity for learning.

Initiatives undertaken in Denmark, the Netherlands, the UK, and the USA were explored through expert interviews as outlined above. Three different types of initiatives were identified:

1. Initiatives based on the institutional landscape, including changes in existing institution's and the establishment of new units/structures
2. Initiatives based on collective industry-led action or private organisations, e.g. data sharing and development of standards
3. Company practices undertaken to address vulnerabilities, e.g. in-house data collection through testing and monitoring.

While three different categorisations existed, and there was an identified need for third-party, independent organisations to be involved, there was a clear recognition of the need for an integrated approach involving public and private actors.

> *"I think it should be separate. Of course, companies are responsible for these things and they should make sure that the whole lot is tidied up but there should be an independent organisation for us all that have checks of their own and of course there is all these food safety management systems but I think they also should have their own view (NL_1)*

> *"What you need is to have the regulators involved in surveillance, routine surveillance, and you need to have the companies seeking in-houses surveillance and certificates of analysis, certificates of conformity, from their suppliers. If there is more testing people will have to be more vigilant" (EU_1)*

### Institutional landscape

The establishment of a multi-agency inter-disciplinary task force in Denmark, known as the "flying squad" was seen as a crucial aspect of addressing food fraud there. While traditional policing skills continue to be important, skills from food inspectors, accountants, people working in logistics and warehousing, journalists, and people with "open source investigation skills" help to investigate and find the required information to support a prosecution whilst a former lawyer within the team can help to determine whether the case is good enough to go to court. As with all resources, the team are conscious of having to target their resources and to prioritise cases. In a similar unit in the Netherlands, they are conscious that they cannot investigate all the cases they are handed. "*In general on a yearly basis we decide on our priorities for the next year and this is fed with reports on the analysis I mentioned*" (NL_2). The deployment of a inter-skilled investigative unit was also emphasised in the Netherlands:

> *"A number of [the unit team] have worked in the industry and literally from farm to fork, so a number of employees came from a farm. They were educated in agricultural science in our university so.. but furthermore we have forensic accountants, financially educated people etcetera, etcetera. Also IT audit people" (NL_2)*

While there was some commentary amongst the interviewees in different jurisdictions as to where such an investigative unit should be located with pros and cons seen in terms of locating it within a regulatory authority as opposed to within a police force, the need to have a dedicated fraud unit was a recognised need in each jurisdiction. This discussion reflects the need for a multi-agency, multi-disciplinary team "*where you have people that have the ability to do authenticity testing, who knew the legislation but also had the power to gather evidence*" (EU_1). The importance of international collaboration between such fraud units and other agencies was highlighted:

> *"In the EU Commission, they have food fraud units in Commission whether it's five people sitting trying to help the countries sharing information across between countries" (DK_1) "We have our own databases, but we also tap in on the databases of the Dutch policy authorities and through Europol and Interpol internationally. So, our information, we supply to Europol and Interpol and they put that in their databases" (NL_2)*

The need for inspectors doing "*front line safety matters*" to have skills and knowledge to be able to do evidence gathering properly was emphasised in the UK, along with the provision of such training to auditors for private accreditation schemes. A team is being developed to address this need.

> *"…and I think someone even said that at one of the conferences I was at recently, and asked the question of me, will we be training and up skilling auditors and the private accreditation schemes in what to look out for? What are we finding, how can we help them with our understanding of criminal behaviour? I think there is a great need for that. I think there is a great need for us to do that. We will be reaching out to industry, and indeed the private assurance bodies. I've got a team that I'm setting up whose job is to do just that, to work to reduce vulnerabilities, and increase the effectiveness of audit in that space, by telling them what to look for and how to go about it perhaps" (UK_3)*

The importance of providing training for public and private actors is also addressed in the US.

> *"FDA has established an Intentional Adulteration Subcommittee with the Food Safety Preventive Controls Alliance to develop food defence training resources for industry and regulators alike"* https://www.fda.gov/food/guidanceregulation/fsma/ucm378628.htm

The range and use of penalties imposed on perpetrators was identified as a key consideration when designing VMIs:

> *"Oh it does. I think, if the likelihood of getting caught increases, then there will be less risk of people engaging in shoddy practices. So, if you think you're not going to get caught, it's very easy to engage in food fraud. But if you're going to be caught, the risk is high. I suppose, we would probably need bigger penalties. So a combination of more draconian penalties, and better detection methods will deter people" (EU_1)*

In Denmark this idea is addressed through changes to the penalty system and high levels of inspections. The penalty system was revised to make the fines a stronger deterrent and more in proportion to the crime. They combine "naming and shaming" with fines to further strengthen the deterrent. According to one interviewee

> *" ….kind of penalties. In Denmark you can get double up.. if you cheat somebody then earn 100,000 you can get a fine of 100,000 and have to pay back confiscated 100,000" (DK_1)*

> *" ….the companies fear our inspection report more than they fear the fine. The fine they can pay easily but telling all their customers.." (DK_1)*

The high level of inspections per annum, combined with reporting of the results of the last four inspections for each company on the internet (findsmiley.dk) is seen as a good tool to fight food fraud. The logic is that customers can easily see this information with the result that companies can lose customers and sustain long term reputation damage. While use of punitive measures to dissuade potential perpetrators emerges as a key element of a preventative strategy, the need to protect the reputation and anonymity was also evident. Hence building trust and stimulating collaboration between industry and regulators emerged as a key challenge.

> *"It's all about collaboration with industry. That, to me, is the thing. It's all about creating that bridge of trust between the legitimate industry and the food regulator. That is a challenge, don't get me wrong. If you are going to base your food crime response within the food regulator, which we are, and the FSAI are, then you are going to have those challenges, because ultimately it's the regulator they're concerned about speaking to. If you're going to base your food crime response within the police service, I think you've got less of a concern, because industry would perhaps be more comfortable with speaking to the police than they would be speaking to the regulator. I think that relationship is*

*absolutely critical, and it will take a long time to build that level of trust, but I think it's essential if we're going to do this properly" (UK_3).*

*"So we don't want to make it bigger for a supplier if there's nothing wrong. So it's always a bit difficult to know what you can share and what's the privacy of the supplier or.. There's an openness to sharing information between the retailers" (NL_3)*

Some regulators are aware that they are being put to the test by companies to ensure their trust in sharing information is warranted. For example, reference to a company sharing test results with a regulator, in this case the Regulator recognised the importance of "walking the walk" and pursuing the case without damaging the company that provided the information.

The Danish Agriculture and Food Council provide a useful service to companies through their horizon scanning service (operated through Fera's HorizonScan system) which should be used as a complement to firm level activities. The Danish Agriculture and Food Council monitors, on a weekly basis, activities in certain commodities on a global basis, e.g. any significant shifts in supply, demand or price. This service is seen as an awareness raising/alerting service which should trigger individual companies to subsequently look at their sourcing decisions and practices in relation to a commodity that may be flagged for concern.

An example of linking different initiatives was also given in the US; high-risk food inspections at ports in the US are complemented with "micro alerts" through the FIDES system, with potential for greater use of such a system indicated.

*"So there are these micro alerts that I think we can learn from when something is breaking or to predict. So I think we have to get there, but those are warnings in the system, they are just telling you 'you need to either go back for better data, or maybe to take action'. So it's not the end-all. So it might just be that is says, 'Okay, now go and …' it might help you target inspections. So, on average, we do high-risk food inspections at the ports in the UK, for example, but it's still only 1% of our food. You can't inspect everything. So what a system like FIDES will do is it will say, 'Hey I think your problem, if there's a needle in the haystack, I think your needle is in quadrant four'. So then you can target your mitigation or your finding" (US_1)*

Provision of guidance documents by regulatory authorities on how to design and implement food fraud vulnerability assessments was seen as an important initiative across a number of countries. These are seen as particularly valuable for smaller companies and are often made freely available online. The number of downloads is tracked as a measure of effectiveness. A government initiative to establish a Food Confidence Task Force in the Netherlands aimed to create a public-private forum to improve measures taken to safeguard food supply chain integrity. This initiative has defined a set of criteria for quality schemes to align the private standards that aim to safeguard food safety and especially food integrity (https://ketenborging.nl/).

The capability of supply chain actors to adopt and operationalise assessment tools and plans emerged as a key theme. In this regard the complexity of the tools requires attention:

*"[T]hey [FDA] shifted from CARVER + Shock, which ended up being very, very complex, and not very efficient. What I hear from industry, informally, it's extremely complex and people weren't getting results. FDA shifted to what they call the FDA Food Defence Plan Builder, to the point that CARVER + Shock, the software, which was free, is no longer available to download on FDA's website" (US_2).*

The capacity of smaller companies emerges as a related theme. In this regard the experience and views of interviewees support the findings from the online survey and highlight resource constraints of small and medium sized food companies:

*"Medium and small companies have no salary for this. It's somebody's extra job. They are not trained in it" (US_1).*

In terms of level of responses food defence presents a particular case. Identifying the sources of ideologically motivated threats informs both appreciation of impact and response required. Similar to

findings from the IoI, interviewees could offer few example of threats other than those intend on sabotage, in particular as disgruntled employees:

> *"That [food defence] tends to be more on-site it's not as widespread as food fraud is. I mean there's been a couple of incidents of food defence here but it's been disgruntled employees as much as anything else" (US_3)*

For these attacks site level defence measures are required, however for those attacks that aim to either sabotage at a sector/country level or terrorise, national and international responses are required. Regarding the former, a USA interviewee referred to the devastating impact of use of cyanide poisoning of grapes of Chilean origin on the USA market in 1989:

> *"It ruined the Chilean grape market for one or two years. Three grapes they found contaminated" (US_3)*

The more recent incident of deliberate contamination of strawberries with needles in Australia is a stark reminder of the devastating impact of such attacks (NSW Food Authority, 2018; Australian Associated Press, 2018 ). While the latter, terrorism, may be unlikely the impact on citizen trust in the food system may be seriously impacted and hence merit attention at governmental level with due consideration for scope of the attack.

> *"For terrorism, it is so hard. It is a low probability event, with extremely high consequences. When I talk to people about it, I often say if one infant got sick from a food safety event, sad. If one infant gets sick from an intentional poisoning or adulteration, our country and maybe the globe will come un-glued. There will be fear" (US_3)*

### Collective industry-led action or private companies

The need for collective action by industry to share knowledge was a feature of several initiatives cited. The Food Industry Intelligence Network (FIIN) emerges as a rather prominent example in the UK. Established in 2015, FIIN has a membership across the supply chain, including major retailers, manufacturers and food service companies. The network aims to create a safe environment for members to share food authenticity test results and wider experience in the area of integrity of the supply chain. One interviewee believes the strength of the FIIN system is that it is anonymised creating an incentive for the participating bodies, retailers, manufacturers as well as the regulatory authority, to share data. Furthermore, another strength that was highlighted in regard to the FIIN system is that negative as well as positive test results are shared. Building trust and stimulating collaboration between industry and regulators is an important aspect of the FIIN so that organisations are very sensitive in what information is shared.

Private companies can provide a valuable service to facilitate information sharing and monitoring and alerts. An example was given of a commercial laboratory that provides a valuable newsletter service to companies in this regard. They monitor databases and other newsletters and produce their own newsletter to keep companies up to date with regards to potential risks, including emerging risks, new detection methods, training courses, events, etc. In addition to providing useful information and intelligence, this service is believed to sensitise companies to the issue and prompt them to: "*start to use the different mind-set that, you know, from the trusting mind-set of a common Dane*". Another benefit of this newsletter is its context within a network of companies facilitated by the lab. The companies share knowledge within a "safe space". The confidentiality associated with this safe space is seen as sacrosanct so authorities and certifying bodies are not part of the network, but retailers are. This horizon scanning and awareness raising system is also offered by other commercial companies.

Risk assessment systems developed by private companies (e.g. SSAFE by GFSI, PwC and nine multinational companies) are identified as important resources for companies. While SSAFE may be a complex system, it is considered useful for vulnerability assessments for raw materials with simpler systems such as FDF also being available online free of charge. Standards in the USA are evolving with the Product-Counterfeiting Incident Cluster Tool (PCICT) being in the final stages of being accepted as an ISO standard. The benefit of such a system is that companies will be able to analyse their incidents and then prioritise within their decision-making activities.

> *"Product-Counterfeiting Incident Cluster Tool (PCICT) that's actually in the final stages of being accepted as an ISO standard…[ ].... It's an ISO standard because it's the process to cluster. But the key is, you don't generalise with general information, you generalise with specific information. So, you have to gather specific incidents. Then you can start to code them, organise them, and then build them up to say that this company has more counterfeits than they do stolen goods, or something. But that's the key, that you can cluster together, so you'll see then, the key with that is that if a company has a lot of return fraud, it's a problem at that store, then they know they should focus on return fraud, not counterfeits. That will help them prioritise their decision making" (US_2)*

### Company practices undertaken to address vulnerabilities

Overall the evidence points to increasing awareness at company level about the need to identify and assess vulnerabilities in their supply chains from raw material through to consumers. In the US, larger companies are known to be hiring food defence professionals.

> *"Well I think now every [name] organisation has a schedule to map their products, to map their suppliers and make cross-connections. You see, you have difficult products, like fish. You have difficult suppliers, because they're maybe from the Far East, and if you combine these kinds of information you can see the combination of what are real, well, if you say dangerous, … And I think … organisations have something in place, a schedule or a system to rank their products and their suppliers" (NL_2)*

Given the different nature of food safety and food security, and thus required responses, some companies in Denmark were identified as having divided their food safety quality departments into food safety and food security. Linking vulnerability assessments to action is seen as important. The need to build in-house capability to detect fraud was seen as important. In some cases, the need to clearly communicate a company's activity in this space was also highlighted; such an approach places greater emphasis on detection and avoidance as opposed to prosecutions. Looking at commodity prices, databases, networking systems to see what is going on was seen as a good practice in relation to food fraud. This facilitates targeting resources. In relation to food defence, testing raw materials coming in, looking at one's supply chain and the members involved in it was seen as a good practice:

> *"I'm in favour of these broad anomaly tests to determine if something is authentic or not and only if you find that it's not authentic then you either go talking to your supplier or you carry out more tests to find out what's going on there. So that will limit the cost enormously but they are very fenced and you get more and more of these handheld portable devices and everything to…but they are not as accurate" (NL_1)*

Requiring certificates of authenticity seems to becoming a routine good practice in some industries to address food fraud. For example, for sales of meat into a particular retailer, a supplier is required to provide a certificate of analysis to say the product is as identified. Manufacturers have rigid supplier management processes in place and retailers are revising their supplier approval's processes to include food fraud as one of the parameters. Adoption of standards such as Publicly Available Standard 96 and BRC Global Standards, are recognised as good practice for use by industry. The free availability of PAS 96 online is seen as offering a significant support to smaller companies in particular. One interviewee believed that standards should be the focus:

> "*Yeah I think you just need a robust defence of Food Standards really*" (UK_1)

The use of "*external data"* through proprietary or public databases to get an idea of the risk complemented by the use of "internal data" was a recurring theme across interviewees across scales, i.e. at sectoral, commodity and individual company level. Stage 1 involves specifying the quadrant of the haystack in which one should look for the needle. However, the multiplicity of such databases is a challenge for companies.

> *"And that's actually that's one of the big problems in industry right now is, what do you use, Decernis or Foodakai? Or do you use Decernis. They're all struggling with that what they're trying to do now is integrate all of these, that actually is a problem, because each of these databases we're talking about are little bit different, they all do the same thing. And they each look at things a little bit differently in the different parameters in them, the algorithms that drive them around a little bit different. So companies are struggling with that now, and that helps them to reduce risk" (US_3)*

## Vulnerability management typology and framework

The design of a vulnerability management typology and a VMF is informed by analysis of the industry survey and interviews with IoI stakeholders and practices in selected OECD countries. Hence the sections below draw on the analysis above and incorporate further analysis resulting in identification of cross-cutting themes, including: span of control, mind-set of perpetrator, information sharing, expertise (including interdisciplinary), collaboration and the roles of different actors both public and private.

### Vulnerability management typology

Building on the classification of VMIs as either firm centric or system-wide, Table 3.1 presents a typology of approaches to vulnerability management on the basis of type and level of interaction among stakeholders.

**Table 3.1: Vulnerability management typology**

| | | |
|---|---|---|
| **Public-Private** | N/A | Policy/Regulatory bodies and Supply Chain actors<br>e.g. Dutch Food Confidence Taskforce |
| **Public** | Agency Centric<br>e.g. Food Crime Unit (incl. "interdisciplinary teams) | Multi-agency<br>e.g. Food Fraud Task Force coordinated by FSAI |
| **Private** | Firm Centric | Supply Chain<br>e.g. Food Fortress |
| | *One Stakeholder* | *Multiple Stakeholders* |

As evident from analysis of data from the survey, industry in the IoI adopts a predominantly firm centric approach. These measures tended to focus on vulnerability assessments together with supplier auditing and enhanced testing. While measures taken often include decisions on supplier relationships these appear to be unilateral (notwithstanding some examples of working with suppliers to address concerns detected). There was some evidence that survey respondents felt more concerned about complex supply-chains, for example ones that involve a "diversity and number of suppliers", hence the emphasis on preferred suppliers. They also expressed concern about indirect inputs (dependence on suppliers' supply-chains): "reliance on suppliers and trusting their supply-chain - as a result we tend only to buy from larger companies". Finally, concerns were recorded about inputs that came from farther away, and in particular from outside of the EU, e.g. "the length of the supply-chain with remote sub-suppliers" or "sourcing of materials from outside EU" or "fraudulent or adulterated raw materials from countries outside the EU". This was supported by interviews with IoI stakeholders, for example:

> *"Now, those things that are most vulnerable tend to be those things that come through complex supply chains, generally coming from outside of the island of Ireland, outside of the United Kingdom, and outside of Europe. So, the more complex the supply chain, the more processing that happens in that supply chain, the more likelihood there is in terms of fraud" (IoI_3)*

Further exploratory research identified an interesting example of a supply chain approach taken in the establishment of the Food Fortress Network (http://foodfortress.co.uk/). This is a collaborative

network of animal feed importers and compounders in the IoI that, with the support of the Institute of Global Food Security, QUB, have established a coordinated testing regime for imported feedstuff. Working with QUB, the network developed risk assessment capability that informs this testing regime. On the basis of test results, guidelines are issued to members, including mitigation measures. The knowledge accumulated from activities over recent years informs risk profiling with resultant improved targeting and use of resources. Furthermore, protocols for information sharing and incident management have been established to facilitate sharing information with DAERA and the FSA NI. QUB continue to provide services to the network; this includes a repository for test results that guarantees anonymity. As indicated in the analysis of IoI data, food supply chains actors' desire for anonymity emerges as a key issue. This is also evident in other interviews with stakeholders, for example:

> *"There are challenges in reporting of victimhood to the authorities … and those challenges are primarily around reputational damage. … And I hear this anecdotally everywhere I go, that if a food business discovers they have been a victim of food fraud, the very last thing they will ever do is pick up a phone to report it, on the basis that this may set in course a chain of events that ultimately damages the commercial interests of the company" (UK_3)*

The Food Industry Intelligence Network (FIIN), referred to above, provides another example of an industry network established to combat food fraud and threat (https://www.campdenbri.co.uk/news/fiin.php). Similar to Food Fortress, FIIN engagement with an independent third-party organisation to provide database management and analytical services ensures anonymity regarding data shared. The network also aims to engage with authorities and has intelligence agreements in place with Scottish and Irish authorities

Hence establishment of industry/supply chain networks and engagement with independent third parties to manage databases and provide data analytical services could go some way to addressing a reluctance among supply chain actors to share experiences. While this data may not be used directly for prosecution of perpetrators in the courts, it would support scanning the system providing a better impression of vulnerabilities.

