BRCGS Standard for Storage and Distribution SD308: Accommodating the requirements of GFSI Benchmark 7.2 into Issue 3 Position Statement

Document Scope:

During the lifetime of a published Standard the BRCGS Technical committee may be asked to either review the wording of a clause in the Standard, provide an interpretation for a requirement or rule on the grading of non-conformity against a clause. Any such judgements are defined in position statements. Position Statements are binding on the way that the audit and certification process shall be carried out and are an extension to the Standard. This document contains a summary of the Position Statements for the BRCGS Standard Storage and Distribution Issue 3.

Change log:

Version no.	Date	Description
1	19/9/2018	Position Statement to allow/accommodate the requirements of GFSI Benchmark 7.2 into S&D Issue 3.
2	12/08/2019	New BRCGS logo and footer changed

GFSI Benchmarking Requirements Version 7.2

Issue 3 of the Global Standard for Storage and Distribution has been benchmarked to the GFSI Benchmark Version 7.1 since April 2018. However, after the application for benchmarking GFSI published an updated version of the benchmarking requirements (version 7.2).

For the Standard to maintain its benchmarked status, it is important that the Standard completely meets the GFSI document and it is therefore necessary to introduce 1 new requirement (shown below).

This new requirement will be included in all audits from 1st February 2019 onwards.

NEW REQUIREMENT

Product authenticity

Clause	Requirements
3.5.3	The company shall undertake a documented product and service fraud vulnerability assessment of the potential risks of adulteration or substitution to products. The output from this assessment shall be a documented vulnerability assessment plan. Where products are identified as being at risk, this plan shall include details of the appropriate assurance and/or processes implemented to mitigate the identified risks. 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 on an annual basis.
Interpretation	A vulnerability assessment is a search for potential weaknesses in the storage and distribution of products to prevent fraudulent activities. It is therefore a form of risk assessment. The scope of the vulnerability assessment shall cover the activities under certification and shall include a mechanism to deal with identified potential risk outside of certification scope. The aim of the vulnerability assessment is to examine products and services for potential concerns or weaknesses, thereby identifying those that are at risk of adulteration or substitution, so that appropriate controls can be put in place.

Given that most sites certificated to this Standard have very little influence over the choice of suppliers and that most products arrive pre-packed it is perfectly possible that the outputs of the vulnerability assessment will be negligible and that no further action will be required. Additional requirements are already in place for sites that operate wholesale activities and have a greater influence on choice of supplier (refer to Section 10.2).

The vulnerability assessment should consider the information relating to each product and service to assess whether there is a potential for fraud. Where a company handles several similar products, it may be possible to consider these as a group rather than individually, providing the risks are similar.

Typical information to incorporate into the assessment includes:

- any emerging issues and information
- historical evidence of substitution or adulteration of the product
- cost or value of the product
- availability (e.g. a poor harvest may restrict availability and increase the potential for adulteration)
- sophistication of routine testing to identify adulterants. If comprehensive testing is completed within the supply chain or by the company and is specifically focused on potential fraud issues, then the likelihood of adulteration is reduced (e.g. fruit juice is often tested for a comprehensive range of parameters to prevent potential fraud, including DNA, isotopic analysis, added sugars and added water)
- country of origin
- whether the nature of the product may change the potential for fraud. For example, if a slaughterhouse intends to make a claim such as 'organic', 'Aberdeen Angus' or 'specified country of origin', then greater controls will be required to ensure that the claim is consistently met. Similarly, prepared ingredients such as beef mince or ground spices are likely to have a greater risk than the whole ingredient
- certification status of the supplier where known. If the supplier has a vulnerability assessment (e.g. it has been certificated to the BRCGS Standard for Food Safety or another GFSI-benchmarked standard that includes the requirement for vulnerability assessment and fraud prevention), then this is likely to be a very useful part of your vulnerability assessment. There is no requirement to duplicate supply chain activity already completed by a supplier. Instead consideration, should be given to the potential for any extra items, such as vulnerabilities between

the certificated supplier and the site completing the vulnerability assessment (e.g. if there is a prolonged period of transport or storage at another location).

Note that the Standard does not require a full supply chain mapping or traceability, but it expects companies to assess the potential risks of adulteration or fraud presented by the products they are handling.

The Standard does not define the exact process that the company must follow when completing the vulnerability assessment; however, it is likely to incorporate the following steps:

- draw up a list of products and services and the controls that are already in operation (e.g. approval of suppliers by customers, pre-packaged products purchased)
- consider any relevant information regarding potential fraud for each product and service
- complete a risk assessment on the vulnerability of the products.

The output of the vulnerability assessment is usually a ranking or scoring of the materials to identify those which need additional controls. The ranking and actions required could, for example, be as follows:

- Very high – a high-profile product with recent reports of adulteration or substitution published by regulatory authorities. Action or monitoring is required to ensure that only genuine materials are purchased.
- High – a high-profile product that provides an attractive target for potential substitution or adulteration. Some action and/or monitoring is required to ensure that only genuine materials are purchased.
- Low – this product is unlikely to be a target for substitution or adulteration. However, a re-assessment may be necessary if new information becomes available.
- Negligible – no further action is required as the product is extremely unlikely to be a target for fraud.

It is important that the vulnerability assessment remains up to date. Good practice is to review it whenever there is a significant change. As a guide, a review may be triggered by changes in the following, although this is not an exhaustive list:

- the country of origin or the supplier of the product
- change in service providers
- the financial situation of product suppliers or countries of origin

- the certification status of the supplier if known
- the cost of products, either upwards or downwards
- the supply chain, logistics and delivery of products
- product availability (e.g. due to seasonal shortages)
- emergence of a new risk (e.g. known adulteration of an ingredient)
- developments in scientific information associated with the process or product
- information received as part of supplier approval or product risk assessment which highlights new or evolving risks.

Several risk assessment tools have been published. These include some specialist vulnerability assessment tools such as CARVER/Shock and Threat Assessment Critical Control Points (TACCP), which may be used to achieve a structured approach to the assessment process.

The BRCGS Standard best-practice guideline, Understanding Vulnerability Assessments, is primarily aimed at food manufacturers but explains the steps to be completed. It is available on BRCGS Participate (**brcgsparticipate.com**) or can be purchased from the BRCGS bookshop (**brcgsbookshop.com**).

Issued 19/09/2018