Global Standard Storage and Distribution, Issue 4

SD404: Position Statements for Issue 4

Document Scope: Where clarification or interpretation of a requirement of the Global Standard Storage and Distribution, Issue 4 or its protocol is necessary this will be published on the BRCGS website (www.brcgs.com) as a Position Statement. Such statements are mandatory in their use from the date specified for implementation or the date of publication, where no date is specified.

Change log:

Version no.	Date	Description
1	15/01/2021	Position Statement 1
2	17/03/2021	Position Statement 2 Transport only scope: Use of BRCGS S&D logo
2.1	17/03/2021	Small change - footer amended.
3	14/06/2021	***NEW*** Position Statement 3 New Section - Wholesale branded products – product fraud risk management ***Amended*** Position Statement 1 Section 9: Open product handling – trimming of fresh produce for aesthetic purposes only
4	15/11/2022	***NEW*** Position Statement 4 Use of hairnets in open product handling areas Clarification regarding handwash facilities in open product areas ***NEW*** Position Statement 5 Changing the certification body for a re-audit ***NEW*** Position Statement 6 Changes to unannounced audit protocol for non-audit days and re-audit dates. ***NEW*** Position Statement 7 Changes to certificate validity for existing 18-month certificates
5	08/11/2023	***NEW*** Position Statement 8 Update to the protocol for section 11 – cross-docking module - NC rating

6	21/12/2023	***NEW*** Position Statement 9 Clause 1.1.10- Update of site responsibility to ensure unannounced audits can be undertaken to protocol. ***NEW*** Position Statement 10 Sites may not change CBs in the 4-month audit window. ***NEW*** Position Statement 11 Clarification of the definition of 'Initial audit'.
7	16/08/2024	***UPDATE*** Position Statement 9 Clause 1.1.10 - to provide additional clarification. PART III – 4.7.1- updated voluntary unannounced audit protocol ****UPDATE**** Position Statement 10 Clarification of 4-month period ****UPDATE**** Position Statement 11 Clarification of the definition of 'initial audit'.
8	27/04/2026	**Effective from 10 August 2026** Minor amendments related to wording in Position Statements 2, 3, 4, 6 and 7 Updated to align with the GFSI Benchmarking Requirements v.2024 ***NEW*** Position Statement 12 Clause 1.3.2 update ***NEW*** Position Statement 13 Clause 2.1 update ***NEW*** Position Statement 14 Clauses 3.5.1.2 and 3.5.2.1 updates ***NEW*** Position Statement 15 Clause 3.5.3.1 update ***NEW*** Position Statement 16 Clause 4.2.1 update ***NEW*** Position Statement 17 Clause 6.1 update ***NEW*** Position Statement 18 Clause 6.4.5 update ***NEW*** Position Statement 19 Section 17 ***NEW*** Position Statement 20 Clause 17.3 update

8.1	28/05/2026	**Effective from 10 August 2026** *__UPDATE__* Position Statement 14 Minor amends

Contents

POSITION STATEMENT 1 (AMENDED)

Section 9: Open product handling - trimming of fresh produce for aesthetic purposes only

This Position Statement summarises BRCGS expectations in terms of Section 9: Open Product Handling where a site currently certified to the Issue 3 of the Global Standard Storage and Distribution completes trimming operation on fresh produce for aesthetic purposes only.

According to the definitions in Appendix 6 of the Standard, operations such as trimming are usually excluded from the scope of Storage and Distribution activities due to the following reasons:

- Processing, however minimal is not allowed as the food safety risks associated with these activities were not a consideration while drafting the standard.
- Furthermore, experience has shown that sometimes even minor changes through processing conditions can have a significant effect on the safety of foods.