When considering public stakeholders, in all European jurisdictions food crime units have been established and are linked to public authorities. The development of inter-disciplinary teams emerged as a key theme across these units. Thus while they represent single stakeholder activity, they have been built upon a mix of investigative, enforcement, business and scientific knowledge. The role of such units is clear as they offer intelligence gathering capability (including use of 'industry informants') and support prosecution of perpetrators; however they also engage with other agencies within and across jurisdictions, e.g. FSAI multi-agency food fraud network. Such multi-agency engagement (e.g. European Food Fraud Network) plays a vital role, however public-private partnerships have the ability to enhance system scanning and facilitate vulnerability assessment at firm, supply chain and national/international levels.

The establishment of the US Food Protection and Defense Institute in the University of Minnesota, as a Homeland Security Centre of Excellence, provides an interesting example of a public initiative that leverages university infrastructure. This Institute has developed close linkages with both industry and regulatory authorities at Federal and State levels, as well as policy-makers and NGOs. In pursuing their mission, the institute has been involved in the development of various tools and supports for industry (e.g. Intentional Adulteration Assessment Tool (IAAT) and FoodSHIELD - a web-based collaboration platform designed for the coordination, education, and training of those who protect and defend the global food supply), with more recent attention on harnessing the potential of data analytics for horizon-scanning and reporting, e.g. FIDES (Focused Integration of Data for Early Signals), a web application designed to fuse multiple streams of data to predict, monitor, and identify food system disruptions and adverse food events. Other universities have also been active in this space, for example global activities of the Food Fraud Initiative based in the University of Michigan and development of the SSAFE Vulnerability Assessment Tool by Wageningen UR and VU Amsterdam, The Netherlands, in collaboration with nine multinational companies and PwC. Hence such initiatives

harness expertise across public and private organisations and have resulted in the development of useful tools designed for industry as well as ongoing development of a body of knowledge in the field.

In addition, more permanent public-private initiatives may offer a useful infrastructure to support resource deployment and development of capability. Establishing the Food Confidence Taskforce, referred to earlier, presents an interesting example of a private-public partnership. This initiative by the Dutch Ministry of Health, Welfare & Sport and Ministry for Agriculture, in cooperation with the Netherlands Food and Consumer Product Safety Authority (NVWA) and industry representative groups (meat, dairy and animal feed sectors) was established in the aftermath of the horsemeat scandal. The Taskforce plan consists of 17 actions for both public and private sectors across three areas: (i) improve quality control systems with product safety and integrity requirements, (ii) surveillance, enforcement and sanctions, and (iii) communication and exchange of information.

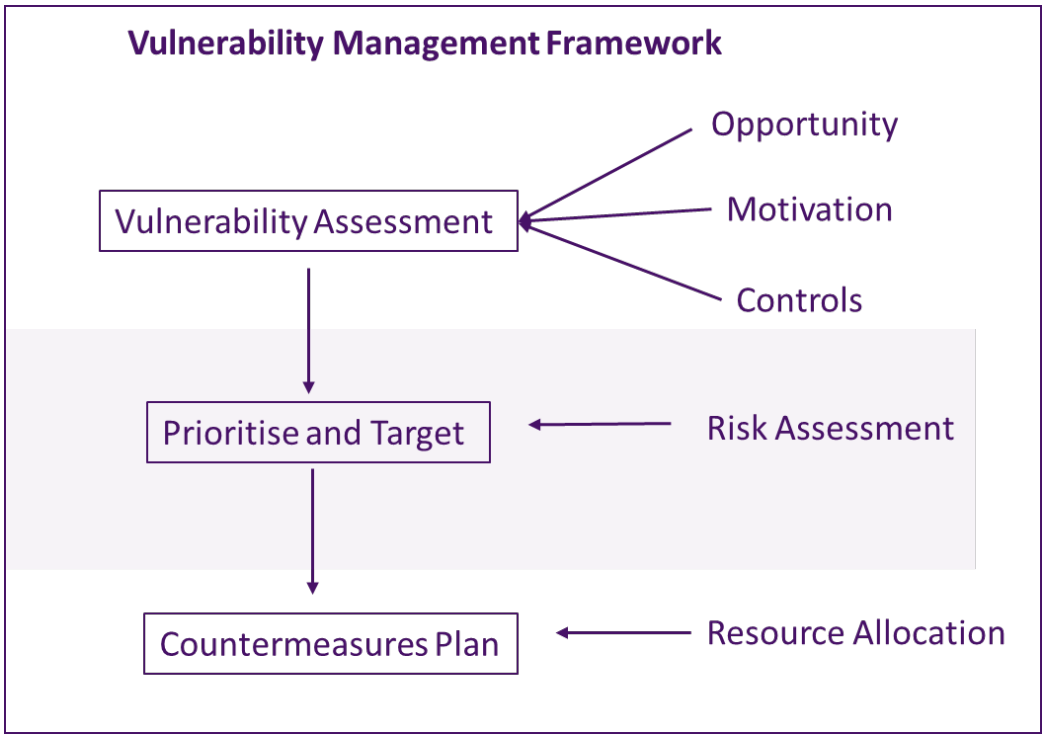
While private accreditation and standards (e.g. GFSI guidance and accreditation of standards; BRC, SQF, IFS, and FSSC standards) have played a key role, there is less evidence of public-private partnerships within the IoI. Furthermore, notwithstanding interaction between Food Safety Authorities/Food Crime units and reference by stakeholders to FIIN, there is a need for greater public-private initiatives in the IoI. Such pooled expertise and perspectives could support information sharing and knowledge building based on, for example, public actor horizon-scanning and sharing experiences of supply chain actors in this area, including incident data. Spink et al. (2016) offer some interesting suggestions in this regard, including a focus on key trade points (public authorities such as customs and excise at border crossings) and exchange of ownership points (from private enterprise) resulting in a more holistic appreciation of and intervention at key exchange points in the supply chain. Furthermore, the findings emphasise the need for national/state level response to food threats that arise from sources external to the food supply chain.

### Vulnerability management framework

An emerging approach to vulnerability management is evident across the literature and research conducted, as outlined in Table 3.1.

In recognition of the nature of intentional adulteration, approaches adopted across all regions have been informed by criminology. Hence approaches adopted consider the factors that lead to adulteration, both drivers and inhibitors. Such responses are evident from research output (e.g. van Ruth et al. (2017) identification of factors related to opportunities, motivations and control measures) and guidance from policymakers and regulators (e.g. FDA Guidance on FSMA Rule 7 - Mitigation Strategies to Protect Food Against Intentional Adulteration). This approach has informed the design of Vulnerability Assessment (VA) tools that require firms to consider each condition (opportunities, motivations and control measures) and related factors across product categories.

Figure 3.10 Vulnerability Management Framework




As illustrated in Figure 3.10, good practice suggests that such testing regimes should be based on vulnerability assessment at product/ingredient level and related prioritisation based on risk assessment. The use of a two-stage vulnerability assessment can enhance efficiency and effectiveness, as an initial quick scan assessment in stage one can identify areas that merit a more detailed second stage assessment. Furthermore, the changing nature of risks and ongoing developments in analytical techniques, points to the need to identify what went well and what did not, and learning from that:

> *"[I]t's all about reviewing what you do" (IOI_4)*

Hence building experience and knowledge of the conditions that creates opportunities for fraud and threats is of fundamental importance:

> *"The key now is that even with food defence, we can still look at past incidents, and look at what people did and why they did it. Every time there is a new incident, it's important for the food defence prevention strategy team, the food fraud prevention strategy team, to get together to say, 'With this new incident, is there something fundamentally different about the way we understand our problem?'" (US_2)*

Risk assessment plays a key role in progressing from assessment and mapping to planning and deployment:

> *"Some of the companies will have started off very well with these vulnerability assessments that mapped all their supply chains everywhere, all different locations in factories and all sites and then if you have a well-structured plan for the monitoring and at the same time the site covered that there are companies who are doing that" (NL_1)*

The capability of supply chain actors to adopt and operationalise such a framework emerges as a key theme. In this regard the complexity of the tools requires attention. The capacity of smaller companies emerges as a related theme. In this regard the experience and views of interviewees

support the findings from the online survey and highlight resource constraints of small and medium sized food companies:

> *"Medium and small companies have no salary for this. It's somebody's extra job. They are not trained in it" (US_1)*

While product/ingredient testing plays an important and can be used as a visible countermeasure, thus deterring perpetrators, analysis of experience across the jurisdictions studied indicate that supply chain actors need to couple testing regimes with supply chain design:

> *"If the QA manager can convince procurement usually what's then needed it's more than just having some checks but it may also be sometimes to cease activities or look for other suppliers. I know that some retailers have done that for meat, for instance, after the horsemeat affair, shortened the chains. Yes, that's also an option and probably more effective than just carrying out tests and they will try to circumvent anyway" (NL_1)*

Analysis of the IoI industry data indicates a particular focus on both product/ingredient testing and supplier auditing as proactive measures and punitive actions/additional requirements placed on suppliers as reactive measures. In this regard it is interesting to find that IoI interviewees raise supply chain issues, and to some extent cultural issues, that may give rise to food fraud/threat. Indeed, deeper analysis of the factors within each of the conditions reveal the key role of culture. For example, some respondents addressed the need to align expectations within and between food business:

> *"[H]aving shared objectives at a management level as well and having a structure that supports shared objectives. … [Referring to a particular incident] There were gaps between the functions, and then you had people on the shop floor who basically had a free reign to do what they wanted to do. There was too much scope for error" (IoI_6)*

Hence the culture that develops may be influenced by alignment of expectations, within the business and with customers (e.g. "open book accounting") and clear operating procedures. Such responses may address "sharp practices" (IoI_1) associated with businesses that are cutting corners, however more planned or deliberate fraud require different countermeasures, for example monitoring and targeted surveillance leading to testing and exposure (Spink et al., 2016).

# 4 Project conclusions

This study is the first on the IoI to explore various stakeholders' perceptions of the nature of the challenges presented by intentional adulteration of food and to investigate emerging strategies and practices to respond to such challenges. In addition, it considered these findings in the context of experiences and practices in four other OECD countries. The study identifies a range of VMIs adopted across these jurisdictions. Analysis of these informs the design of a VMF which may guide future VMI deployment in the IoI.

A number of underlying themes emerged from this analysis. The classification of countermeasures put forward by Spink et al. (2016) provides a useful organising framework to consider the nature and impact of these themes, as presented in Table 4.1 below.

Given the intentional motivation behind food fraud/threat it requires a different mind-set to that typically applied to food safety or quality. This thinking is evident in the adoption and use of vulnerability assessments, based on three conditions (opportunity, motivation and control measures), and supply chain mapping tools. A fundamental understanding of each of the three conditions is required to operationalise a VMF to greatest effect. Targeting and prioritising emerges as a key activity to support the movement from assessment to action (i.e. identification and deployment of relevant countermeasures). In this regard risk assessment is essential to assess potential impact and guide resource allocation. This applies to both food supply chain actors and regulators. For the latter, intelligence gathering is of fundamental importance. As this tends to identify a range of potential targets, the need to develop prioritisation methodologies is essential to guide resource allocation decisions and long-term success.

Two very different aspects of a recurring theme of 'reputation' are evident. One relates to the perpetrator and the other to the victim. Regarding the former, while typical fines which follow legal convictions and negative tests tend to have limited impact on motivation, evidence from some jurisdictions suggest that fines designed to recover ill-gotten gains may shift motivation and attractiveness to a much greater extent. It is likely that the reputational damage resulting from online publication of negative results has a strong impact and reduces motivation/attractiveness.

Potential reputational damage to the victim was found to impact negatively on willingness to share information. The more information shared the higher the level of detection of perpetrators, and therefore measures that ensure anonymity and build trust between various stakeholders are of particular value. In this regard, network initiatives that create a safe environment for information sharing were found to encourage networking among industry stakeholders and provide a mechanism to interact with other stakeholders, including regulators. Some of these industry-based networks were found to engage third party service providers to manage databases, data analysis and dissemination of test results; in this way anonymity regarding test results was ensured within the network. In some cases, these networks have put protocols in place to facilitate sharing test results, other data and information with regulatory authorities.

In addition to information-sharing, the use of data analytics was identified as an area of some potential, particularly with regard to pre-emptive measures based on targeting products/sources identified as susceptible. Horizon-scanning coupled with Machine Learning (ML) (or other quantitative techniques) is in a relatively early stage of development. In comparison, there has been considerable attention given to the development of databases that in turn draw on open source data (from regulatory authorities, commodity price data, etc.) as well as services that provide specific lists of susceptible products/sources in a timely manner. In the latter case, food supply chain actors would benefit from guidance on selection and use of such databases and capacity-building.

A range of expertise underpins the approaches discussed above. The interdisciplinary teams assembled by food crime units point to the nature of the challenge and hence the need for food science, business and legal perspectives. Further, multi-agency and public-private partnership initiatives provide necessary infrastructure to build and harness the expertise required to address challenges faced. Such partnerships offer considerable potential through access to data already assembled across the range of members (e.g. trade flows, commodity prices, production data/forecasts, test results, etc.) as well as expertise and perspectives that each can offer.

Industry initiatives that provide safe environments for information sharing leverage firm-centric response to an industry-wide response. As such these initiatives offer considerable value in their own right, but they can also form a key element of the overall 'institutional landscape', as they have the potential to link with other stakeholders, including regulators. In this context public-private partnerships offer a useful mechanism to pool the range of expertise required and make best use of resources.

Table 4.1: Key themes underpinning VMI countermeasures

| Theme | Detect | Deter | Prevent |
|---|---|---|---|
| Mind-set - conditions that give rise to fraud. | Vulnerability assessment and mapping identifies fraud/threat opportunities and motivations | Visibility of vulnerability assessment and mapping dissuades perpetrators | Addressing conditions (opportunities and control measures) for specific products/sources (based on prioritization) – i.e. shifts and disrupts |
| Prioritisation – based on risk assessment | Target products/ ingredients identified for testing | Increased likelihood of detection is a deterrent.<br>Visibility of testing dissuades perpetrators | Informs selection/ design of additional countermeasures (i.e. may shift/disrupt) |
| Reputation – from perpetrators' perspective | | Financial penalties have limited impact. Recovery of illegal gains has greater impact. Publication of illegal practice is a stronger deterrent. | |
| Collaboration – within and between stakeholder groups. | Measures to ensure anonymity and protocols that promote sharing negative test results and experiences. | | |
| Data analytics | Use of databases to detect likely targets based on attractiveness (motivation) to perpetrators. | | Pre-emptive measures that avoid specific products/sources (in addition to targeted surveillance and testing). |
| Expertise | Interdisciplinary teams required to support intelligence gathering, investigation and enforcement<br>Training of company and agency auditing personnel | | Increased probability of detection and professional collection of evidence to facilitate prosecutions acts as a deterrent |

# 5 Added value and anticipated benefits of the research

This project provides an evidence base to underpin the development of more resilient supply chain in IoI for the first time. As such, it provides an insight into future potential food threats and vulnerabilities and presents an opportunity to consider innovative solutions. In particular, it proposes targeted actions for the various responsible governmental, public and private agencies (e.g. policy-makers, regulators and industry) involved in developing resilient supply chains. Furthermore, the nature of research approach (specifically engaging stakeholders in the research process) contributed to raising awareness and knowledge about the issues and the final event provided a forum to discuss and debate the crucial actions that must be taken, on an island wide basis, to develop more resilient supply chains. The ongoing development of resilient food supply chains in the IoI is essential for economic (at individual firm, sector and national levels) and social (e.g. public health) reasons.

During the project, an international network of experts has been accessed by the project team. This network will continue to be leveraged to contribute to the knowledge base in Ireland on the theme of supply chain resilience through a related Teagasc-Musgrave funded PhD study (the PhD candidate will be registered in UCC). The industry network developed during this project will also contribute to directing this PhD study to be of maximum benefit to the industry and will facilitate effective dissemination and knowledge exchange activities.

# 6 References

A. T. Kearney and GMA. (2010), Consumer Product Fraud: Deterrence and Detection, Grocery Manufacturers Association, Washington, DC, available at: Http://www.gmaonline.org/downloads/wygwam/consumerproductfraud.pdf.

Acheson, D.W. (2007), "Vulnerability Assessment Tools", available at: http://www.ift.org/~/media/Knowledge%20Center/Science%20Reports/Conference%20Papers/GlobalFoodSafety_Acheson2.pdf (accessed 15 April 2019).

Adams, R.J., Smart, P. and Huff, A.S. (2017), "Shades of Grey: Guidelines for Working with the Grey Literature in Systematic Reviews for Management and Organizational Studies: Shades of Grey", International Journal of Management Reviews, Vol. 19 No. 4, pp. 432–454.