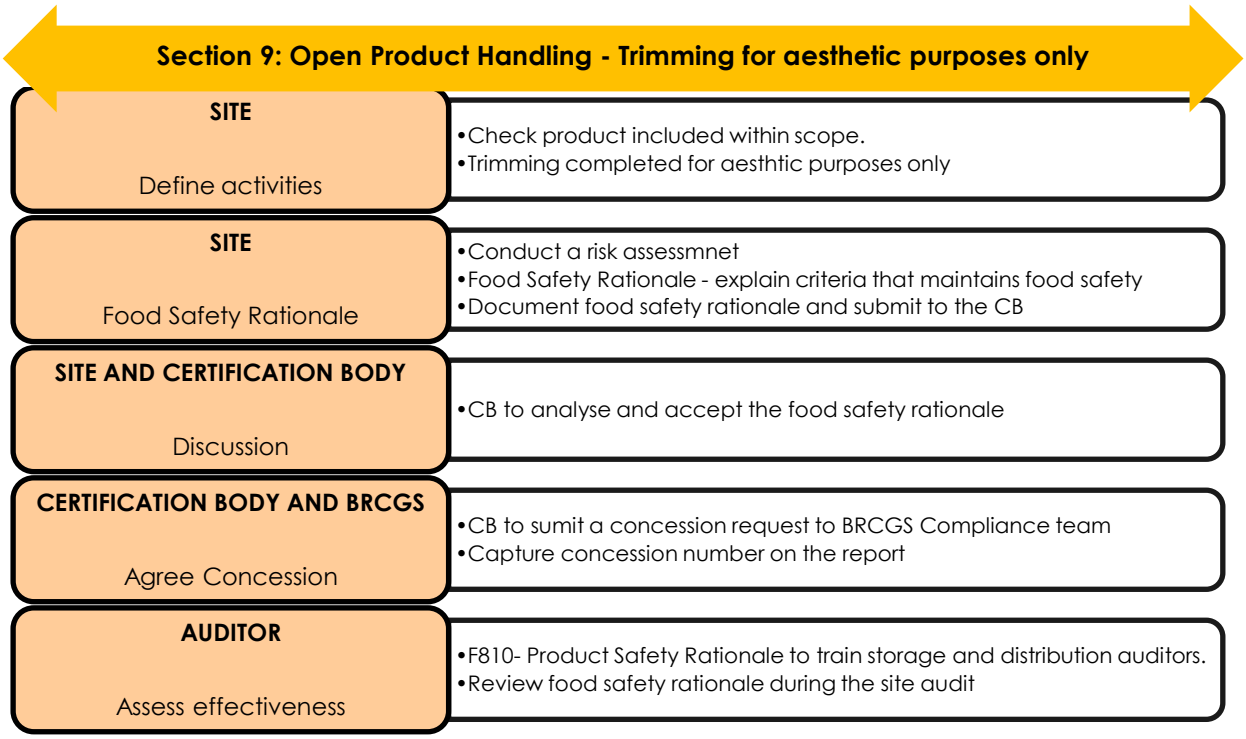
However, the Standard recognises that occasionally trimming operation is completed to enhance the visual attributes of the fresh produce and this additional processing step does not introduce any additional food safety implications or a new food safety process step.

Where a site currently certificated to Issue 3 of the Standard is completing trimming operations on fresh produce for aesthetic purposes only, they must complete a risk assessment and suitably demonstrate the food safety rationale behind this operation (i.e. explain the criteria that maintains food safety) to their certification body, who in turn can request a concession with the BRCGS team. Upon confirmation from the BRCGS team, the site can continue to include this operation under their main certification audit. Once agreed the concession will be valid for the lifetime of Issue 4 of the Global Standard Storage and Distribution.

Key criteria for consideration:

1. Only sites certificated to Issue 3 of the Standard can request a concession.
2. Trimming operations on fresh produce competed for aesthetic purposes only
3. Ready to eat (RTE) fresh produce is excluded from scope of this activity.
4. No new food safety process steps are introduced to complete this activity.

Auditors are required to challenge the basis of the risk assessment and the food safety rationale to make sure the site has carefully considered likely issues and is demonstrably based on robust science, where applicable. Considering most Storage and Distribution auditors are experienced Food Safety auditors, they would understand food safety rationale. However, where the auditors are specifically Storage and Distribution only auditors, certification bodies can use the F810: Product Safety Rationale document to train them as required.



Statement publication date: 1 January 2021. **Amended:** 14 June 2021.

POSITION STATEMENT 2 (AMENDED)

Transport only scope: Use of BRCGS Storage and Distribution logo

Sites certificated to the 'Transport only' scope are now eligible to use the BRCGS Storage and Distribution logo, as explained in BRCGS Global Standard Storage and Distribution Issue 4- Part III, section 6.6 – BRCGS logos.

Statement publication date: 17 March 2021 **Amended:** 27 April 2026

POSITION STATEMENT 3

New section - Wholesale branded products – product fraud risk management

10.2.2 - Product fraud risk management

Statement of intent: The wholesaler shall ensure that systems are in place to minimise the risk of purchasing branded fraudulent or adulterated products.

INTERPRETATION

It is accepted that when wholesalers are trading branded products, the wholesaler's responsibility will be more limited than would be the case for own-brand products therefore it is not normally required for the company to fully understand the manufacturing supply chain of the products handled.

Nevertheless, it is expected that wholesaler should take some responsibility for ensuring that their facilities are not being used for the storage and distribution of illegal or fraudulent or adulterated products. At its simplest, where the site purchases products from a company – either a processor, packer, consolidator or an agent or broker, the supplier must provide sufficient information so the wholesaler can undertake basic checks to ensure that the branded products are legitimate, and the site is not likely to be trading fraudulent or adulterated products.

The objectives of this section are to ensure that:

- the site has assessed its supplier and their associated supply chain activities for vulnerability to product fraud or adulteration activities (such as the adulteration or substitution of products prior to delivery to the site)
- the site has appropriate controls in place (based on its product fraud vulnerability assessment plan) to minimise the risk of purchasing or handling fraudulent products.

10.2.2.1	The company shall develop a documented fraud vulnerability assessment plan to establish levels of confidence in the suppliers from whom the wholesaler purchases branded products to reduce the risk of handling fraudulent or adulterated products; the plan shall be fully implemented. The plan may consider: • historical trading relationships • the nature of the products with regard to the risk of fraud or adulteration • the need for supplier approval process to include trading history, financial security, supplier profile The fraud vulnerability assessment plan shall be kept under review to reflect any changing circumstances that may alter the potential risks. It shall be formally reviewed annually.