Appelhof, T. and Heuvel, R. van den (2011), "Inventory of private food law", in van der Meulen, B.M.J. (Ed.), *Private Food Law: Governing Food Chains through Contract Law, Self-Regulation, Private Standards, Audits and Certification Schemes*, Wageningen Academic Publishers, pp. 113–148.

Askew, K. (2018), "'Complex and unclear' safety system contributed to fipronil scandal, Dutch probe finds", *Foodnavigator.Com*, July, available at: https://www.foodnavigator.com/Article/2018/07/09/Complex-and-unclear-safety-system-contributed-to-fipronil-scandal-Dutch-probe-finds (accessed 29 July 2018).

Australian Associated Press. (2018), "Six strawberry brands recalled as $100,000 reward offered to catch needle saboteur", *The Guardian*, 14 September, available at: https://www.theguardian.com/australia-news/2018/sep/15/six-strawberry-brands-recalled-as-100000-reward-offered-to-catch-needle-saboteur (accessed 15 September 2018).

Baruch, Y. and Holtom, B.C. (2008), "Survey response rate levels and trends in organizational research", *Human Relations*, Vol. 61 No. 8, pp. 1139–1160.

Bieberstein, A. and Roosen, J., 2015. Gender differences in the meanings associated with food hazards: A means-end chain analysis. *Food quality and preference*, *42*, pp.165-176.

Black, C., Chevallier, O.P. and Elliott, C.T. (2016a), "The current and potential applications of Ambient Mass Spectrometry in detecting food fraud", *TrAC Trends in Analytical Chemistry*, Vol. 82, pp. 268–278.

Black, C., Haughey, S.A., Chevallier, O.P., Galvin-King, P. and Elliott, C.T. (2016), "A comprehensive strategy to detect the fraudulent adulteration of herbs: The oregano approach", Food Chemistry, Vol. 210, pp. 551–557.

BRC. (2018a), *Global Standard Food Safety Issue 8*, BRC Global Standards, available at: https://www.brcgsbookshop.com/bookshop/global-standard-food-safety-issue-8/c-24/p-414 (accessed 17 April 2019).

BRC. (2018b), "BRC Global Standard for Food Safety. F804a: Issue 8 Auditor Checklist and Site Self-Assessment Tool", BRC Global Standards, August, available at: https://www.brcglobalstandards.com/media/1055378/food-safety-issue-8-checklist-english.docx (accessed 17 April 2019).

Briner, R.B. and Denyer, D. (2012), "Systematic review and evidence synthesis as a practice and scholarship tool", in Rousseau, D.M. (Ed.), The Oxford Handbook of Evidence-Based Management, Oxford University Press, Oxford, UK, pp. 112–129.

BSI (2014), *PAS 96:2014: Guide to Protecting and Defending Food and Drink from Deliberate Attack*, BSI Standards Limited, London, UK, p. 44.

Callao, M.P. and Ruisánchez, I. (2018), "An overview of multivariate qualitative methods for food fraud detection", *Food Control*, Vol. 86, pp. 283–293.

Corini, A. and van der Meulen, B. (2018), "Regulating food fraud: Public and private law responses in the EU, Italy and the Netherlands", in Allison, G. and Ronald, H. (Eds.), *A Handbook of Food Crime: Immoral and Illegal Practices in the Food Industry and What to Do about Them*, Bristol: Policy Press.

Corrado, G. (2016), "Advances in DNA typing in the agro-food supply chain", *Trends in Food Science & Technology*, Vol. 52, pp. 80–89.

CSO. (2016), "Business Demography NACE Rev 2 by Activity, Employment Size, Year and Statistic", *CSO Statbank*, available at: https://www.cso.ie/px/pxeirestat/Statire/SelectVarVal/Define.asp?maintable=BRA11&PLanguage=0 (accessed 16 April 2019).

Dalziel, G.R. (2009), Food Defence Incidents 1950-2008: A Chronology and Analysis of Incidents Involving the Malicious Contamination of the Food Supply Chain, Centre of Excellence For National Security (CENS), S. Rajaratnam School of International Studies, Nanyang Technology University, Singapore, available at: http://www3.ntu.edu.sg/rsis/cens/publications/reports/RSIS_Food%20Defence_170209.pdf

Danezis, G.P., Tsagkaris, A.S., Camin, F., Brusic, V. and Georgiou, C.A. (2016), "Food authentication: Techniques, trends & emerging approaches", *Trends in Analytical Chemistry*, Vol. 85, pp. 123–132.

Deloitte ERM Services. (2013), *A Risk Intelligent Approach to Managing Global Supply Chains*, Deloitte Development LLC., available at: https://www2.deloitte.com/global/en/pages/governance-risk-and-compliance/articles/risk-intelligent-approach-managing-supply-chains.html (accessed 7 June 2018).

Elliott, C. (2014), Elliott Review into the Integrity and Assurance of Food Supply Networks – Final Report: A National Food Crime Prevention Framework, HM Government, London, UK.

Elliott, C. (2015), "China raises the food safety bar.", *The Grocer*, 21 November, pp. 21–21.

Ellis, D.I. and Goodacre, R. (2016), "Detecting food authenticity and integrity", *Analytical Methods*, Vol. 8 No. 16, pp. 3281–3283.

Ellis, D.I., Muhamadali, H., A. Haughey, S., T. Elliott, C. and Goodacre, R. (2015), "Point-and-shoot: rapid quantitative detection methods for on-site food fraud analysis – moving out of the laboratory and into the food supply chain", Analytical Methods, Vol. 7 No. 22, pp. 9401–9414.

European Parliament. (2002), *Regulation (EC) No 178/2002 of the European Parliament and of the Council of 28 January 2002 Laying down the General Principles and Requirements of Food Law, Establishing the European Food Safety Authority and Laying down Procedures in Matters of Food Safety*, available at: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32002R0178 (accessed 18 May 2018).

European Parliament. (2017), *Regulation (EU) 2017/625 of the European Parliament and of the Council of 15 March 2017*, p. 142.

European Commission. (2018), *The EU Food Fraud Network and the System for Administrative Assistance & Food Fraud Annual Report 2017*, Brussels, Belgium, available at: https://ec.europa.eu/food/sites/food/files/safety/docs/food-fraud_network_activity_report_2017.pdf (accessed 19 April 2018).

Fassam, L. and Dani, S. (2017), "A conceptual understanding of criminality and integrity challenges in food supply chains", *British Food Journal*, Vol. 119 No. 1, pp. 67–83.

FDA. (2007), *CARVER + Shock: Enhancing Food Defense*, U.S. Food and Drug Administration, Washington, D.C., available at: www.fda.gov/consumer/updates/carvershock061107.Consumer Health.Information.html (accessed 20 February 2018).

FSA and NSF. (2015), Risk Modelling of Food Fraud Motivation, available at: https://www.food.gov.uk/research/research-projects/risk-modelling-of-food-fraud-motivation-nsf-fraud-protection-model-intelligent-risk-model-scoping-project (accessed 25 April 2018).

FSAI (2019), "FSAI first with new DNA food scanning tool", 18 February, available at: https://www.fsai.ie/news_centre/press_releases/DNA_based_food_scanning_tool_18022019.html (accessed 5 April 2019).

Georgiou, C.A. and Danezis, G.P. (2015), "Elemental and Isotopic Mass Spectrometry", in Picó, Y. (Ed.), *Comprehensive Analytical Chemistry*, Vol. 68, Elsevier, pp. 131–243.

Global Food Safety Initiative (GFSI) 2014. *GFSI Position on Mitigating the Public Health Risk of Food Fraud*, available at: https://www.mygfsi.com/files/Technical_Documents/Food_Fraud_Position_Paper.pdf (accessed 28 April 2018).

Global Food Safety Initiative (GFSI), 2017. GFSI benchmarking requirements - GFSI guidance document version 7.1, available at http://www.mygfsi.com/files/Technical_Documents/BR_V7.1/Benchmarking_Requirements_v7.1_Part4.pdf, last accessed 23/10/18

Gossner, C.M.-E., Schlundt, J., Ben Embarek, P., Hird, S., Lo-Fo-Wong, D., Beltran, J.J.O., Teoh, K.N., et al. (2009), "The Melamine Incident: Implications for International Food and Feed Safety", *Environmental Health Perspectives*, Vol. 117 No. 12, pp. 1803–1808.

Gregson, N. and Crang, M. (2017), "Illicit economies: customary illegality, moral economies and circulation", *Transactions of the Institute of British Geographers*, Vol. 42 No. 2, pp. 206–219.

Hong, E., Lee, S.Y., Jeong, J.Y., Park, J.M., Kim, B.H., Kwon, K. and Chun, H.S. (2017), "Modern analytical methods for the detection of food fraud and adulteration by food category", *Journal of the Science of Food and Agriculture*, Vol. 97 No. 12, pp. 3877–3896.

Huff, A.G., Hodges, J.S., Kennedy, S. and Kircher, A. (2015), "Evaluation of the Food and Agriculture Sector Criticality Assessment Tool (FASCAT) and the Collected Data", *Risk Analysis*, Vol. 35 No. 8, pp. 1448–1467.

Huff, A.G., Kircher, A., Hoffman, J. and Kennedy, S. (2013), "The development and use of the Food and Agriculture Systems Criticality Assessment Tool (FASCAT)", *Food Protection Trends*, Vol. 33 No. 4, pp. 218–223.

Jack, B. (2018), "Food Fraud: Protecting European Consumers Through Effective Deterrence.", *European Public Law*, Vol. 24 No. 1, pp. 147–168.

Jijon, A. (2014), "Food Fraud: The Role of Standards and the Litigation Implications".

Jung, Y. and Kang, H., 2010. User goals in social virtual worlds: A means-end chain approach. *Computers in Human Behavior*, *26*(2), pp.218-225.

Karunathilaka, S.R., Yakes, B.J., He, K., Brückner, L. and Mossoba, M.M. (2018), "First use of handheld Raman spectroscopic devices and on-board chemometric analysis for the detection of milk powder adulteration", *Food Control*, Vol. 92, pp. 137–146.

Kleboth, J.A., Luning, P.A. and Fogliano, V. (2016), "Risk-based integrity audits in the food chain – A framework for complex systems", Trends in Food Science & Technology, Vol. 56, pp. 167–174.

Kolence, K.W. (1973), "The Software Empiricist", *SIGMETRICS Perform. Eval. Rev.*, Vol. 2 No. 2, pp. 31–36.

Kurtzweil, P. (1995), "Orange Juice Scheme Gone Sour", *FDA Consumer*, 1 January, available at: https://www.highbeam.com/doc/1G1-16224155.html (accessed 7 June 2018).

Layton, L. (2009), "House Approves Food-Safety Bill; Law Would Expand FDA's Power", The Washington Post, 31 July, available at: http://www.washingtonpost.com/wp-dyn/content/article/2009/07/30/AR2009073003271.html (accessed 9 May 2018).

López, M.I., Trullols, E., Callao, M.P. and Ruisánchez, I. (2014), "Multivariate screening in food adulteration: Untargeted versus targeted modelling", *Food Chemistry*, Vol. 147, pp. 177–181.

Lord, N., Flores Elizondo, C.J. and Spencer, J. (2017), "The dynamics of food fraud: The interactions between criminal opportunity and market (dys)functionality in legitimate business", *Criminology & Criminal Justice*, p. 1748895816684539.

Manning, L. (2016a), "Guest editorial: Food Integrity", *British Food Journal*, Vol. 119 No. 1, pp. 2–6.

Manning, L. (2016), "Food fraud: policy and food chain", Current Opinion in Food Science, Vol. 10 No. Supplement C, pp. 16–21.

Manning, L. and Soon, J.M. (2016), "Food Safety, Food Fraud, and Food Defense: A Fast Evolving Literature", Journal of Food Science, Vol. 81 No. 4, pp. R823–R834.

Marks, S. and Paravicini, G. (2017), "Parma ham probe shakes confidence in EU gourmet labels", POLITICO, 13 June, available at: https://www.politico.eu/article/parma-ham-probe-shakes-confidence-in-eu-gourmet-labels/ (accessed 18 May 2018).

McElwee, G., Smith, R. and Lever, J. (2017), "Illegal activity in the UK halal (sheep) supply chain: Towards greater understanding", Food Policy, Vol. 69 No. Supplement C, pp. 166–175.

Megget, K. (2018), "Mismatch in organic food data in raises fraud questions in US", Securing Industry, 8 March, available at: https://www.securingindustry.com/food-and-beverage/mismatch-in-organic-food-data-in-raises-fraud-questions-in-us/s104/a7087/ (accessed 9 March 2018).

van der Meulen, B.M.J. (2011a), "Private food law: The emergence of a concept", in van der Meulen, B.M.J. (Ed.), *Private Food Law: Governing Food Chains through Contract Law, Self-Regulation, Private Standards, Audits and Certification Schemes*, Wageningen Academic Publishers, pp. 29–50.

van der Meulen, B.M.J. (2011b), "The anatomy of private food law", in van der Meulen, B.M.J. (Ed.), *Private Food Law: Governing Food Chains through Contract Law, Self-Regulation, Private Standards, Audits and Certification Schemes*, Wageningen Academic Publishers, pp. 75–111.

Mitenius, N., Kennedy, S.P. and Busta, F.F. (2014), "Food Defense", in Motarjemi, Y. and Lelieveld, H. (Eds.), Food Safety Management, Academic Press, San Diego, pp. 937–958.

Modeland, V. (1988), "Juiceless baby juice leads to full-strength justice", *F.D.A. Consumer (USA)*, available at: http://agris.fao.org/agris-search/search.do?recordID=US8867351 (accessed 7 June 2018).

Mol, A.P.J. (2014), "Governing China's food quality through transparency: A review", Food Control, Vol. 43, pp. 49–56.

Moyer, D.C., DeVries, J.W. and Spink, J. (2017), "The economics of a food fraud incident – Case studies and examples including Melamine in Wheat Gluten", *Food Control*, Vol. 71, pp. 358–364.

NISRA. (2018), "Inter Departmental Business Register", *Northern Ireland Statistics and Research Agency*, 31 January, available at: https://www.nisra.gov.uk/statistics/business-statistics/inter-departmental-business-register (accessed 23 November 2018).

NSW Food Authority, (2018). Updated Alert: Strawberry contamination 21 September 2018, *New South Wales (NSW) Food Authority*. NSW, Australia http://www.foodauthority.nsw.gov.au/news/newsandmedia/departmental/2018-09-14-obsession-berrylicious-strawberries (accessed 29/11/18)

Ordoudi, S.A., Cagliani, L.R., Melidou, D., Tsimidou, M.Z. and Consonni, R. (2017), "Uncovering a challenging case of adulterated commercial saffron", *Food Control*, Vol. 81, pp. 147–155.

Pagnattaro, M.A. and Peirce, E. (2010), "If I Eat This Will it Kill Me? An Analysis of China's New Food Safety Law and Other Protections to Regulate Food Produced in China".

Pedersen, B., Gorzkowska-Sobas, A.A., Gerevini, M., Prugger, R., Belenguer, J., Maletti, M., Ljønes, M., et al. (2016), "Protecting our food: Can standard food safety analysis detect adulteration of food products with selected chemical agents?", *Trends in Analytical Chemistry*, Vol. 85, Part B, pp. 42–46.

PricewaterhouseCoopers. (2016), "PwC and SSAFE release tool for food companies to assess vulnerabilities", *PwC*, available at: https://www.pwc.ie/media-centre/press-release/2016/2016-pwc-ireland-ssafe-release-tool-food-companies-assess-vulnerabilities.html (accessed 23 February 2018).

Reid, L.M., O'Donnell, C.P. and Downey, G. (2006), "Recent technological advances for the determination of food authenticity", *Trends in Food Science & Technology*, Vol. 17 No. 7, pp. 344–353.

Reilly, A. (2018), *Overview of food fraud in the fisheries sector*, FAO, Rome, available at: www.fao.org/3/i8791en/I8791EN.pdf (accessed 19 April 2018).

Roberts, M.T. (2011), "A perspective on emerging law, consumer trust and social responsibility in China's food sector: The 'bleaching' case study", *Food and Drug Law Journal*, Vol. 66 No. 3, pp. 405–415.

van Ruth, S.M., Huisman, W. and Luning, P.A. (2017), "Food fraud vulnerability and its key factors", Trends in Food Science & Technology, Vol. 67, pp. 70–75.

Sauermann, H. and Roach, M. (2013), "Increasing web survey response rates in innovation research: An experimental study of static and dynamic contact design features", Research Policy, Vol. 42 No. 1, pp. 273–286.

Securing Industry. (2018), "Adulterated supplements use 'resold' barcodes to avoid enforcement", *Securing Industry*, 7 March, available at: https://www.securingindustry.com/food-and-beverage/adulterated-supplements-use-resold-barcodes-to-avoid-enforcement/s104/a7081/ (accessed 9 March 2018).

Sentandreu, M.Á. and Sentandreu, E. (2014), "Authenticity of meat products: Tools against fraud", *Food Research International*, Vol. 60, pp. 19–29.

Spink, J. (2014), "GFSI Direction on Food Fraud and Vulnerability Assessment (VACCP)", *Food Fraud Initiative*, 8 May, available at: http://foodfraud.msu.edu/2014/05/08/gfsi-direction-on-food-fraud-and-vulnerability-assessment-vaccp/ (accessed 28 April 2018).

Spink, J. (2018), "Glossary of Food Fraud-Related Terms (03/2018)", Food Fraud Initiative, 20 March, available at: http://foodfraud.msu.edu/2018/03/20/for-comment-glossary-of-food-fraud-related-terms-03-2018-please-participate/ (accessed 19 April 2018).

Spink, J., Elliott, C.T. and Swoffer, K. (2013), "Defining food fraud prevention to align food science and technology resources", Food Science and Technology (London), Vol. 27 No. 4, pp. 39–42.

Spink, J., Fortin, N.D., Moyer, D.C., Miao, H. and Wu, Y. (2016), "Food fraud prevention: Policy, strategy, and decision-making - Implementation steps for a government agency or industry", CHIMIA International Journal for Chemistry, Vol. 70 No. 5, pp. 320–328.

Spink, J., Moyer, D.C. and Whelan, P. (2016), "The role of the public private partnership in Food Fraud prevention—includes implementing the strategy", *Current Opinion in Food Science*, Vol. 10, pp. 68–75.