INTERPRETATION

The fraud vulnerability assessment plan should document:

- the checks that will be undertaken of new and existing suppliers and products.
- the frequency at which the checks will be carried out
- who is responsible for carrying out the checks
- how the results of any such checks will be documented and interpreted.

The checks are designed to establish confidence in the company's supplier and thereby the branded products which the site is purchasing. The checks may include a review of:

- the suppliers trading history with the site.
- any documented issues of fraud or prosecutions of the supplier (discovered, for example, by questionnaire or internet search)
- the supplier's financial stability (probably already undertaken as part of financial due diligence)
- the type of products being handled and their propensity for fraud or adulteration (e.g. manuka honey has a poor record for fraud)
- reputation – a supplier with an established reputation may present a lower risk than a new or unknown business.

The Standard does not define the exact process that the site must follow when completing the fraud vulnerability assessment, but its output should rank or score the supplier and products to identify those which need additional controls. The ranking and actions required could, for example, be as follows:

Very high The product and/or supplier has been the subject of recent reports of fraud or adulteration published by regulatory authorities, and the supplier of this product has a poor or no previous trading history with the site. Action or monitoring is required to ensure that only genuine products are handled if the site wishes to continue to work with this supplier.
High The product provides an attractive target for potential fraud or adulteration, although the supplier of this product has a reasonable trading history with the site. Some action and/or additional assurances may be required to ensure that only genuine products are handled.
Low The product is unlikely to be a target for fraud or substitution, and the supplier of this product has a good trading history with the site; however, a re-assessment may be necessary if new information becomes available.
Negligible No further action required as the products handled are extremely unlikely to be a target for product fraud and the supplier of this product has an excellent trading history with the site.

It is important that the fraud vulnerability assessment remains up to date and is reviewed at least annually (or when there is a significant change to the product). As a guide, a review may be triggered by the following, although this is not an exhaustive list:

- a change in the financial situation of the supplier from whom the site purchases products
- a change in the supply chain, logistics and delivery of products
- the emergence of a new risk (e.g. known adulteration of an ingredient or shortage)
- a development in the regulatory information associated with a product.

10.2.2.2	Where a potential risk of purchasing fraudulent or adulterated product is identified, the fraud vulnerability assessment plan shall include appropriate processes to mitigate the identified risks.

INTERPRETATION

Output from the vulnerability assessment

Where products are identified as being at particular risk of fraudulence, adulteration or substitution, appropriate assurance controls are needed to ensure that only genuine products are handled. Depending on the perceived risk, the supplier may be required to have an in-depth understanding of the additional assurance controls in place to understand, for example, the supply chain risks, perhaps through audit or certification, product sampling or testing, etc..

Where concerns relate to the supplier, mitigations may include more frequent reviews of the issues causing concern or, in extreme circumstances, ceasing the trading relationship.

Effective date: 15 August 2021

Statement publication date: 14 June 2021

POSITION STATEMENT 4

Based on the feedback and enquiries received from various sites and certification bodies, we are making some clarifications about clauses relating to Section 9 – Handling of open food products.

9.2 Personnel facilities

9.2.2	Where open food products are stored and handled, toilets shall not open directly into the storage areas, and hand-washing facilities cannot be located within the toilets.

INTERPRETATION
Toilets must be adequately segregated and must not open directly into product-handling areas. There should be an intermediate ventilated space between the toilet cubicle and product-handling area to prevent foul odours. Dedicated hand-washing facilities must be provided at entrances to product-handling areas and, where appropriate, at additional points within the operation.

Clarification
If open product handling on site is restricted to the employees' lifting and moving trays of open product limited to fresh produce e.g. open boxes and trays of fruit and vegetables, including produce in palletainers, stillage, etc, then a risk assessment may be used to determine the risk to the open product and hence, to determine the requirement of separate hand wash facilities.

If there is any additional handling of the open product e.g., picking or sorting, etc. then a separate hand wash facility is required. The hand washing facilities cannot be located within the toilets.

9.6 Protective clothing

9.6.5	All hair shall be fully covered to prevent product contamination.

INTERPRETATION
Headwear such as mob hats or hairnets must completely cover head hair to minimise potential contamination.

Clarification
If open product handling on site is restricted to the employees' lifting and moving trays of open product limited to fresh produce e.g. open boxes and trays of fruit and vegetables, including produce in palletainers, stillage, etc, then a risk assessment may be used to determine the risk to the open product and hence, to determine the requirement of hair nets or mob caps.

If there is any additional handling of the open product e.g., picking or sorting, etc. then hair nets or mob caps shall completely cover head hair to minimise potential contamination.

Effective date: 1 January 2023

POSITION STATEMENT 5

Changing certification body for a re-audit

In addition to the situations described in section 2.8.7 of the audit protocol, an early re-audit may occasionally be requested by a site – usually shortly after the previous audit or following a failure to get certificated. This often occurs because the site wants to improve its audit grade.

Sites have the ability to request a re-audit however this must be completed by the certification body who issued the current certificate.