Spink, J., Ortega, D.L., Chen, C. and Wu, F. (2017a), "Food fraud prevention shifts the food risk focus to vulnerability",Trends in Food Science & Technology,Vol.62,pp.215–220.

Spink, J. and Moyer, D.C. (2017b), "Food Fraud Vulnerability Assessment and Prefilter for FSMA, GFSI, and SOX requirements", Food Safety Magazine, No. February-March, pp. 56–61.

Stadler, R.H., Tran, L.-A., Cavin, C., Zbinden, P. and Konings, E.J.M. (2016), "Analytical Approaches to Verify Food Integrity: Needs and Challenges", *Journal of AOAC International*, Vol. 99 No. 5, pp. 1135–1144.

Török, T.J., Tauxe, R.V., Wise, R.P., Livengood, J.R., Sokolow, R., Mauvais, S., Birkness, K.A., et al. (1997), "A Large Community Outbreak of Salmonellosis Caused by Intentional Contamination of Restaurant Salad Bars", Journal of the American Medical Association, Vol. 278 No. 5, pp. 389–395.

Varallo, C. (2018), "Food fraud update at EU level and Interpol/Europol Opson VII operation preliminary findings", *Food Law Latest*, 25 April, available at: https://foodlawlatest.com/2018/04/25/food-fraud-update-at-eu-level-and-interpol-europol-opson-vii-operation-preliminary-findings/ (accessed 27 April 2018).

Walker, G.S. (2017), "Food authentication and traceability: An Asian and Australian perspective", Food Control, Vol. 72, pp. 168–172.

WHO. (2002), Terrorist Threats to Food Guidance for Establishing and Strengthening Prevention and Response Systems, available at: http://apps.who.int/iris/bitstream/handle/10665/42619/9241545844.pdf?sequence=1&isAllowed=y (accessed 26 April 2018).

Wielogorska, E., Chevallier, O., Black, C., Galvin-King, P., Delêtre, M., Kelleher, C.T., Haughey, S.A., et al. (2018), "Development of a comprehensive analytical platform for the detection and quantitation of food fraud using a biomarker approach. The oregano adulteration case study", *Food Chemistry*, Vol. 239, pp. 32–39.

Zanoli, R. and Naspetti, S., 2002. Consumer motivations in the purchase of organic food: a means-end approach. *British food journal*, *104*(8), pp.643-653.

Zhang, W. and Xue, J. (2016), "Economically motivated food fraud and adulteration in China: An analysis based on 1553 media reports", Food Control, Vol. 67, pp. 192–198.

# 7 Glossary of acronyms

| | |
|---|---|
| AAC | Administrative Assistance and Cooperation |
| AFBI-NI | Agri-Food and Biosciences Institute (NI) |
| AI | Artificial Intelligence |
| ALERT | Assure, Look, Employees, Report, Threat |
| BRC | British Retail Consortium |
| BSI | British Standards Institution |
| CARVER | Criticality, Accessibility, Recuperability, Vulnerability Effect and Recognizability |
| CBL | Centraal Bureau Levensmiddelenhandel |
| CIES | International Committee of Food Chains |
| CGF | Consumer Goods Forum |
| CSO | Central Statistics Office |
| DAERA | Department of Agriculture, Environment and Rural Affairs |
| DAFM | Department of Agriculture, Food & the Marine |
| DHS | Department of Homeland Security |
| DNA | Deoxyribonucleic acid |
| DTU | DTU Technical University of Denmark |
| EC | European Community |
| EFFN | European Food Fraud Network |
| EFSA | European Food Safety Authority |
| EFFN | European Food Fraud Network |
| EMA | Economically-motivated adulteration |
| EU | European Union |
| FAO | Food and Agriculture Organization |
| FASCAT | Food and Agriculture Systems Criticality Assessment Tool |
| FCC | Food Chemicals Codex |
| FDA | Food and Drug Administration |
| FDF | Food and Drink Federation |
| FERA | Food and Environment Research Agency (Fera Science Ltd.) |
| FIDES | Focused Integration of Data for Early Signals |
| FIIN | Food Industry Intelligence Network |
| FSA | Food Standards Agency |

| | |
|---|---|
| FSAI | Food Safety Authority of Ireland |
| FSMA | Food Safety Modernization Act |
| FSSC | Food Safety System Certification |
| GATS | Global Agricultural Trade System |
| GFSI | Global Food Safety Initiative |
| GMA | Grocery Manufacturers Association |
| HACCP | Hazard Analysis and Critical Control Points |
| IAAT | Intentional Adulteration Assessment Tool |
| IDBR | Inter Departmental Business Register |
| IFS | International Featured Standards |
| IFT | Institute of Food Technologists |
| IoI | Island of Ireland |
| ISO | International Standard Organisation |
| IT | Information Technology |
| MDC | Main Distribution Centre |
| ML | Machine Learning |
| MS | Mass Spectrometry |
| NACE | Nomenclature générale des Activités Économiques dans les Communautés Européennes |
| NFCU | National Food Crime Unit |
| NI | Northern Ireland |
| NIFDA | Northern Ireland Food & Drink Association |
| NIGTA | Northern Ireland Grain Trade Association |
| NISRA | Northern Ireland Statistics Authority |
| OECD | Organisation for Economic Co-operation and Development |
| ORM | Operational Risk Management |
| PAS 96 | Publicly Available Standard 96 |
| PCICT | Product-Counterfeiting Incident Cluster Tool |
| PDO | Protected Designation of Origin |
| PGI | Protected Geographical Indication |
| PI | Principal Investigator |
| PRN | Priority Risk Number |
| QUB | Queens University Belfast |
| RAS-BICHAT | Rapid Alert System for Biological and Chemical Attacks and Threats |
| RASFF | Rapid Alert System for Food and Feed |
| RAT | Routine Activity Theory |

| | |
|---|---|
| RFID | Radio-frequency identification |
| RoI | Republic of Ireland |
| SPSS | Statistical Package for the Social Sciences |
| SQF | Safe Quality Food |
| SSAFE | Safe Supply of Affordable Food Everywhere |
| TACCP | Threat Assessment Critical Control Point |
| UCC | University College Cork |
| UCD | University College Dublin |
| UK | United Kingdom |
| USA | United States |
| USDA | U.S. Department of Agriculture |
| USC | United States Code |
| USP | U.S. Pharmacopeial Convention |
| VA | Vulnerability Assessment |
| VACCP | Vulnerability Assessment and Critical Control Points |
| VMIs | Vulnerability Management Initiatives |
| VMF | Vulnerability Management Framework |
| WHO | World Health Organization |

# 8 Appendices

## Appendix 1: Standards and protocols

### Introduction

TBD ... Accreditation, Certification, Defence Protocols ...

Finally, the discussion will consider a different set of standards and processes that were developed in the USA in the period after 2001 to analyse "food systems" as a response to food threats and the possibility of bio-terrorism.

### Accreditation Standards

The category of private law in Figure 1.6 comprised two layers, which were there termed here "Accreditation" and "Certification". Because of the proliferation of schemes at the Certification level in relation to food safety, and the consequent burden of regulation and auditing on businesses (Kleboth et al, 2016), efforts were initiated by industry actors to create more loosely-specified and more encompassing schemes, that would accredit the various "Standards" developed and promoted by the Certification bodies.

Most prominent among these are the Global Food Safety Initiative (GFSI), established in 2000, under the auspices of CIES, a group comprising most of the major international food retailers. One of the initiatives major goals was to reduce redundancy of audits, so that a producer could be "certified once, accepted everywhere" (Appelhof & van den Heuvel, 2011, p.116). A second accreditation body is the International Standard Organisation (ISO), which developed a food safety standard ISO 22000, supported by the multi-national food producers, i.e. the "big brand holders" (Appelhof & van den Heuvel 2011, p132). However, the retailers were slow to accept and adopt ISO 22000, and so a new organisation was established, The Foundation for Food Safety Certification (FSSC) and this organisation developed a broader standard, FSSC 22000[2], issued first in 2009. FSSC 2200 is among the standards accepted by GFSI.

#### ISO

The International Standards Organisation (ISO) is an independent NGO whose membership is composed of national standards bodies (161 of them in 2018). While the ISO has developed and published some twenty thousand standards across a wide variety of fields, the most influential current standard in relation to food processing is ISO 22000 on "Food safety management systems -- Requirements for any organization in the food chain". This was published in 2005, and enjoyed the support of the major international food processors. It was not however equally supported by the major retailers. Consequently, a further proposal was developed and merged with ISO 22000 to create FSSC 22000, managed by a new organisation the Foundation for Food Safety Certification (FSSC), and this standard was accredited by the GFSI in 2009. Details of FSSC 22000 are given below. Under ISO procedures standards should be reviewed and re-issued every 5 years, and ISO 22000 was so confirmed in 2009, but has not been since then, although the work stream is still active under the guidance of Technical Committee 34, whose scope is described as "food safety management systems, covering the food supply chain from primary production to consumption, human and animal foodstuffs as well as animal and vegetable propagation materials".

#### GFSI

GFSI is clearly the most influential of the accreditation schemes. In fact, van der Meulen (2011b, p.103) states that "GFSI is developing into the standard of standards". GFSI "benchmarks" certification

[2] FSSC 22000 integrated ISO 22000, and additional module that was called PAS 220, issued first in 2008.

schemes and endorses those which meet its "benchmarking requirements", or "key elements" (van der Meulen, 2011b, p.103). There have been several revisions to and editions of the GFSI requirements, described in "Guidance Documents", of which the most notable are the 6th Edition issued in January 2011, and the 7th Edition, issued in February 2017[3]. The 7th edition was the first to require conformance in relation to fraud and threat. It has separate, though parallel, requirements in relation to fraud and threats (defence), in each case requiring that any accredited standard should require an appropriate assessment and the development of planned responses. In addition, it is required that the standard should ensure that the "Food Defence Plan" and the "Food Fraud Mitigation Plan" be integrated into the organisation's Food Safety Management Plan.

**Table A1.1: GFSI Requirements on Food Defence and Food Fraud[4]**

| | | |
|---|---|---|
| Food Threats | Food defence threat assessment | The standard shall require that the organisation have a documented food defence threat assessment procedure in place to identify potential threats and prioritise food defence measures. |
| | Food defence plan | The standard shall require that the organisation has a documented plan in place that specifies the measures the organisation has implemented to mitigate the public health risks from any identified food defence threats. |
| Food Fraud | Food fraud vulnerability assessment | The standard shall require that the organisation has a documented food fraud vulnerability assessment procedure in place to identify potential vulnerability and prioritise food fraud mitigation measures. |
| | Food fraud mitigation plan | The standard shall require that the organisation has a documented plan in place that specifies the measures the organisation has implemented to mitigate the public health risks from the identified food fraud vulnerabilities. |

At the time of writing, there were 14 "Certification Programs" approved by GFSI:

1. Global Red Meat Standard (GRMS), 4th Ed.
2. Global Aquaculture Alliance Seafood
3. Global G.A.P. (Farm Assurance Scheme)
4. Canada G.A.P. (Farm Assurance)
5. BRC Global Standards (Issue 7)
6. BRC – Agents & Brokers
7. BRC – Packaging
8. BRC – Storage & Distribution
9. IFS Food Standard (Version 6)
10. IFS PAC-Secure (Version 1) (Packaging)
11. IFS Logistics (Version 2.1)
12. SQF (7th Edition)

[3] A minor revision, 7.1, was issued in April 2017, in order to increase alignment with FDA rules, and its interpretation of the FSMA (GFSI, 2017).

[4] Note that these requirements are listed in Part III of the Benchmarking Requirements, available at http://www.mygfsi.com/certification/benchmarking/gfsi-guidance-document/download-the-gfsi-benchmarking-requirements.html

13. FSSC 22000 (October 2011)
14. Primus GFS (v2.1, December 2011)

The first four of these schemes are designed for primary producers, and will not be discussed further here, as details are given in Appelhof & van den Heuvel (2011, pp.125-128). In addition, there are several variants e.g. of BRC's scheme adapted to Logistics or to Packaging and Packaging Materials, and the variants will not be discussed here in any detail.

The sections that follow discuss the five principal certification schemes approved by GFSI: IFS, BRC, SQF, FSSC, and Primus. In addition, some other organisations - notably SSAFE and USP - that are influential in standard setting will be discussed, although they are not formally certification providers in the GFSI framework.

## Certification Standards

### BRC Global Standards (7th and 8th Versions)

The British Retail Consortium (BRC) was founded in 1996 by the major UK-based food retailers, with the primary goal of reducing audit duplication (similarly to GFSI). The standards developed under the umbrella of that group have become globally-influential, and are now operated by a separate company[5], and issued as BRC Global Standards. The BRC scheme was approved by GFSI in 2008, and was one of the earliest to include requirements relating to food fraud or food defence (pre-dating the inclusion of general requirements in GFSI's benchmarking requirements). The 7th Edition was issued in January 2015, and strengthened requirements in relation to food fraud, in response in particular to the discovery of horsemeat in the beef supply chain in Europe, and that of melanin in milk-powder in China. These requirements are detailed in Section 5.4 "Product Authenticity, Claims and Chain of custody".

[5] LGC group, https://www.brcglobalstandards.com/about/

**Table A1.2: BRC (7th Edition) - Food Fraud (adapted from (British Retail Consortium (BRC), 2015))**

| Statement of Intent | |
|---|---|
| 5.4 | Systems shall be in place to minimise the risk of purchasing fraudulent or adulterated raw materials and ensure that all product descriptions and claims are legal, accurate and verified. Of traceability, identification and segregation of raw materials, intermediate and finished products shall be in place to ensure that all claims relating to provenance or assured status can be substantiated. |
| 5.4.1 | The company shall have processes in place to access information on historical and developing threats to the supply chain which may present a risk of adulteration or substitution of raw materials e.g. trade associations, government sources, private resource centres. |
| 5.4.2 | A documented vulnerability assessment shall be carried out of all raw materials to assess the potential risk of adulteration or substitution. This shall take into account: historical evidence of substitution or adulteration; economic factors; ease of access to raw materials through the supply chain; sophistication of routine testing to identify adulterants; nature of the raw material.<br>The vulnerability assessment shall be kept under review to reflect changing economic circumstances and market intelligence which may alter the potential risk. It shall be formally reviewed annually |
| 5.4.3 | Where raw materials are identified as being at particular risk of adulteration or substitution appropriate assurance and/or testing processes shall be in place to reduce the risk. |

In the draft of the 8th Version, which is currently under review, an additional requirement is made in relation to fraud that requires the company to have a documented supplier-approval procedure which include a risk assessment that considers (*inter-alia*) the "potential for adulteration or fraud" (BRC, 2017) [6].

Thus, the key processes required by the BRC standard are the execution of a vulnerability assessment and its documentation in a plan, together with the development of mitigation measures in order to reduce the risks arising from those vulnerabilities.

### FSSC 22000

FSSC 22000 was developed on the basis of the ISO standard, ISO 22000 (2005), which was not approved by GFSI because it was considered to lack prerequisite programs and also because of issues over the legal ownership of the scheme. An additional module, called PAS 220 was developed in 2008 to provide the prerequisite programs, and FSSC 22000 was issued as a combination of ISO 22000 and PAS 220 (ISO/TS 22002-1). FSSC 22000 was fully recognised by GFSI in 2010. Version 4.1 of the scheme was issued in mid-2017. The FSSC standard is structured along the lines of the ISO 9001 quality standard, but includes only requirements on food safety, that are in turn based on HACCP (Appelhof & van den Heuvel, 2011, p.132). In relation to food fraud and food defence, just as with BRC, FSSC 22000

[6] This is in clause 9.1.1 of the published BRC standard, Issue 8 (BRC, 2018a). This issue, which applies to all audits conducted after the beginning of January 2019, additionally added a section (4.2) on "Site Security and Food Defence", and therein defined those threats as "any deliberate attempt to inflict contamination or damage" where that includes "both internal and external threats" (BRC 2018b).

requires a vulnerability assessment, the identification of control measures, and the documentation of both of these in a prevention plan.

**Table A1.3: FSSC 22000 - Food Fraud & Defence (adapted from (FSSC, 2017))**

| **2.1.4.4 Food Fraud prevention** | |
|---|---|
| 2.1.4.4.1 Vulnerability assessment | 1) The organization shall have a documented and implemented vulnerability assessment procedure in place that: a) identifies potential vulnerabilities, b) develops control measures, and c) prioritizes them against the identified vulnerabilities. |
| | 2) To identify the vulnerabilities, the organization shall assess the susceptibility of its products to potential food fraud acts. |
| 2.1.4.4.2 Control measures | The organization shall put in place appropriate control measures to reduce or eliminate the identified vulnerabilities. |
| 2.1.4.4.3 Plan | 1) All policies, procedures and records are included in a food fraud prevention plan supported by the organization's Food Safety Management System for all its products. |
| | 2) The plan shall comply with applicable legislation |

### International Featured Standards (IFS)

IFS issues a large number of standards, and its standard for food (properly IFS Food) is now in version 6.1 (November 2017). IFS was established by a group of French and German food retailers, is headquartered in Berlin, and now operates globally, publishing its standards and documents in some twenty languages. The IFS Food standard includes provisions relating to Food Fraud, as detailed in the table below.

### Table A1.4: IFS Food (6.1) - Food Fraud (adapted from (IFS, 2017))

| **4.21** Food Fraud | |
|---|---|
| 4.21.1 | A documented food fraud vulnerability assessment shall be undertaken on all raw materials, ingredients, packaging and outsourced processes, to determine the risk of fraudulent activity in relation to substitution, mis-labelling, adulteration or counterfeiting. The criteria considered within the vulnerability assessment shall be defined. |
| 4.21.2 | A documented food fraud mitigation plan shall be developed, with reference to the vulnerability assessment, and implemented to control any identified risk. The methods of control and monitoring shall be defined and implemented. |
| 4.21.3 | In the event of increased risk, food fraud vulnerability assessment shall be reviewed.<br>Otherwise all vulnerability assessments shall be reviewed at least annually.<br>Control and monitoring requirements of the food fraud mitigation plan shall be reviewed and amended when applicable. |

## Safe Quality Food (SQF)

The SQF Code was first developed in Australia in 1994, but is managed by The Safe Quality Food Institute based in the USA, and is now in Edition 7.2 (July 2014). It is described as "a HACCP-Based Supplier Assurance Code for the food industry". It doesn't include any provisions explicitly about Food Fraud, but it has a mandatory provision relating to Food Defence (2.7.1), as in the table below.

### Table A1.5: SQF (7.2) - Food Defence (adapted from (SQF, 2018))

| **2.7.1** Food Defence | |
|---|---|
| 2.7.1.1 | The methods, responsibility and criteria for preventing food adulteration caused by a deliberate act of sabotage or terrorist-like incident shall be documented, implemented and maintained. |
| 2.7.1.2 | A food defence protocol shall be prepared and include:<br>i. The name of the senior management person responsible for food defence;<br>ii. The methods implemented to ensure only authorized personnel have access to manufacturing and storage areas through designated access points;<br>iii. The methods implemented to protect sensitive processing points from intentional adulteration;<br>iv. The measures taken to ensure the secure storage of raw materials, packaging, equipment and hazardous chemicals;<br>v. The measures implemented to ensure finished product is held under secure storage and transportation conditions; and<br>vi. The methods implemented to record and control access to the premises by employees, contractors, and visitors. |

Compared to the previous standards described, SQF is less prescriptive, specifying only the requirement for a plan and its documentation, but saying little about vulnerability assessment.

### Primus

PrimusGFS is a certification scheme developed by Primus Labs in the USA as a GFSI conformant version of their proprietary Primus food safety standard. As with SQF, PrimusGFS includes clauses on Food Defence, but not regarding Food Fraud.

**Table A1.6: PrimusGFS - Food Defence (adapted from ("Primus GFS", n.d.))**

| | |
|---|---|
| 1.8 Food Defence | a. The company should have a documented food defence policy that outlines the organization security controls necessary based on the risk associated with the operations.<br>b. The company should have available a current list of emergency contact phone numbers for company management, law enforcement and appropriate regulatory agencies.<br>c. Visitors to the company operations should be required to adhere to food safety and security policies. |

### Other certification schemes and organisations

#### Safe Supply of Affordable Food Everywhere (SSAFE)

SSAFE is a non-profit organisation founded in 2006, whose membership is comprised primarily of the major food manufacturers (e.g. Nestle, Kellogg, Cargill, Danone). It has established partnerships with many of the other key organisations in the field, such as GFSI, ISO, FSSC, and the FAO and WHO. Its importance in relation to Food Fraud is that it has developed an influential model for assessing vulnerability (in conjunction with WUR) and makes available IT tools for applying that model (work done in conjunction with WUR and PwC).

The SSAFE model of Food Fraud Vulnerability is based on the criminological theory of "Routine Activity Theory) (Cohen & Felson, 1979). In this model crime arises as "the outcome of the convergence in time and place of

1. motivated offenders;
2. suitable targets;
3. The absence of capable guardians." (van Ruth et al., 2017)

Van Ruth et al. (2017) argue that since most food fraud occurs in the supply chain, it is a corporate crime, and further that, because the role and position of "white-collar offenders" gives them specialised knowledge and privileged access, this facilitates opportunity for such criminal activity. Thus, the model is composed of three factors: opportunities; motivations; and control measures. The combination of the first two factors increases vulnerability, but vulnerability can be decreased by improved control measures (van Ruth et al., 2017, p. 71).

SSAFE's "food fraud vulnerability assessment tool" (detailed further later on) was developed through "an interactive and iterative process with representatives from the global food industry, retail, authorities and scientific community" (van Ruth et al., 2017) and comprises 50 questions (11 opportunities, 19 motivations, and 20 controls) and associated answer scales, so that the three factors of opportunities, motivations, and control measures can be quantified and assessed, e.g. using radar plots. (van Ruth et al., 2017, p.74, Fig 3).

#### British Standards Institute (BSI) (PAS 96 / TACCP)

The FSA and DEFRA developed a draft standard in coordination with the BSI in the form of a "PAS", or "Publicly Available Specification), PAS 96, on "protecting and defending food and drink from

deliberate attack". This was issued by the BSI in October 2014 (The British Standards Institution, 2014). Several multi-national food processors (e.g. Cargill, Heineken) together with some UK retailers (Tesco, Sainsbury) and food service providers (MacDonalds) were involved in the development of the specification. Agencies and specialists, such as the FDF and Leatherhead Food Research, were involved also.

The specific process described in this specification is named "TACCP" or "Threat Assessment Critical Control Point", and as the name suggests is modelled closely on HACCP. TACCP is considered to be "a risk management methodology, which aligns with HACCP, but has a different focus that may need input from employees from different disciplines, such as HR, procurement and/or security" (BSI 2014, p iii). It argues that many precautions taken to assure food safety are also likely to act as deterrents against fraud and threats, or to increase the likelihood of their detection., and so it makes sense to have a process that builds on a business's existing HACCP process (which is now required under legislation). It should also be noted that GFSI adopted the term "TACCP" from the BSI PAS, but applied it only to "behaviourally or ideologically motived" attacks (i.e. what this review has called threat), and coined the term "VACCP" by analogy with TACCP (and HACCP) to cover response to "economically motivated" attacks (what this review has called fraud) (Spink, 2014).

The model underlying TACCP, and the details of the process to be followed in implementing it will be discussed later under Implementation, but first the aims and actions involved in the process (BSI, 2014, p.9) are briefly outlined.

**Table A1.7: TACCP aims (adapted from BSI, 2014, p.9)**

| AIMS | |
|---|---|
| 1. | reduce the likelihood (chance) of a deliberate attack |
| 2. | reduce the consequences (impact) of an attack |
| 3. | protect organisational reputation |
| 4. | reassure customers, press and public that proportionate steps are in place to protect food |
| 5. | satisfy international expectations and support the work of trading partners |
| 6. | demonstrate that reasonable precautions are taken, and due diligence is exercised in protecting food |

**Table A1.8: TACCP actions (adapted from BSI, 2014, p. 9)**

| ACTIONS | |
|---|---|
| 1. | identify specific threats to the company's business |
| 2. | assess the likelihood of an attack by considering the motivation of the prospective attacker, the vulnerability of the process, the opportunity, and the capability they have of carrying out the attack |
| 3. | assess the potential impact by considering the consequences of a successful attack |
| 4. | judge the priority to be given to different threats by comparing their likelihood and impact |
| 5. | decide upon proportionate controls needed to discourage the attacker and give early notification of an attack |
| 6. | maintain information and intelligence systems to enable revision of priorities |

In general, therefore, the method in TACCP, is akin to that in SSAFE's method - to "think like the criminal"- or what the Food Defence systems call a "Red Team" approach. The PAS details this in two pairs of questions, the first pair focussed on the attackers' identity, motivations, and opportunities; and the second on the defenders' vulnerabilities and possible counter-measures (BSI 2014, p.9):

1. Who might want to attack us?
    a. How might they do it?
2. Where are we vulnerable?
    b. How can we remove (or reduce) those vulnerabilities?

### US Pharmacopeia (USP)

USP is a long-established non-profit organisation operating in the field of food quality and food safety. It develops and publishes the Food Chemicals Codex (FCC)[7], which specifies standards for food ingredients, methods for testing, and defines measures of "food-grade" that are widely referred to in legislation, particularly by the FDA in the USA, but also in other countries including Canada, Australia, New Zealand, and Brazil (Jijon, 2014). The FCC is published in a main section, and three supplements, and revised editions have been issued regularly – recently every two years, with the main section of the current edition (11th) issued in January 2018. Material on food fraud was added as an Appendix to the Third Supplement of the 9th edition in 2015, as a "guidance document" on "food fraud mitigation". The focus of the FCC's documents is solely on "intentional and economically motivated adulteration (EMA) of foods", and it is not intended to cover what has been termed here "extrinsic" adulteration (e.g. counterfeits, document fraud) nor does it cover food defence.

## Food defence protocols

A number of systems relating specifically to Food Defence, rather than Food Fraud, were developed under the sponsorship of departments and agencies of the US government beginning in the early 2000's. These do not fit clearly within the framework of accreditation and certification and have more of the characteristics of public law (legislation). They are not however legal texts and are more akin to the "guidance documents" encountered above, in that they suggest processes and procedures to be followed by regulators or food businesses to prevent and mitigate intentional (ideological or terrorist) threats to the food supply system. In many cases they take a "food systems" approach, rather than a "premises-based" approach, so that for example, vulnerabilities are assessed in relation to the potato-production system in Idaho, rather than at the level of an individual potato powder production facility.

### Assure, Look, Employees, Report, Threat (ALERT)

ALERT was a program aimed at raising awareness by food businesses, under the general guidance of the Public Health Security & Bioterrorism Preparedness Response Act of 2002. This has been superseded by the FSMA, and by the FDA's rules on preventive controls. While materials on ALERT are still available on the FDA training web-site, they note that they have not been updated to match the FSMA, and it is not clear whether ALERT is still considered current. This account is based on Acheson (2007).

[7] The FCC was published by the Institute of Medicine- now the Health and Medicine Division of the US National Academies of Sciences, Engineering, and Medicine - from 1966 until 2006. USP have been the publisher since the 6th Edition in 2006.

ALERT has 5 main principles:

1. What do you know about the foods arriving at your establishment? (Assure)
2. How do you maintain security in your establishment? (Look)
3. What do you know about people with access to your establishment? (Employees)
4. Do you keep track of food security issues in your establishment? (Report)
5. What would you do if you were threatened? (Threat)

Thus, ALERT was primarily an education program aimed at raising awareness among businesses and other actors in the food chain to the threat of intentional adulteration in the food chain, and towards a general approach to preventing and mitigating the effect of such activity.

### Operational Risk Management (ORM)

ORM was also developed by the FDA, in its office of regulatory affairs, as a general approach and process for risk identification and management within a food sub-system. The account here of ORM is based primarily on Acheson (2007). The program evaluated a set of "agents" or ingredients, a set of foods, (e.g. baby foods, soft drinks, yogurt), and a set of what they termed "food/agent scenarios", such as primary production, manufacturing, transportation, retail or food service – i.e. tiers in the food supply chain. The level of risk was quantified along the dimensions of severity and probability in a matrix (quadratic model). The ORM assessment identified four common attributes of higher-risk foods:

- Large Batches – large number of consumers
- Uniform Mixing – contaminate all servings in batch
- Short Shelf Life – minimal time to identify problem and intervene
- Ease of Access – accessible targets are more attractive

### Criticality, Accessibility, Recuperability, Vulnerability Effect and Recognisability (CARVER)+Shock

CARVER+Shock is another system developed by these agencies, and conceptually forming part of the same stream of research. It is designed to be applied at a state level, and to be used to analyse risk within a subsystem of the food supply system, not by an individual plant or supply-chain actor. Typically, in the CARVER process, teams representing actors at the various tiers of the subsystem supply-chain would be convened and would contribute the process of risk-assessment. CARVER was originally developed by the U.S. military to identify areas that may be vulnerable to an attacker, and the FDA and the USDA adapted it for the food and agriculture sector (FDA, 2007). A downloadable software tool was developed by the Institute of Food Technologists (IFT) and Sandia National Laboratories, working with the FDA, to support the CARVER process. The general approach in the CARVER process is aimed at determining the criticality of a particular food-system, with the goal of allocating resources, which may be scarce, to provide counter-measures for those food-systems that are determined to be most critical. The approach is described fairly concisely by Acheson (2007) as follows:

1. Break a food-system into its smallest pieces - "nodes" - in the farm to table continuum
2. Identify "critical nodes" – those that are the most likely targets for terrorist attack, by applying the analysis to each node
3. Develop countermeasures to reduce the risk at the critical nodes

The software tool begins with the development of a flow diagram of the food system being analyzed. It has a bank of some 100 questions about facilities and processes within the system. Scores are assigned based on the answers to the questions, where the attractiveness of a target is ranked on a

scale of 1 (lower) to 10 (higher) based on scales that have been developed for each of the seven CARVER attributes:

**Criticality:** What impact would an attack have on public health and the economy?

**Accessibility:** How easily can a terrorist access a target?

**Recuperability:** How well could a system recover from an attack?

**Vulnerability:** How easily could an attack be accomplished?

**Effect**: What would be the direct loss from an attack, as measured by loss in production?

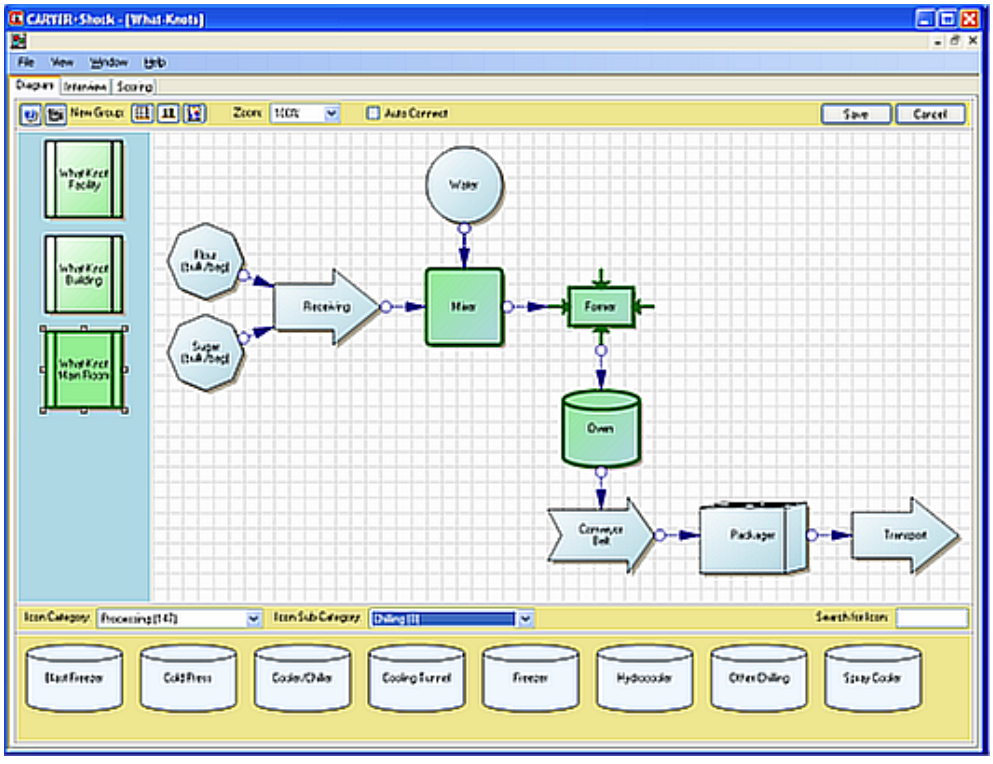
**Recognisability:** How easily could a terrorist identify a target?

The general model therefore is to "think like an attacker" with the intention of identifying weaknesses and putting counter-measures in place. These might include enhancements to physical security, personnel security, or process operations.

Note that CARVER+Shock was a later refinement of the basic CARVER model, in which "Shock" was an additional seventh attribute representing the "combined physical, public health, psychological, and economic effects of an attack".

A sample screen from the CARVER+Shock software is shown below:

**Figure A1.1: Screenshot of CARVER + Shock vulnerability assessment tool (Acheson, 2007)**




### Food and Agriculture Systems Criticality Assessment Tool (FASCAT)

FASCAT is a successor to CARVER, that was developed by the National Center of Food Protection and Defence at the University of Minnesota (Huff et al., 2013). Access to it is reserved to US government

agencies and employees. It takes the same general approach of analysing sub-systems at the level of a US state, and quantifying criticality.

The researchers who developed FASCAT have continued to refine the system – with three major versions, the most recent FASCAT 3.0 released in 2010. In addition, they have analysed the system and the data collected with a view to evaluating its quality and validity (Huff et al., 2013, 2015). Huff et al. (2013) suggest that it has two limitations:

> The use of subjective expertise to quantify probabilities of threats and of the magnitude of consequences;
>
> The possibility of a "group think" influencing those assessments.

However, they pointed out that validation really required a comparison of its predictions against actual outcomes, and so it could not really be validated unless some such threats actually occurred.

In a subsequent paper Huff et al. (2015) assessed FASCAT using quantitative analyses of data collected using the tool over the period 2010 to 2012, comparing variation in assessment scores by people in differing job types, comparing measurement of risk using FASCAT against similar measurements made using a process from the DHS, and also analysing which type of measures (threat, impact, consequence) had the most influence on the overall FASCAT criticality scores. They found that ratings of criticality varied significantly by job type, with food defence managers giving the lowest ratings and emergency managers about twice as high ratings. The threat of Intentional adulteration was not in fact identified as a significant contributor to criticality scores, whereas drought, pathogens, and foreign animal diseases were. Under consequences, loss of output and mass casualties were significant, whereas economic impacts were not. Considering factors included as "impact", it was found that large-scale loss of life or protracted loss of supply were significant predictors of overall criticality scores. Under second- and third-order effects, overall scores were significantly associated with "soft" factors such as loss of confidence, rather than more market-oriented ones, such as cost to government or costs resulting from litigation. They conclude that the inclusion of economic measures had limited value in differentiating the criticality of different food subsystems from one another (the goal of the FASCAT process). Finally, they analysed the contribution of different tiers in the supply chain and found that retail processing operations and non-refrigerated domestic processed foods were highly critical and remained so across regional variations.

## Appendix 2: Online survey

Because the survey was administered as an online web-based survey (developed and hosted using Qualtrics) "branch-logic" was used to minimize the number of questions shown to participants based on their answers to earlier questions. The question on process details (Q23) was shown only to those participants who answered "Yes, system in place and active" to the preceding question (Q22). The block of questions on "Incident Details" (Q26-Q31) was displayed only if the respondent answered in the affirmative to having encountered incidents in Q24.

The numbering in the listing of the questionnaire below corresponds to the numbering of items in Qualtrics, but some of these are informational graphics (e.g. Q1) or text (e.g. Q2). The total number of questions to which substantive responses could be made was 33, and the minimum (dependent on the branches taken) was 26.

### Survey questionnaire

Information and consent

Q1:

UCC
University College Cork, Ireland
Coláiste na hOllscoile Corcaigh

teagasc
Agriculture and Food Development Authority

**Q2: This study is conducted by a group of researchers based at University College Cork and at Teagasc, who are interested in food supply chain integrity, and specifically in intentional adulteration or intentional misrepresentation in the food supply chain. The study is funded by *safe*food, an all-Ireland body whose general remit is to promote awareness and knowledge of food safety and nutrition issues.**

The questionnaire takes approximately 20 minutes to complete.