In exceptional circumstances, a site may be permitted to change certification bodies for the re-audit when agreed in advance by BRCGS.

Where a change in certification body has not been sanctioned, the re-audit will be null and void and will not be accepted onto the BRCGS Directory.

Justification shall be provided in writing to the certification body who shall submit it to BRCGS for consideration through the formal concession process.

This requirement applies only when an early re-audit has been requested; it does not change the process for re-audits completed to the normal 6- or 12-month schedule.

Effective date: 1 February 2023

POSITION STATEMENT 6

Changes to the unannounced audit protocol (Option 1- single visit) for recertification audit window and number of non-audit days:

To ensure that all BRCGS Standards maintain comparable audit protocol for unannounced audits, BRCGS have made two changes to the unannounced audit protocol (Option 1- single visit) for Global Standard Storage and Distribution Issue 4. These changes can be summarised as:

- a reduction of the unannounced audit window from 9 months to 4 months.
- a reduction in the number of non-audit days which a company can nominate from 15 days to 10 days.

These changes come into effect on 1 February 2023 (i.e. apply to all unannounced storage and distribution audits starting on or after 1 February 2023).

Therefore, from 1 February 2023 the following text replaces sections 4.1.4 and 4.8.1 of the audit protocol currently in the Standard:

Section 4.1.4 Nominating non-audit days
The unannounced audit programme allows sites to nominate up to 10 days when the site is not available for an audit. The dates must be provided at least 4 weeks in advance and the reason must be provided (e.g. a planned customer visit). The certification body may challenge a reason where it does not appear appropriate.

Days when the site is not operating (e.g. weekends, public holidays, planned shutdowns for site holidays or maintenance) are not included within the 10 days. Any such days shall be notified to the certification body when opting into the unannounced scheme.

Certification bodies are expected to operate discretion in the case of emergencies.

It is a condition of joining the unannounced scheme that the auditor shall be granted access to the site on arrival. If access is denied, the site will be liable for the auditor's costs and will revert to the announced audit scheme. At the discretion of the certification body, the existing certificate may also be suspended or withdrawn.

Sites on a 6-month audit schedule (e.g. sites certificated to the Standard with grades C or D) may nominate a maximum of 5 days.

Part III, section 4.8.1 of the Audit Protocol, Scheduling re-audit dates.
Unannounced audit protocol: Option 1 (Single visit): has been updated:
The site can choose whether to:
• remain within the unannounced Option 1 programme
• transfer to the unannounced Option 2 programme
• revert to the announced audit programme.

If the site wishes to remain in the Option 1 programme, the audit may occur at any stage within the last 4 months of the audit cycle, including the 28 calendar days before the audit due date. The audit will be unannounced, and the date of the audit shall not be notified to the site in advance.

It is the responsibility of the certification body to ensure that the audit is undertaken within the certification window.

If the site opts to move to the unannounced Option 2 programme, the rules for that programme will apply and the announced systems audit will occur within the 28-day window based on the initial audit date.

If the site wishes to withdraw from the unannounced audit programme, the next audit will be scheduled to occur within the 28 days up to and including the anniversary of the last audit date; this ensures that the maximum time between audits is not more than a year.

In some situations, the certification body may have already scheduled the unannounced audit with a 9-month timescale (for example, to ensure time for planning of visas). To accommodate this, BRCGS will allow certification bodies to complete audits outside the 4-month window but within the 9-month window until 1 July 2023. After this date, all unannounced audits will be carried out within the 4-month window as described in this position statement.

Effective date: 1 February 2023

POSITION STATEMENT 7

Currently, the BRCGS Global Standard Storage and Distribution allows an 18-month validity of the certificate for existing, certificated sites which are handling consumer products only (or 12 months for sites with grades C/C+ and D/D+).

To align with our other Standards, this maximum certificate validity will change from:

- 18 months to 12 months for sites with grades AA/AA+, A/A+ or B/B+
- 12 months to 6 months for sites with grades C/C+ or D/D+

Effective date: 1 February 2023

POSITION STATEMENT 8

Currently, the BRCGS Global Standard Storage and Distribution Standard Issue 4 does not specify how the non-conformities are rated for section 11 - Cross-Docking Module. The aim of this position statement is to further clarify the protocol for the Cross-Docking Module described in the Audit Protocol (Part III, section 1.6) of the Standard.

1.6.5 Audit reporting and certification
A separate audit report is completed for each Cross-Docking site - SDAM11401. The non-conformities of the Cross Docking Module are not included in the main site's count of non-conformities and hence, it does not affect the grade or the certification status of the main site.

The non-conformities for the Cross Docking Module and the scoring will be as per the table below.

Critical	Major	Minor	Process for corrective action
0	0	3 or less	Provide objective evidence within 28 calendar days
0	1	2 or less	
		>3	Certificate not issued. Full re-audit required for the cross-dock site to be certificated.
	>1	>2	
1 or more			

The classification of the non-conformities will remain the same as per section 2.4 of the Audit Protocol.