**Consent:**

- Your participation in this survey is completely voluntary
  You may skip any question for any reason (although fully completed surveys are more valuable for our research).
- Respondents are anonymised in the data collected, and therefore no identifiable reference will be made to you or your company in the data collected or in our reports and publications
- Respondents cannot be connected to specific statements from the survey responses.
- The survey data will be kept securely at University College Cork, available only to the researchers.
- Your response to this questionnaire will be stored on Qualtrics' servers. Qualtrics operate to industry best-practice on security and privacy. Full details of Qualtrics' privacy and security policies and controls are available at https://www.qualtrics.com/privacy-statement/

Please do not hesitate to contact the researchers if you need any further information:

Department of Food Business & Development, Cork University Business School, University College Cork, Cork, Ireland

**Q3: I have read the information about the project and on consent, and I agree to participate in this research study:**

- ○ Yes
- ○ No

Demographics - you & your company

**Q4: Where are you (yourself) working?**

- ○ Northern Ireland
- ○ Republic of Ireland

**Q5: What is your role in this company?**

- ○ Owner/CEO/General Manager
- ○ Food Quality or Safety Manager
- ○ Production
- ○ Buyer
- ○ Other (please give your job title or a brief description of your role)

**Q6: Please specify the size of the company for which you work:**

- ○ Less than 10 employees
- ○ More than 10, but less than 50 employees
- ○ More than 50, but less than 250 employees
- ○ More than 250 employees

**Q7: Please specify on which levels of the food supply chain your company operates.**
**TICK AS MANY CHOICES AS ARE APPLICABLE. MULTIPLE CHOICES ARE ALLOWED.**

- ☐ Food Ingredients
- ☐ Processing (Intermediate Products)
- ☐ Processing (Consumer-Ready)
- ☐ Retail
- ☐ Food Service

**Q8: In what countries/regions is your company active?**

**TICK AS MANY CHOICES AS ARE APPLICABLE. MULTIPLE CHOICES ARE ALLOWED.**

| | Operations | Sales | Suppliers |
|---|---|---|---|
| Republic of Ireland | ☐ | ☐ | ☐ |
| Northern Ireland | ☐ | ☐ | ☐ |
| Rest of UK | ☐ | ☐ | ☐ |
| Rest of EU | ☐ | ☐ | ☐ |
| Europe, outside of EU | ☐ | ☐ | ☐ |
| USA | ☐ | ☐ | ☐ |
| Rest of World | ☐ | ☐ | ☐ |

**Q9: What types of products does your company produce?**

**TICK AS MANY CHOICES AS ARE APPLICABLE. MULTIPLE CHOICES ARE ALLOWED.**

- [ ] Fruit, Vegetables, Nuts
- [ ] Ambient Foods
- [ ] Oils & Fats
- [ ] Dairy - Milk, Butter, Cheese, or Ice Cream
- [ ] Raw Red Meat (inc. Pork)
- [ ] Raw Poultry
- [ ] Raw Fish Products
- [ ] Liquid Egg
- [ ] Egg
- [ ] Raw Prepared Products (Meat or Vegetarian)
- [ ] Raw Cured Meat or Fish
- [ ] Cooked Meat Products
- [ ] Dried Food or Ingredients
- [ ] Spices, Condiments, or Seasonings
- [ ] Ready Meals, Sandwiches, or Desserts
- [ ] Bakery
- [ ] Confectionery
- [ ] Cereals or Snacks
- [ ] Jams, Preserves, or Spreads
- [ ] Low/High Acid Foods in Cans or Glass
- [ ] Alcoholic Drinks or Brewed/Fermented Products
- [ ] Beverages
- [ ] Other (please describe)

## Prevalence (opinions)

**Q10: The following questions ask your opinions about adulteration and misrepresentation in food products. For our purposes these terms are defined as follows:**

***Adulteration*** *means the intentional substitution or addition of a substance in a product for the purpose of increasing the apparent value of the product or reducing the cost of its production, or to cause harm.*

***Misrepresentation*** *means in general a false or misleading label - for example counterfeit labels, up-labeling (a label that designates a higher quality product than is in the package), incorrect manufacturers, or incorrect country of origin.*

**Q11: In your opinion, in the food supply chain in general, do you think:**

| | Very Infrequent | Infrequent | Occasional | Frequent | Very Frequent |
|---|---|---|---|---|---|
| intentional adulteration is ... | ○ | ○ | ○ | ○ | ○ |
| intentional misrepresentation is ... | ○ | ○ | ○ | ○ | ○ |

**Q12: To what extent do you agree or disagree with each of the following statements?**

| | Strongly agree | Somewhat agree | Neither agree nor disagree | Somewhat disagree | Strongly disagree |
|---|---|---|---|---|---|
| Adulteration/misrepresentation issues are one of the major risks my company faces | ○ | ○ | ○ | ○ | ○ |
| Adulteration/misrepresentation issues are a growing problem in our sector | ○ | ○ | ○ | ○ | ○ |
| Adulteration/misrepresentation issues are a growing problem in Ireland | ○ | ○ | ○ | ○ | ○ |

**Q13: Which, in your opinion, is the more serious problem?**

- ○ Adulteration for economic gain
- ○ Adulteration for malicious or ideological reasons
- ○ Equally
- ○ Don't Know

**Q14: Which of adulteration for economic gain, or adulteration for malicious or ideological reasons, is more likely to be carried out by each of the following types of actors?**

| | Adulteration for economic gain | Adulteration for malicious or ideological reasons |
|---|---|---|
| Insider (inside your company) | ○ | ○ |
| Direct Supplier | ○ | ○ |
| Your supplier's supplier | ○ | ○ |
| Competitor | ○ | ○ |
| Organised Criminals | ○ | ○ |
| Terrorists | ○ | ○ |

**Q15: To what extent do you think each of the following food product categories are susceptible to adulteration/misrepresentation?**

| | Very Highly susceptible | Highly susceptible | Susceptible | Minimally susceptible | Not at all susceptible |
|---|---|---|---|---|---|
| Meat and meat products | ○ | ○ | ○ | ○ | ○ |
| Fish and seafood products | ○ | ○ | ○ | ○ | ○ |
| Dairy products (inc. milk powder) | ○ | ○ | ○ | ○ | ○ |
| Fruit and vegetables (non-organic) | ○ | ○ | ○ | ○ | ○ |
| Nuts and nut products | ○ | ○ | ○ | ○ | ○ |
| Fruit Juices | ○ | ○ | ○ | ○ | ○ |
| Herbs & Spices | ○ | ○ | ○ | ○ | ○ |
| Flavours | ○ | ○ | ○ | ○ | ○ |
| Coffee | ○ | ○ | ○ | ○ | ○ |
| Honey | ○ | ○ | ○ | ○ | ○ |
| Olive Oil | ○ | ○ | ○ | ○ | ○ |
| Prepared and Ready meals | ○ | ○ | ○ | ○ | ○ |
| Alcoholic Drinks & Beverages | ○ | ○ | ○ | ○ | ○ |
| Organic Products | ○ | ○ | ○ | ○ | ○ |
| Products with special claims of origin or process (e.g. "free-from", "Halal") | ○ | ○ | ○ | ○ | ○ |

**Q16: For the production categories in which you operate, how would each of the following increase or decrease someone's motivation or opportunity to adulterate or to misrepresent a product?**

| | Strongly Increase | Increase | Neither Increase nor Decrease | Decrease | Strongly Decrease |
|---|---|---|---|---|---|
| Simplicity of adulteration/misrepresentation | ○ | ○ | ○ | ○ | ○ |
| Availability of knowledge and/or technology to adulterate/misrepresent | ○ | ○ | ○ | ○ | ○ |
| Easy availability and low cost of test/detection methods | ○ | ○ | ○ | ○ | ○ |
| High security on access to materials during production | ○ | ○ | ○ | ○ | ○ |
| Steady pricing of ingredient or final product (i.e. no price spikes) | ○ | ○ | ○ | ○ | ○ |
| High value of ingredient or final product (e.g. vanilla, manuka honey) | ○ | ○ | ○ | ○ | ○ |
| Differences in pricing of ingredient across countries | ○ | ○ | ○ | ○ | ○ |
| Differences in business culture and governance across countries | ○ | ○ | ○ | ○ | ○ |
| Financial difficulties in producer's business | ○ | ○ | ○ | ○ | ○ |
| High level of demand for product | ○ | ○ | ○ | ○ | ○ |
| Financial pressure on suppliers | ○ | ○ | ○ | ○ | ○ |
| Transparency of supply chain and security of audit trail | ○ | ○ | ○ | ○ | ○ |
| Short or local supply chain | ○ | ○ | ○ | ○ | ○ |

## Awareness and practices

**Q17: The following question lists some well-known incidents of adulteration/misrepresentation of food that occurred in past years. For each, please indicate your awareness of it. And - based on your own experience and knowledge - please estimate how profitable or effective you think it might be for the perpetrator, and how likely you think you it would be detected today.**

| | I am aware of this incident | | | How profitable or effective would it be? | | | How likely to be detected? | |
|---|---|---|---|---|---|---|---|---|
| | Aware | Not Aware | Don't Know | Highly | Moderately | Little/Not at all | Likely | Unlikely |
| Sudan 1 Dye in Chili Powder | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ |
| Melamine (melanin) in Milk | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ |
| Pomegranate Juice diluted with grape or pear juice, sugar etc. | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ |
| Horsemeat in beef products | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ |
| Soybean and corn fraudulently mislabelled as "USDA Organic" | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ |
| Ham labelled as "Parma", but not produced in accordance with brand rules | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ |
| Falsifying data-stamps on eggs to intentionally spread salmonella | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ |

**Q18: For each of the following certification schemes, please indicate whether your company has that certification, is in the process of preparing or applying for it, or whether you personally have knowledge of it.**

| | Has Certification | Preparing or Applying for Certification | Personally aware, but no plans to apply | Not aware / Don't Know |
|---|---|---|---|---|
| BRC (BRC Global Standards) | ○ | ○ | ○ | ○ |
| SQF | ○ | ○ | ○ | ○ |
| IFS | ○ | ○ | ○ | ○ |
| ISO/FSSC 22000 | ○ | ○ | ○ | ○ |

**Q19: Does your company have any other relevant certification, or is applying for it? If so, please name it, or describe it briefly:**

**Q20: Do you consult any of the following adulteration/misrepresentation databases?**

| | Yes, regularly | Yes, occasionally | No, never | Not aware / Don't Know |
|---|---|---|---|---|
| EU RASFF (Rapid Alert System for Food and Feed) | ○ | ○ | ○ | ○ |
| FERA Horizon Scanning | ○ | ○ | ○ | ○ |
| USP Food Fraud Database | ○ | ○ | ○ | ○ |
| Commodity Price Indicators (e.g. USDA-GATS, UN-COMTRADE) | ○ | ○ | ○ | ○ |

**Q21: Do you consult any other database or source of market information on adulteration/misrepresentation? Please name or describe below:**

**Q22: Does you company currently have systems or processes in place to deal specifically with adulteration/misrepresentation?**

- ○ Yes, system in place and active
- ○ Not yet, but system being put in place
- ○ No, but considering doing so
- ○ No, and no current plans

## Process details

**Q23: Which, if any, of the following processes or methods do you currently use to protect your company against adulteration/misrepresentation?**

**TICK AS MANY CHOICES AS ARE APPLICABLE. MULTIPLE CHOICES ARE ALLOWED.**

- ☐ Specialised Testing Methods and Protocols (e.g. spectroscopy, DNA typing)
- ☐ Risk Management that incorporates Food Fraud and Threat
- ☐ Vulnerability Assessments (e.g. SSAFE Tool)
- ☐ Adherence to GFSI-accredited standards
- ☐ Intelligence gathering (e.g. using RASFF, participation in industry networks)
- ☐ Paid subscription to commercial adulteration/misrepresentation database (e.g. USP, FERA)
- ☐ Outsourced surveillance and intelligence gathering
- ☐ Site Security
- ☐ Employee vetting
- ☐ Supplier certification requirements
- ☐ Supplier auditing or inspections
- ☐ Outsourced or 3rd-party Auditing for adulteration/misrepresentation
- ☐ Purchasing policy (e.g. direct supply, long-term relationships)
- ☐ Other (please describe):

## Incidents

**Q24: Over the past 3 years, could you give an estimate of approximately how frequently your company has encountered adulteration/misrepresentation incidents, either directly or through your suppliers?**

- ○ More than once a year
- ○ No more than once a year
- ○ No more than once or twice in the period
- ○ Never
- ○ Don't Know

## Incident details

**Q25: In the next group of questions, please select the descriptions below which best fit your understanding of the incident, for the most recent one of those incidents.**

**Q26: Do you consider it to have been a fraud (economically-motivated) or a threat (malicious or ideological/political)?**

- ○ Fraud (economically-motivated)
- ○ Threat (malicious or ideological/political)

**Q27: If the perpetrator was identified, what sort of perpetrator would you consider best describes them?**

- ○ Supplier cutting corners
- ○ Supplier deliberately and rationally committing fraud
- ○ Organised crime
- ○ Malicious or disaffected employee/ex-employee
- ○ Ideologically or politically-motivated perpetrator

**Q28: Where geographically was the perpetrator located relative to your own company?**

- ○ Within Island of Ireland (Republic or Northern Ireland)
- ○ UK
- ○ Within EU (excluding UK)
- ○ Outside EU

**Q29: How was the incident detected?**

**AS MANY CHOICES AS ARE APPLICABLE. MULTIPLE CHOICES ARE ALLOWED.**

- ☐ Own testing or auditing
- ☐ Supplier testing or auditing
- ☐ Third-party testing or auditing
- ☐ Whistleblower
- ☐ Public Authorities or Regulators
- ☐ Customer or Consumer testing or alert

**Q30: How did you respond to the incident?**

**TICK AS MANY CHOICES AS ARE APPLICABLE. MULTIPLE CHOICES ARE ALLOWED.**

- ☐ Recalled product
- ☐ Alerted authorities
- ☐ Enhanced product testing
- ☐ Enhanced audit or inspection of suppliers
- ☐ Delisting supplier
- ☐ Undertook public-relations or reputation-management exercise
- ☐ Other (please describe):

**Q31: How do you think you could improve your systems or processes so as to prevent or respond to such an incident in the future?**

Expectations (opinions)

**Q32: Who do you think has the most important role in helping prevent incidents of fraud (economically-motivated adulteration/misrepresentation) or threat (malicious or ideological/political adulteration/misrepresentation in the future?**

**RANK YOUR TOP THREE (3) CHOICES IN ORDER, FROM MOST IMPORTANT (1) TO LEAST IMPORTANT (3). YOU NEED ONLY RANK AS MANY AS YOU WISH.**

- _____ Employees
- _____ Food Safety and Quality Team
- _____ Management
- _____ Auditors
- _____ Individual producer or processor businesses
- _____ Industry representative bodies (e.g. NIFDA, IBEC)
- _____ Accreditation/Certification organisations (e.g. GFSI, BRC)
- _____ Regulators (FSAI, FSA-NI)
- _____ National Government
- _____ EU Commission & Legislators

**Q33: Which of the following practices do you think are the most promising developments for tackling food fraud and threats?**

**RANK YOUR TOP THREE (3) CHOICES IN ORDER, FROM MOST IMPORTANT (1) TO LEAST IMPORTANT (3). YOU NEED ONLY RANK AS MANY AS YOU WISH.**

_____ Publicly-funded food fraud databases

_____ Private (fee-based) food fraud databases

_____ Formal information sharing networks

_____ Informal, industry-specific, information sharing forums

_____ Shared testing services

_____ More advanced testing and detection

_____ Better traceability technologies

_____ Improved enforcement of laws and regulations

_____ Enhanced regulatory capability

_____ New laws and stiffer penalties on conviction

**Q34: How do you rate each of the following new technologies as aids in fighting food fraud and threats?**

| | Highly promising | Somewhat Promising | Slightly Promising | Not at all Promising | Don't Know / No Opinion |
|---|---|---|---|---|---|
| Handheld rapid testing devices (e.g. Raman spectrometers) | ○ | ○ | ○ | ○ | ○ |
| Active and intelligent packaging | ○ | ○ | ○ | ○ | ○ |
| DNA barcoding | ○ | ○ | ○ | ○ | ○ |
| Edible tags | ○ | ○ | ○ | ○ | ○ |
| 3D-printed smart caps | ○ | ○ | ○ | ○ | ○ |
| "Big Data" and other computational tools for data analysis | ○ | ○ | ○ | ○ | ○ |
| RFID (traceability) | ○ | ○ | ○ | ○ | ○ |
| Blockchain (distributed ledger technology) | ○ | ○ | ○ | ○ | ○ |
| Smart contracts | ○ | ○ | ○ | ○ | ○ |

**Q35: Are there any new technologies (not listed above) that you consider to have significant promise as aids in fighting food fraud and threats?**

**Q36: In your own sector which, if any, companies do you consider to be the leaders in responding to food fraud and threats?**

**Q37: What do you consider to be the most important dangers and costs that food fraud and threats pose to your business?**

**RANK IN ORDER FROM MOST IMPORTANT (1) TO LEAST IMPORTANT (5). YOU NEED ONLY RANK AS MANY AS YOU WISH.**

_____ Food safety dangers to human consumers

_____ Direct economic consequences in lost business, product recalls etc.

_____ Indirect economic consequences in lost contracts, reputation etc.

_____ Legal criminal consequences for the company e.g. prosecution, fines etc.

_____ Legal criminal consequences for directors or employees e.g. prosecution, custodial sentences etc.

**Q38: Briefly describe the issue or situation, if any, that causes you the greatest worry about your company's vulnerability to food fraud or threats:**

**Thank you for taking the time to complete this survey. Your response has been recorded.**

# Appendix 3: Survey methods

## Sample and coverage

The sample frame had exactly 1,000 contacts, 750 in the RoI and 250 in NI[8]. Using data from the CSO's Business Demography series (BRA11), which is based on VAT registrations, there were 1,894 food or beverage (NACE Codes 10 and 11) producers in the RoI[9]. Data from NISRA's Inter Departmental Business Register (IDBR) which similarly is based on VAT registrations, shows that there were 455 food or beverage producers in NI[10]. The sample frame therefore covered 39.6% of food & beverage producers in the RoI and 54.9% in NI. Coverage was therefore not dissimilar in the two territories, and overall represented 42.6% of the population of food & beverage manufacturers in the IoI.