Critical: Where there is a critical failure to comply with a product safety or legal compliance issue.
Major: Where there is a substantial failure to meet the requirements of a statement of intent or any clause of the Standard, or where a situation is identified which would, on the basis of available objective evidence, raise significant doubt as to the conformity of the product or services being supplied.
Minor: Where a clause has not been fully met but, on the basis of objective evidence, the conformity of the product is not in doubt.

After a successful outcome of the audit process, a Cross-Docking annex shall be issued by the certification body, along with the main certificate. The annex shall include the names and location details of the cross-docking facilities (see Appendix 5 of the Standard for a template of the Cross-Docking annex).

If a cross-docking site/facility fails its audit, the company in turn will fail to gain certification to the Cross-Docking Module. Where certification has previously been awarded to a cross-docking site, the certification body shall withdraw and re-issue the certificate without the Cross-Docking Module being included in the scope.

In this case where a cross-docking site/facility fails its audit, only the cross-docking site/facility will require a re-audit and not the main site.

Publication date: 8 November 2023

POSITION STATEMENT 9

BRCGS previously published this position statement indicating that from 1 May 2024 the text for clause 1.1.10 was updated to the following:

1.1.10	Where the site is certificated to the Standard, it shall ensure that announced recertification audits occur on or before the audit due date indicated on the certificate. It is the site's responsibility to ensure that all requirements are in place to ensure the unannounced audit can be undertaken in accordance with the protocol.

INTERPRETATION

Please note, that this position statement applies to all audits for the Global Standard Storage and Distribution, Issue 4, and to all audit options, including both voluntary and mandatory unannounced audits.

For the year in which a site is due their 1 in 3 unannounced audit, storage and distribution operations will have two audit options to choose from:

- Option 1 - fully unannounced
- Option 2 - part unannounced/part announced.

Certification bodies will discuss audit options (announced, mandatory unannounced, voluntary unannounced), with sites and notify them which year a mandatory unannounced audit will take place (the actual date of the unannounced audit will not be communicated to the site). This discussion must occur within 3 months following the last audit, to ensure that the site knows if an unannounced audit will take place in the coming year.

It is the site's responsibility to ensure that all requirements are in place to ensure the unannounced audit can be undertaken in accordance with the protocol (this includes both voluntary and mandatory unannounced audits). This includes agreeing contractual terms with the certification body in advance of the start of the 4-month audit window and keeping the certification body up to date on changes that may affect this planning, such as maintenance shutdowns.

Where the site has not made adequate arrangements with the certification body in due time prior to the start of the 4-month audit window, the audit due date will be moved to accommodate the 'late start' and the unannounced audit may be completed at any time in the following 4 months. Sites should acknowledge that their current certificate may therefore expire. In addition, a major non-conformity shall be awarded. Certification bodies shall inform BRCGS through the usual concession process.

As a consequence, Section 4.8.1 of the audit protocol (Part III, Section 4) Scheduling re-audit dates for the voluntary unannounced audit programme is also amended as follows:

4.8.1 Scheduling re-audit dates

The site can choose whether to:

- remain within the unannounced Option 1 programme
- transfer to the unannounced Option 2 programme

- revert to the announced audit programme.

If the site wishes to remain in an unannounced programme, the next audit will be unannounced. The audit may occur at any stage within the last 4 months of the audit cycle, including the 28 calendar days before the audit due date. This allows sufficient time for corrective action to take place in the event of any non-conformities being raised without jeopardising continued certification.

It is certification body's responsibility to initiate the unannounced audit process within 6 months after the last audit and request all information from the site/company to be able to schedule the audit within the audit window. However, the site is responsible to ensure that all requirements are in place to ensure the unannounced audit can be undertaken in accordance with the protocol, and this includes agreeing contractual terms with the certification body in advance of the start of the 4-month window, and keeping the certification body up to date on changes that may affect this planning, such as maintenance shutdowns.

Where the site has not made adequate arrangements with the certification body in due time prior to the start of the 4-month audit window, the audit due date will be moved to accommodate the 'late start' and the unannounced audit may be completed at any time in the following 4 months. Sites should acknowledge that their current certificate may therefore expire. In addition, a major non-conformity shall be awarded. Certification bodies shall inform BRCGS through the usual concession process.

If the site wishes to withdraw from the voluntary unannounced audit programme, the next audit will be scheduled to occur within the 28 calendar days up to and including the anniversary of the last audit date; this ensures that the maximum time between audits is not more than a year. Where the site received a grade of C+ or D+ at the last audit and wishes to withdraw from the voluntary unannounced audit programme, the next audit due date will be 6 months after the last audit date, and the audit will occur within the 28 calendar days prior to this date.

Effective date: 1 September 2024

POSITION STATEMENT 10

Changing certification body

There are a number of arrangements to be made by both a site and its chosen certification body to ensure a BRCGS audit is undertaken to the correct protocol.

The protocol requires that within 3-months of the previous audit date, the site either opts into the voluntary unannounced programme or if within the announced or blended announced programme that the certification body will communicate to the site whether the next audit will be announced or unannounced.

A site may choose to change to a different certification body from its current certifying body. However, changes will not be permitted in the last 4-months before the re-audit due date, whether an unannounced audit is scheduled or not, unless agreed in writing with BRCGS through the certification body concession process.