### Responses

At the time the survey closed on 27th September, there were a total of 186 responses recorded in Qualtrics (118 in the RoI, 31 in NI, and 37 unspecified). Of these we accepted 176 as valid[11] (117 in the RoI, 31 in NI, and 28 unspecified.

### Response rates

The overall response rate was 17.6%, but it was slightly higher in the RoI than in NI. We recorded 117 respondents located in the RoI, 31 in NI, and another 28 who skipped answering that question (although they continued with the survey). This suggests that quite a few respondents felt some sensitivity about answering this question, or possibly that the question wording was in some way unclear. These non-respondents complicate the calculation of separate response rates for the RoI and NI. However, if we assume that non-response is uniformly distributed between the two territories, then weighting by the original 75%/25% distribution, out of the 28 non-respondents, 21 are placed in the RoI and 7 in NI. The adjusted frequencies are then 138 in the RoI and 38 in NI, and the corresponding response rates are 18.4% in the RoI and 15.2% in NI. Both are in the generally accepted range for surveys of higher management and similar organisational representatives (Baruch and Holtom, 2008), and especially for web-based surveys (Sauermann and Roach, 2013) and are not dissimilar to one another. Relative to the Business Register data in the RoI and NI, our (adjusted) numbers of respondents represent 7.3% of the relevant population of businesses in the RoI and 8.4% of those in NI.

As a point of comparison, the study done in 2015 by NSF for the FSA in the UK resulted in 91 responses (FSA and NSF, 2015). Its sample frame was all those processors and manufacturers in the FSA's database and, in addition, respondents were invited to pass the survey on to their suppliers. The NSF/FSA report doesn't give numbers for those in the FSA database nor for how many more were included from the supply-chain, so that we can't calculate a response rate. However, the ONS's "UK Business – Activity, Size, and Location" database gives 4,135 food or beverage producers in England, suggesting that the NSF survey reached 2.2% of the relevant population of businesses[12].

---

8 There may have been some additional invites via NIFDA in NI, but most likely few if any.

9 Private communication from the CSO, giving breakdown between NACE codes 10, 11, and 12.

10 Table 1.11 in IDBR 2016 appendix.

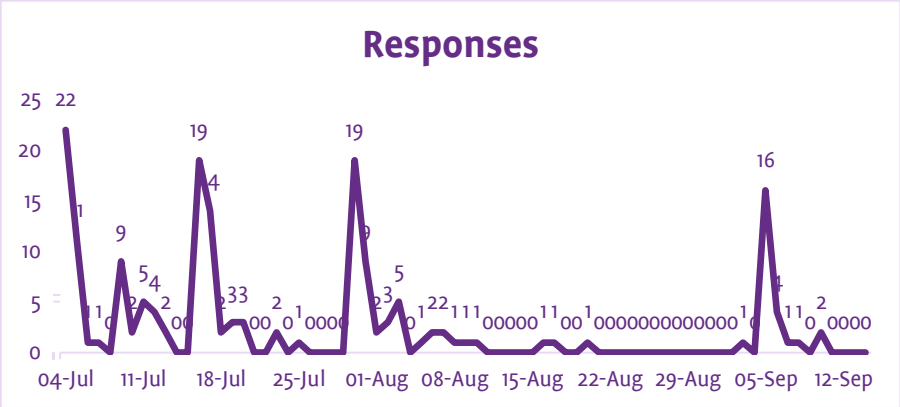
11 A response was considered invalid and excluded if lees than 1 minute was spent answering, or if no substantive questions were answered.

12 This database lists only 190 such businesses in NI, much fewer than the 455 obtained from the IDBR. This is because it doesn't include businesses operating in NI, but whose VAT registration is in another part of the UK (England and Wales, or Scotland).

### Responses over time – trend

The trend over time is shown in Figure A3.1 below.

**Figure A3.1: Response trend over time (July 4th to Sept. 14th, 2018)**

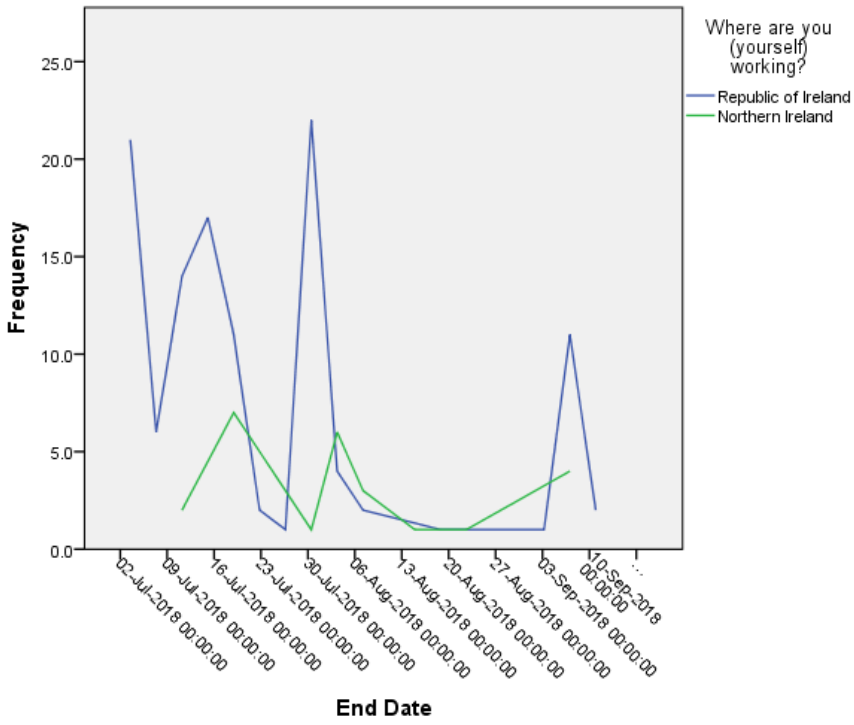



Responses peaked when the survey was first sent out, and again after each of our three reminder letters. Responses were very sparse during the last 3 weeks of August (holiday period). The reminders however were effective and important. The trends in RoI and NI were not distinctly different (Figure A3.2), except that there was no initial group of responses in NI (because we didn't send it out there until a little later)

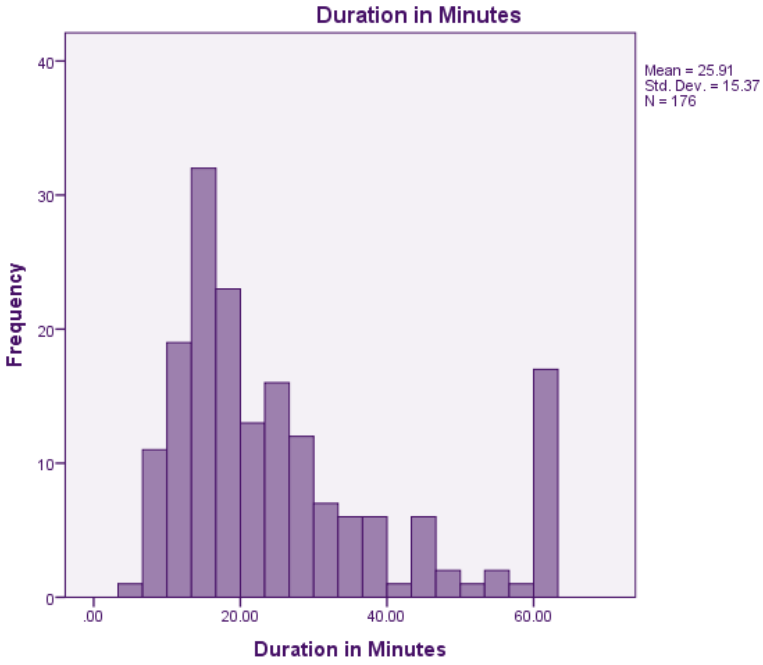
### Response duration

Because a respondent could leave a part-completed survey open (e.g. overnight) and return to complete it at a later time, some of the durations are quite lengthy (Figure A3.3). Therefore, in order to make the graphs and stats in this section useful we set upper outliers to be 60 minutes (1 hour). The median response time is just over 20 minutes, which is within reasonable quality guidelines for completion times, and closely matches the guidance given in the instructions ("approximately 20 minutes to complete").

### Figure A3.2: Responses in RoI versus NI




### Figure A3.3: Questionnaire duration



# Appendix 4: Survey demographics

## Demographic variables

### Location

Of the respondents, 117 were located in the RoI, 31 in NI, and another 28 skipped answering that question (although they continued with the survey). Overall therefore just about two-thirds of respondents were in the RoI, one-sixth in NI, and one-sixth left it anonymous (Table A4.1).

**Table A4.1: Location**

**Where are you (yourself) working?**

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| Valid | Republic of Ireland | 117 | 66.5 | 79.1 | 79.1 |
| | Northern Ireland | 31 | 17.6 | 20.9 | 100.0 |
| | Total | 148 | 84.1 | 100.0 | |
| Missing | Non Response | 28 | 15.9 | | |
| Total | | 176 | 100.0 | | |

If we exclude non-respondents, the distribution in the sample is as shown below, with the proportion RoI/NI at 79%/21%.

This is closely comparable to the distribution in the population as a whole (CSO, 2016; NISRA, 2017), where the proportion RoI/NI is 80%/20%. Therefore, the distribution of the sample is very closely representative to the distribution of the population across the two territorial locations.

### Role in organisation

Two-thirds (67%) of the respondents are either the Owner/CEO/General Manager, or the Food Quality/Safety Manager, and so the survey reached respondents with appropriate knowledge for the purposes of this research (Figure A4.1).

There are quite a few roles in the "Other" category (26%), and these seem to be principally from two additional categories: R&D, and Sales/Commercial, accounting for 41% of the "Other" category between them. If we include those two additional categories we have R&D (5.7%), Sales & Marketing (5.1%) – i.e. each about the same as Production - and the remaining Other (15.3%).

### Size of company

There's a spread among the respondents and reasonable coverage of all categories, although large-scale (by number of employees) companies dominate (38% of the total) (Figure A4.2).

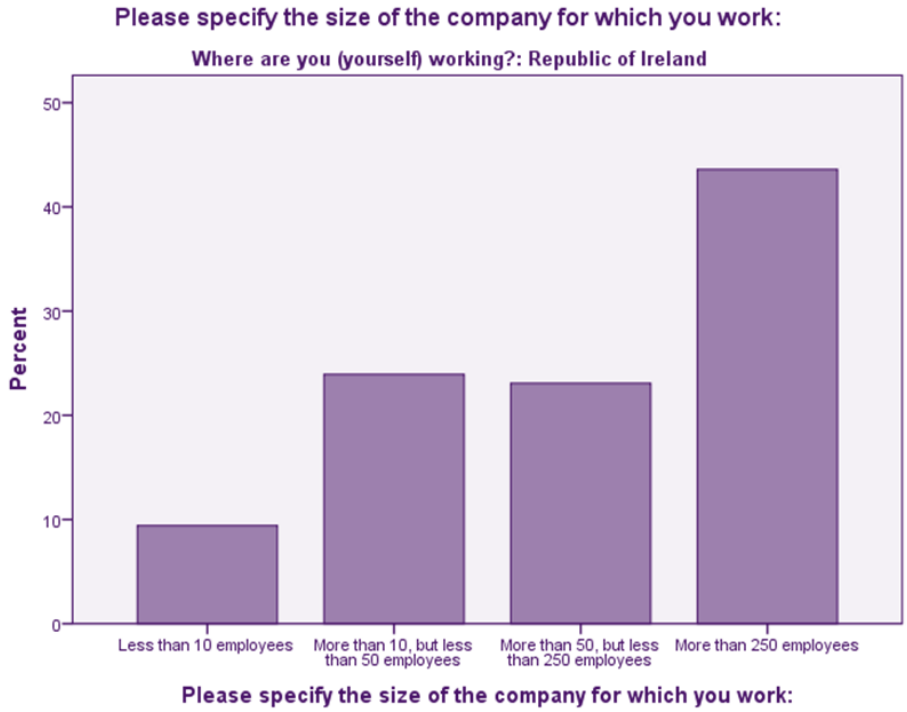
Figure A4.1: Role in company


Figure A4.2: Size of company

Below we have broken out the distributions for the RoI and NI independently (Figures A4.3 – A4.6), and we have compared them to distributions from the relevant statistical census tables: Business Demography (CSO, 2016) for the RoI[13], and the Interdepartmental Business Register (NISRA, 2017) for NI[14].

Clearly the distribution in our sample for NI appears to be much more like the population-level distribution than it does for the RoI, where the survey was responded to by a much greater proportion of large firms (250+ employees) than small ones (especially in the "Under 10" category).

### Figure A4.3: Size of company (Sample, RoI)




[13] Note that this data includes Tobacco manufacturers (Nomenclature générale des Activités Économiques dans les Communautés Européennes (NACE), C12), but there are only 6 of these in RoI (CSO, Private Communication), so the distribution shown here remains representative.

[14] This detailed data was provided privately to us by NISRA, but aggregate figures can be obtained in Table 1.11 of the Inter Departmental Business Register (IDBR).

Figure A4.4: Size of company (Population, RoI)

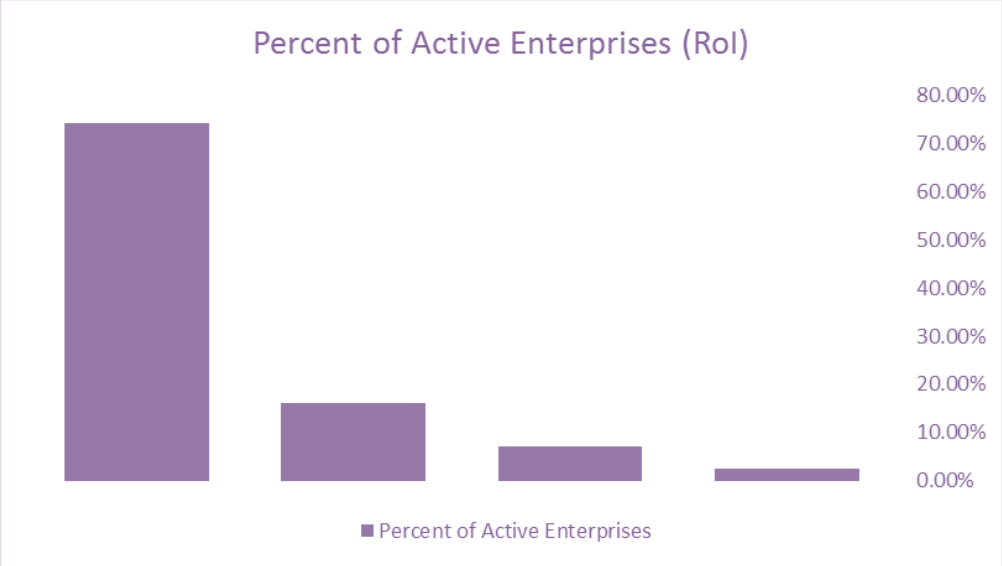
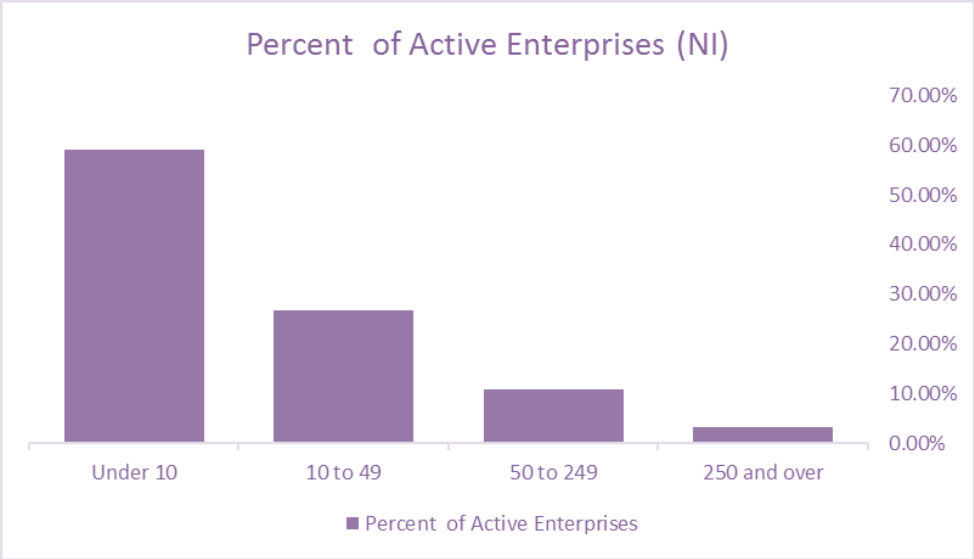



Figure A4.5: Size of company (Sample, NI)

### Figure A4.6: Size of company (Population, NI)




Finally, we show the corresponding sample and population distributions and response rates across size-categories for each of RoI and NI (Figures A4.7 and A4.8).