Effective date: 1 May 2024

POSITION STATEMENT 11

Update to Appendix 6 Glossary of terms

Definition of 'initial' audit

Currently, the BRCGS Global Standard Storage and Distribution, Issue 4 defines an initial audit as:

Initial audit	The BRCGS audit at a company/site which is not in possession of a valid BRCGS certificate. This may be the first audit at a site or a subsequent audit of a site whose certification has lapsed.

This definition has been updated to:

Initial audit	The first BRCGS audit at a specific site address or audit carried out at a site where the previous certificate has lapsed for more than 24 months.

It should be noted that this change impacts the requirement for a mandatory unannounced audit to be undertaken at least once in every 3 years. This 3-year cycle will continue irrespective of a lapse in certification as specified for 24 months.

Effective date: 1 January 2024

POSITION STATEMENT 12

An amendment has been made to clause 1.3.2 to align with the new requirements of GFSI BMR 2024. These changes are shown in **bold** in the clause below.

1.3.2	The **site's** senior management shall ensure that all **personnel** are aware of their responsibilities and **demonstrate that work is carried out in accordance with documented site policies, procedures, work instructions and existing practices for activities undertaken. All personnel shall have access to relevant documentation.**

INTERPRETATION

Personnel roles and responsibilities
The objective of this clause is to ensure that all personnel, including temporary personnel and employment agency personnel, can work effectively and ensure that safety, quality and legality are maintained.

Consistent application of these systems relies on the correct and established processes being documented, accessible by relevant personnel and used in practice.

There is no requirement for a detailed job description; however, personnel should be aware of their particular responsibilities. Where the role or an activity that makes up part of the role covers a safety, quality or legality issue described within a procedure (e.g. a critical control point (CCP) or prerequisite programme), the personnel must understand what is expected and be able to access the relevant procedure.

It should be clear to the auditor from discussions with personnel during site audits that everyone clearly understands their responsibilities with respect to the product safety, quality and legality issues covered by the Standard.

Monitoring of employees may be through effective supervision, measurement of objectives or a more formalised appraisal system.

Effective date: 10 August 2026

POSITION STATEMENT 13

An amendment has been made to clause 2.1 to align with the new requirements of GFSI BMR 2024. These changes are shown in **bold** below.

2.1	Prior to conducting a risk analysis, the company shall ensure **that appropriate** prerequisites programmes are in place. The control measures and monitoring procedures for the prerequisites programmes **shall** be clearly documented, **verified where appropriate,** and included within the development and reviews of the HARA or HACCP plan. Where applicable, product safety prerequisites or handling requirements shall include, but not be limited to: • the condition and maintenance of buildings, equipment and transport vehicles as appropriate • documented practices for the safe handling, storage and transport of products • procedures for handling damages, waste product and returns • procedures related to the allergen management plan • pest management procedures • the approval of services or subcontractors • sanitation procedures (cleaning and disinfection) • maintenance of the cold chain (not applicable to ambient stable products) and controlled environment (e.g. humidity, modified air) • personal hygiene standards (limited applicability to pre-packed food products or consumer products) • training • any other activities covered by the additional voluntary modules

INTERPRETATION

The prerequisite processes are expected to meet the requirements set out in the Standard. They represent the fundamental organisational and operational conditions needed to control generic hazards within the scope of an agent or broker's activities. Although many prerequisites form part of routine business processes, it remains essential that they operate effectively and to an appropriate standard. This is because:

- the prerequisite programme provides the foundation on which the rest of the HARA or HACCP plan is developed
- the company depends on these prerequisite activities to mitigate identified hazards and support the delivery of safe product (for example, when supplier approval or traceability is identified as a prerequisite, the company relies on these activities to ensure that hazards are adequately controlled within the supply chain)

Each identified prerequisite benefits from a structured workstream that ensures the relevant activities, procedures and policies are in place, functioning correctly, and consistently delivering the intended level of control. While the prerequisite programme is expected to be effective, not every prerequisite requires validation, as these programmes often relate to broad organisational controls whose outcomes may not be quantifiable. Verification may be applied where appropriate to confirm that the prerequisites continue to operate as intended. Good practice is to verify and review the prerequisite programmes and their management. The frequency of this verification and review should be based on risk, but it could be included in the annual review of the HARA or HACCP plan.

The definition of "where appropriate" is included in Appendix 6 – Glossary of Terms of the Global Standard Storage and Distribution, Issue 4.

Where appropriate	In relation to a requirement of the Standard, the site will risk assess the actual requirement of the Standard and, where applicable, put in place systems, processes, procedures or equipment to meet the requirement. The site shall be mindful of legal requirements, best-practice standards, good manufacturing practice and industry guidance, and of any other information relating to the manufacture of safe and legal product.

Effective date: 10 August 2026

POSITION STATEMENT 14

An amendment has been made to clause 3.5.1.2 and 3.5.2.1 to align with the new requirements of GFSI BMR 2024 These changes are shown in **bold** below.