### Figure A4.7: Response rates by company size (RoI)

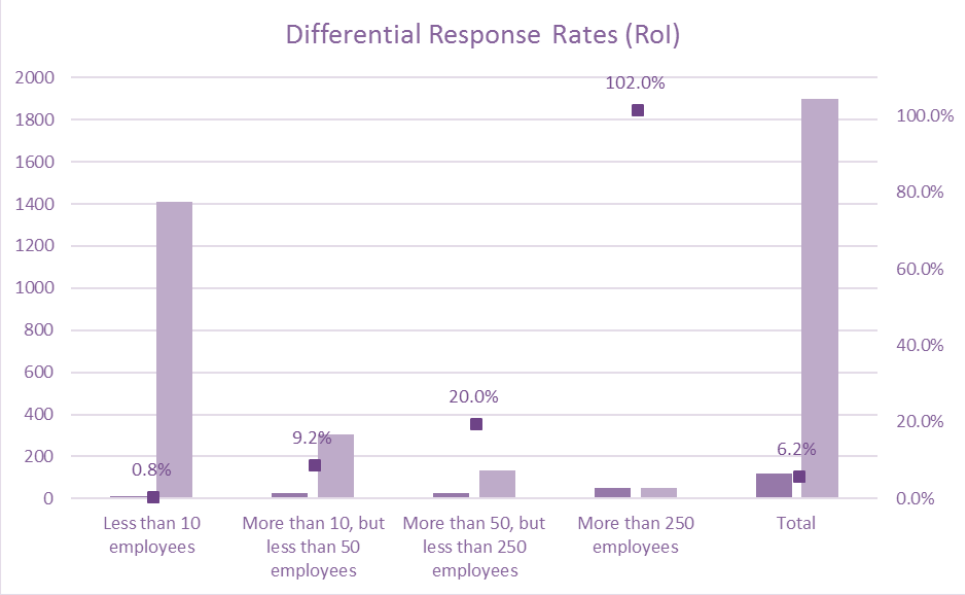
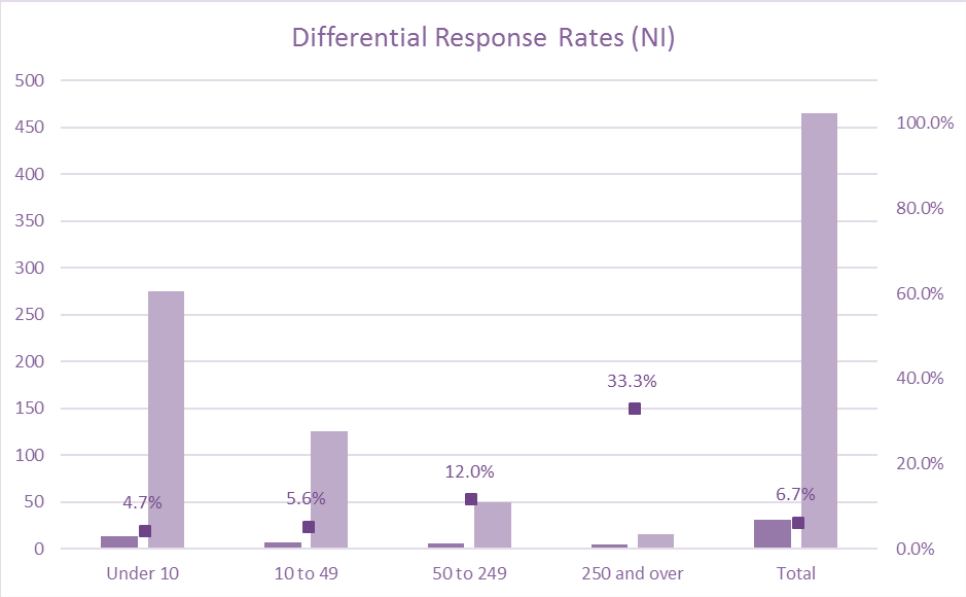


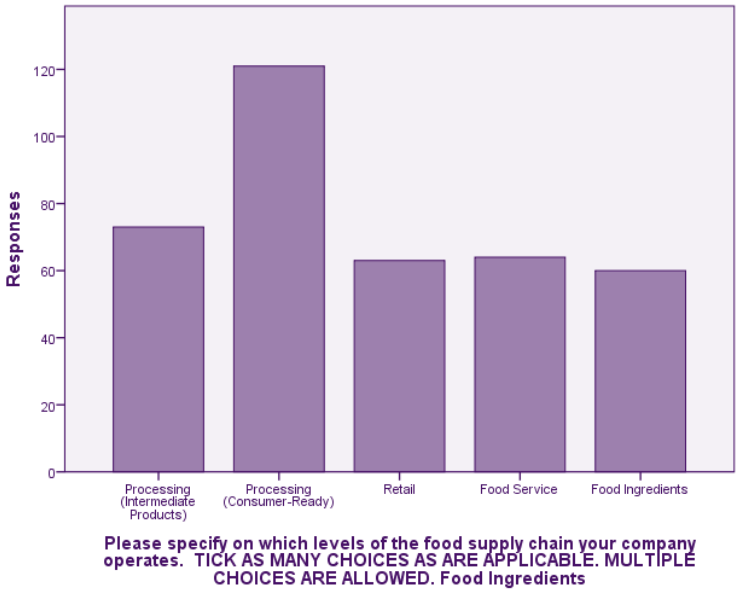
**Figure A4.8: Response rates by company size (NI)**




## Supply chain levels

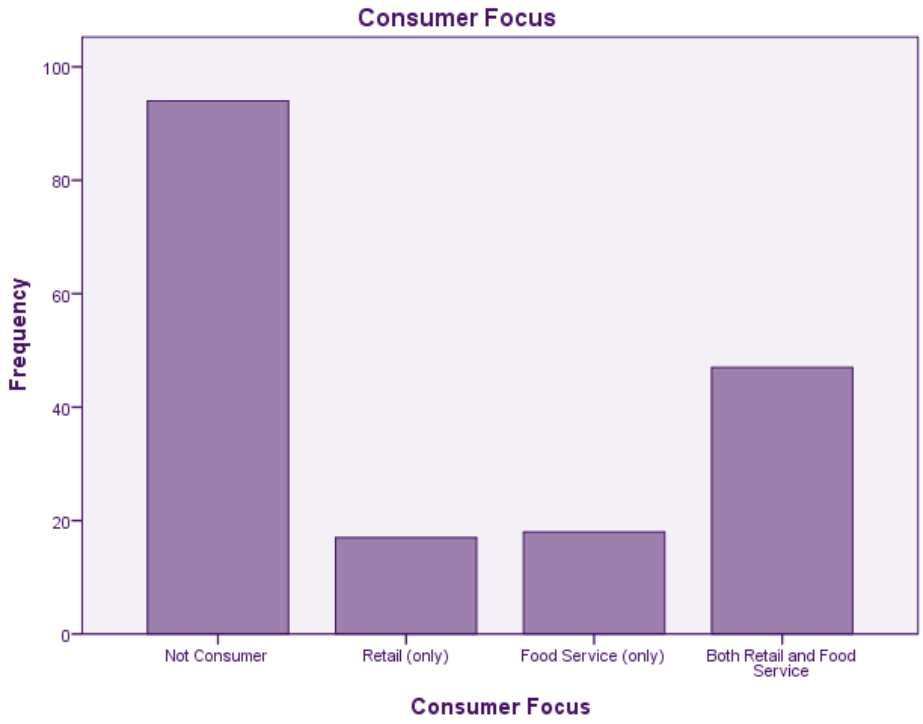
The most common category by far was "Processing (Consumer-Ready)" in which 71.0% of respondents (125 of the 176) operated, but on average respondents operate on 2 levels of the supply-chain (393 responses across 176 respondents, or 2.32 levels per respondent) (Figure A4.9).

**Figure A4.9: Supply chain levels**



The respondents were divided evenly based on whether or not they had a “consumer focus”, i.e. whether they were involved in production at a supply-chain level that involved the end-consumer, whether as retail or food-service (Figure A4.10).

**Figure A4.10: Consumer or non-consumer focus**




## Countries/regions active

Operations were concentrated – as might be expected – within the IoI (58.3%), but Sales (38.4%) and Suppliers (40.3%) were less so. 30.4% had sales outside the EU; 25.9% had suppliers, and 21.2% had operations outside of the EU (Tables A4.2, A4.3 and A4.4).

### Table A4.2: Location of operations

| | | Response | Column Response % (Base: Count) | Column Responses % |
|---|---|---|---|---|
| **Operations** | Republic of Ireland Operations | 143 | 83.6% | 39.3% |
| | Northern Ireland Operations | 69 | 40.4% | 19.0% |
| | Rest of UK Operations | 39 | 22.8% | 10.7% |
| | Rest of EU Operations | 36 | 21.1% | 9.9% |
| | Europe, outside of EU Operations | 24 | 14.0% | 6.6% |
| | USA Operations | 25 | 14.6% | 6.9% |
| | Rest of World Operations | 28 | 16.4% | 7.7% |
| | Total | 364 | 212.9% | 100.0% |

### Table A4.3: Location of sales

| | | Response | Column Response % (Base: Count) | Column Responses % |
|---|---|---|---|---|
| **Sales** | Republic of Ireland Sales | 149 | 88.7% | 20.5% |
| | Northern Ireland Sales | 130 | 77.4% | 17.9% |
| | Rest of UK Sales | 121 | 72.0% | 16.6% |
| | Rest of EU Sales | 106 | 63.1% | 14.6% |
| | Europe, outside of EU Sales | 74 | 44.0% | 10.2% |
| | USA Sales | 67 | 39.9% | 9.2% |
| | Rest of World Sales | 80 | 47.6% | 11.0% |
| | Total | 727 | 432.7% | 100.0% |

### Table A4.4: Location of suppliers

| | | Response | Column Response % (Base: Count) | Column Responses % |
|---|---|---|---|---|
| **Suppliers** | Republic of Ireland Suppliers | 129 | 88.4% | 23.1% |
| | Northern Ireland Suppliers | 96 | 65.8% | 17.2% |
| | Rest of UK Suppliers | 94 | 64.4% | 16.8% |
| | Rest of EU Suppliers | 95 | 65.1% | 17.0% |
| | Europe, outside of EU Suppliers | 49 | 33.6% | 8.8% |
| | USA Suppliers | 40 | 27.4% | 7.2% |
| | Rest of World Suppliers | 55 | 37.7% | 9.9% |
| | Total | 558 | 382.2% | 100.0% |

## Products

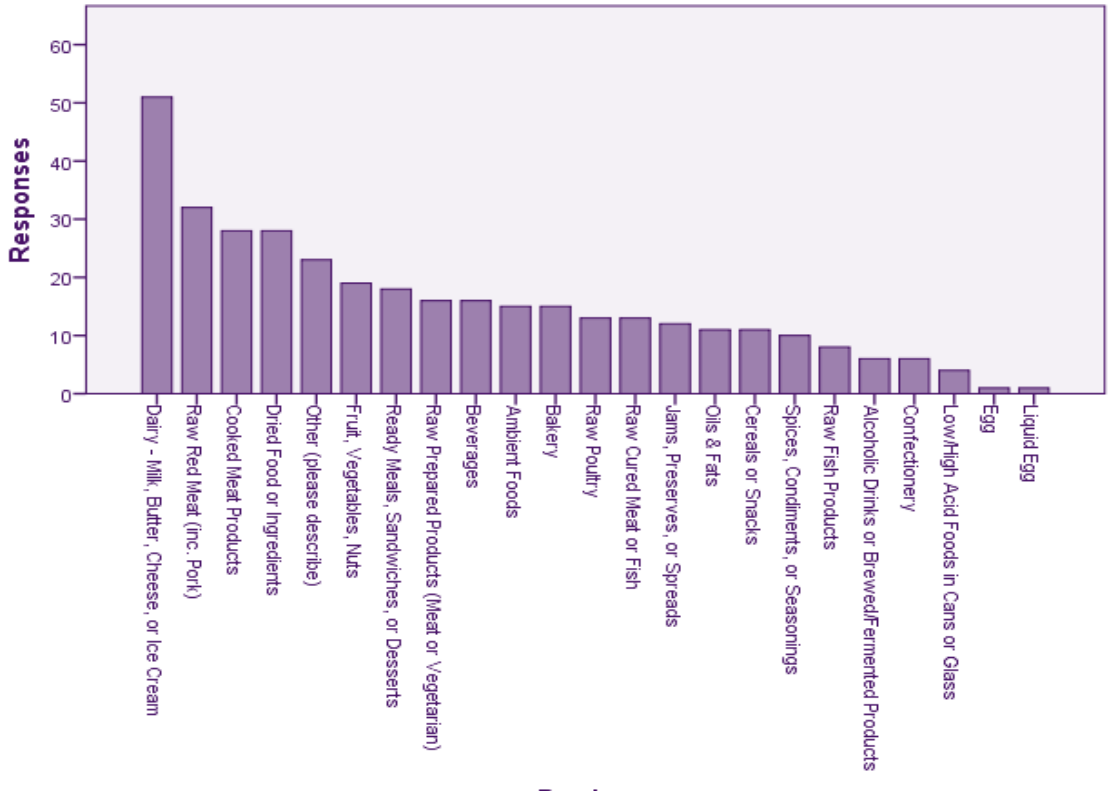
Dairy and Meat dominate here, so we first show the distribution across three broad categories (Table A4.5): Meat, Dairy and Other. Note that respondents are on average only involved in one of these three categories (223 responses from 176 respondents gives an average of 1.34). Meat is the most frequent product (26% of respondents), and both it and dairy (22%) account for approximately one quarter of respondents, with Other making up the remaining half (52%).

### Table A4.5: Basic product groups

| | | Count | Column Response % (Base: Count) | Column Count % (Base: Responses) |
|---|---|---|---|---|
| | | | | |
| | Dairy products | 51 | 29.0% | 21.7% |
| | | | | |

Broken down by more detailed categories of products, “Dairy - Milk, Butter, Cheese, or Ice Cream” is the most frequent, being produced by 14.3% of respondents (figure A4.11). “Raw Red Meat (inc. Pork)” (9%), “Cooked Meat Products” and “Dried Food or Ingredients” (each 8%) are the other most prominent product categories. There were some products which the respondents did not consider fit well into our categories, so that “Other” accounts for 6% of respondents and 13% of responses. These cover a wide range, from food colouring to snack foods. No other category of products accounted for more than 5% of respondents. We lack data on food and beverage manufacturers in RoI and NI overall at either of these two levels of detail, so that we cannot assess the representativeness of our sample across the product dimension. However, the predominance of meat and dairy products is consistent with experience and other evidence.

## Figure A4.11: Detailed Product Groups



## Appendix 5: Semi-structured questionnaire

### Interview schedule

Thank you for meeting us for this interview.

As we mentioned previously we are a group of researchers based in University College Cork and Teagasc, Ireland, interested in food fraud and food defence. We've successfully responded to a call for research proposals from ***safe*food** to conduct a study on **"A comparison of Vulnerability Management Initiatives in the Agri-food production and manufacturing chain on the island of Ireland and in selected OECD countries"**. Hence this study is funded by ***safe*food**, an Island of Ireland body set up under the British-Irish Agreement with a general remit to promote awareness and knowledge of food safety and nutrition issues.

We have a short consent form that outlines the nature of this research and how data will be used. Could you review this and if you happy to proceed sign it?

We're interested in your experience of food fraud and/or food defence incidents and, in particular, how these arose, how they were dealt with and their impact.

[Definitions - food fraud is intentional adulteration/misrepresentation for economic gain and food defence is intentional adulteration to cause harm].

| Theme | Lead in question [AGENCIES] |
|---|---|
| Prevalence | Firstly, in your opinion how prevalent is food fraud and defence? |
| | - Could we discuss the drivers and likelihood of food adulteration/misrepresentation a little further, including the differences between fraud and 'defence'?<br>- Could we discuss the impact of food adulteration a little further? |
| Incidents overview | Could you outline the incidents of both food fraud and food defence that you have dealt with/responded to? |
| | - How would you classify these, incl. type of offender?<br>- How prevalent are incidents of 'defence'?<br>- What are the key characteristics emerging from your experience? |
| Incidents detection | How were these incidents detected and at what stage? |
| | - Could you tell me a little about the mechanism/surveillance system used?<br>- What has been learned about surveillance and detection over the last few years?<br>- Are there particular challenges faced?<br>- Does the mechanism/system need to be adapted to deal with 'defence'?<br>- How did mechanism/ system work – did this particular incident inform its design/improvement?<br>- What if anything could have been done to prevent or detect these earlier/ |
| Incidents response | How have you responded to incidents?<br>What, if any, was the role of others (supply chain actors, other regulatory bodies, other jurisdictions) – was this helpful, how could this be improved.<br>- Do share information across databases and/or networks (would you, why not (if not), what concerns about that)?<br>What has worked well and has not?<br>What do you see as the key challenges and areas of improvement? |
| Prevention Vs Response | We've discussed how various incidents have been detected and how they've been dealt with.<br>How would you describe your overall strategy in terms of prevention and capability to respond?<br>Do see roles of public law (i.e. national/international law & regulations), private law (e.g. standards & audits) and public-private partnerships?<br>How significant were these incidents and for whom? |
| Good Practice | From your own experience and/or other cases, what examples have you seen of good practice?<br>- Can you tell us about any examples of good practice you've seen elsewhere? What countries/sectors/other are at the forefront? |

## Appendix 6: Organisations consulted

| Table of participating organisations[15] |
|---|
| Institute for Global Food Security, Queen's University Belfast |
| Food Safety Authority of Ireland (FSAI) |
| Food Standards Agency (FSA) in Northern Ireland |
| The Department of Agriculture, Environment and Rural Affairs (DAERA), Northern Ireland |
| UCD Centre for Food Safety, University College Dublin |
| Institute of Food and Health, University College Dublin |
| Danish Veterinary and Food Administration |
| Technical University of Denmark (DTU) |
| Danish Agriculture and Food Council |
| RIKILT, Wageningen University, The Netherlands |
| Criminal Investigation Unit, The Netherlands Food and Consumer Product Safety Authority |
| CBL, Centraal Bureau Levensmiddelenhandel, The Netherlands |
| Eurofins |
| National Food Crime Unit (NFCU), Food Standards Agency (FSA), UK |
| Food and Drink Federation (FDF), UK |
| Food Protection and Defense Institute, University of Minnesota, USA |
| Food Fraud Initiative, Michigan State University, USA |
| Science and Education Foundation, Grocery Manufacturers Association (GMA) |
| Three food supply chain actors on IoI |

15 Representatives of these organisations participated in the semi-structured interviews.

safefood

7 Eastgate Avenue, Eastgate, Little Island, Co.Cork, T45 RX01
7 Ascall an Gheata Thoir, An tOiléan Beag, Co. Chorcaí, TT45 RX01
7 Aistyett Avenue, Aistyett, Wee Isle, Co. Cork, T45 RX01

**Tel** +353 (0)21 230 4100
**Fax** +353 (0)21 230 4111

**Email:** info@safefood.eu

---

@safefood_eu

@safefood_eu

**Helpline**
**ROI** 1850 404 567 **NI** 0800 085 1683

safefood 20 years promoting North/South working