3.5.1.2	Specifications or contracts shall exist between the company and the supplier to define the service provided and ensure that potential product safety risks associated with the service have been addressed. They shall include key data to meet customer and legal requirements and assist the site in the safe handling of the product **(e.g. chemical, microbiological, physical or allergen standards)**. Where specifications are not formally agreed, the company shall be able to demonstrate that it has taken steps to put a formal agreement in place.

3.5.2.1	A contract or written agreement shall exist with all subcontractors, which shall, on the basis of risk and any specified customer contracts, define requirements for the safe handling, storage and transport of products (e.g. **chemical, microbiological, physical or allergen standards**, temperature range, special handling requirements, product security, segregation of incompatible products, vehicle type).

INTERPRETATION

3.5.1.2 - Specifications or contracts

Contracts or specifications must be established for all service providers (as detailed in clause 3.5.1.1) to ensure that the appropriate level of service is delivered and that any potential risks are effectively addressed. Specifications, depending on the nature of the product and its intended use, may include parameters such as chemical, microbiological, physical, or allergen standards. Where such parameters are used for food safety purposes, they shall be based on appropriate scientific principles.

On-site service providers must receive appropriate training to guarantee that their activities are conducted in a manner that safeguards compliance with these standards. Where a supplier does not provide a formal contract specification, the site shall document the requirements and incorporate them into the contract. All contracted service specifications must be periodically reviewed to confirm that they continue to meet the site's operational and regulatory requirements.

3.5.2.1 Contract or written agreement

Contracts must be established with all approved subcontractors to ensure that:

- The correct level of service is consistently provided.
- All product-handling requirements are clearly defined in terms of the work to be undertaken (e.g., temperature range, special handling requirements, product security, segregation of incompatible products, vehicle type).
- Specifications, depending on the nature of the product and its intended use, may include parameters such as chemical, microbiological, physical, or allergen standards, ensuring that subcontractor activities do not compromise product safety, quality, or legality. The examples provided are illustrative and should be applied based on risk and the nature of the product or service, and where used, such specifications should be based on appropriate scientific principles.
- Contracts shall require subcontractors to operate to at least the same standards as the site being audited, with the contract or written agreement signed by both parties. Customer contracts (such as those with brand owners) must be reviewed to confirm that

any additional product-handling requirements are incorporated.
It is considered good practice to notify the product owner of any intention to outsource part of the operation, as some brand owners require the opportunity to formally approve or reject subcontractor use. Where outsourcing is clearly detailed on the approved product specification, this demonstrates customer agreement with the process.
Additionally, documented mechanisms must be in place to ensure full traceability throughout the process.

Contracts shall require subcontractors to operate to at least the same standards as the site being audited, with the contract or written agreement signed by both parties. Customer contracts (such as those with brand owners) must be reviewed to confirm that any additional product-handling requirements are incorporated.

It is considered good practice to notify the product owner of any intention to outsource part of the operation, as some brand owners require the opportunity to formally approve or reject subcontractor use. Where outsourcing is clearly detailed on the approved product specification, this demonstrates customer agreement with the process.

Additionally, documented mechanisms must be in place to ensure full traceability throughout the process.

Effective date: 10 August 2026

POSITION STATEMENT 15

An amendment has been made to clause 3.5.3.1 to align with the new requirements of GFSI BMR 2024. These changes are shown in **bold** below.

3.5.3.1	The company shall develop a documented fraud vulnerability assessment plan to establish levels of confidence in the customers for whom the company stores and/or distributes products to reduce the risk of handling fraudulent products; the plan shall be fully implemented. The plan may consider: • historical trading relationships • the nature of the products with regard to the risk of fraud • the need for a new customer approval process (e.g. trading history, financial security, customer profile). **Where personnel are engaged in vulnerability assessments, the individual or team responsible shall understand potential product fraud risks. This shall include knowledge of the principles of vulnerability assessment.**

INTERPRETATION

Competency of the vulnerability assessment and product fraud team

It is important that personnel completing vulnerability assessments for product fraud are competent to develop the plan; they need to understand the risk they are trying to prevent.

Therefore, it is expected that within the team there will be knowledge of:

- the principles of product fraud (e.g. what product fraud is, why its management is important)
- risk assessment or vulnerability assessment techniques
- the risks associated with the raw material, product, supply chain or process being assessed where relevant, noting that the term "raw material" includes any incoming product that is handled, reconfigured, assembled or repacked and therefore functions operationally as an input to the process.

The Standard is not prescriptive regarding how this knowledge is demonstrated and may include:

- formal training (e.g. a training course in product fraud, vulnerability assessment or VACCP)
- internal training, development and experience (e.g. demonstrable knowledge of the site)
- other competency (e.g. the completeness and effectiveness of the vulnerability assessment and its implementation).

Risk assessments may be completed either by responsible individuals or by a team. The advantage of a team is that every company has several departments that are likely to possess useful information, for example:

- technical or QA personnel are often subject matter experts
- supplier approval will see information relating to specific raw materials, suppliers and supply chains
- purchasing departments are usually well informed about availability or pricing concerns
- goods receipt and production teams see the materials actually delivered to the site.

Where a team is used to complete assessments, it is important to consider the overall capability of the team.

If the site does not have the appropriate in-house knowledge, external expertise (e.g. consultants) may be used; however, reference should be made to section 3.5.1.

Effective date: 10 August 2026

POSITION STATEMENT 16

An amendment has been made to clause 4.2.1 to align with the new requirements of GFSI BMR 2024. These changes are shown in **bold** below.

4.2.1	A site-specific documented risk assessment (threat assessment) shall be undertaken to identify any potential risks to the security of products held on the premises in storage or on vehicles, and appropriate controls shall be implemented. The threat assessment shall include both internal and external threats, and shall be reviewed at an appropriate frequency or, as a minimum, annually. It shall also be reviewed whenever: • a new risk emerges (e.g. a new threat is publicised or identified) • an incident occurs, where product security or product defence is implicated. **Where personnel are engaged in threat assessments and food defence plans, the individual or team responsible shall understand potential product defence risks. This shall include knowledge of products stored and distributed and the principles of product defence. Where there is a legal requirement for specific training, this shall be in place.**

INTERPRETATION

Competency of the threat assessment and product security/food defence team

It is important that personnel completing product security/food defence threat assessments are competent to develop the plan; they need to understand the risks they are trying to prevent. Therefore, it is expected that within the team there will be knowledge of the principles of product security/food defence and an understanding of the site's activities, including storage and/or distribution, as applicable.

The Standard is not prescriptive regarding how this knowledge is demonstrated and may include, for example:

- training (e.g. a training course in food defence)
- experience (e.g. demonstrable knowledge of the site such as security-related duties, or length of service at the site)
- other competency (e.g. the completeness and effectiveness of the threat assessment and its implementation).

Where there is a legal requirement for specific training, the site is expected to be able to demonstrate that this has been appropriately completed.

In the event of the site not having the appropriate in-house knowledge, external expertise (e.g. consultants) may be used; however, reference should be made to section 3.5.1.

Effective date: 10 August 2026

POSITION STATEMENT 17

An amendment has been made to clause 6.1 to align with the new requirements of GFSI BMR 2024. These changes are shown in **bold** below.

6.1 Statement of intent	Equipment shall be suitably designed for the intended purpose and shall be used **and stored to** minimise the risk of damage to, or contamination of, product.

INTERPRETATION

Suitability of equipment for its intended purpose includes its condition so it does not pose a product contamination hazard; its ability to be effectively cleaned; and its capability regarding the safe handling of products. Where equipment is stored, storage conditions must ensure the safety and integrity of the equipment so that it cannot become a source of contamination; for example, equipment should be stored in a clean condition and in such a way that it does not harbour pests. Movable equipment should be restricted to use in designated areas; for example, equipment used in open product areas should be controlled to prevent contamination risks when moving between different environments.

Effective date: 10 August 2026

POSITION STATEMENT 18

An amendment has been made to clause 6.4.5 to align with the new requirements of GFSI BMR 2024. These changes are shown in **bold** below.

Change to clause 6.4.5

6.4.5	Adequate personnel, facilities and equipment shall be provided to allow cleaning to be undertaken at a level commensurate with the activities being undertaken by the site. **Cleaning equipment shall be:** • **hygienically designed and fit for purpose** • **suitably identified for intended use (e.g. colour-coded or labelled)** • **cleaned and stored in a hygienic manner to prevent contamination.**

INTERPRETATION
Cleaning equipment
Cleaning equipment, including any equipment or utensils used for cleaning activities, must be suitable for the purpose for which it is intended and capable of achieving the desired level of cleaning. For example, equipment would not be suitable if it:

- had the potential to shed fibres
- was not hygienically designed (to facilitate easy cleaning after use).

Cleaning equipment must be clearly identified at all times. This could be done by colour-coding and/or labelling, or any alternative methods that works effectively for the site. This is necessary to ensure that different types of equipment are clearly distinguishable between areas. Cleaning equipment must also be stored hygienically and in a manner that prevents contamination (e.g. stored in designated locations and not in contact with the floor).

Effective date: 10 August 2026

POSITION STATEMENT 19

Further to a review by the BRCGS Storage and Distribution Technical Advisory Committee, an amendment has been made to the title and Statement of Intent of Section 17 to add irradiation. These changes are shown in **bold** below.

Update to Section 17 title and Statement of Intent

17 Contract chilling/freezing/tempering/defrosting/high-pressure process and **irradiation** operations

Where the site undertakes contract chilling/freezing/tempering/defrosting/high-pressure process and **irradiation** operations on pre-packaged product, it shall undertake such operations in accordance with specifications provided by the owner of the product, and ensure that the processes are monitored and that product safety, legality and quality are not compromised.

Effective date: 10 August 2026

POSITION STATEMENT 20

An amendment has been made to clause 17.3 further to a review by the BRCGS Storage and Distribution Technical Advisory Committee. These changes are shown in **bold** below.

Change to clause 17.3

17.3	The process shall be monitored by the use of **adequate process parameters (e.g.: real-time temperature, pressure, irradiation, etc.) recording** equipment linked to an automatic failure alarm system or, where appropriate, manual checks at a suitable frequency which allows for intervention before product temperatures exceed defined limits for the safety, legality, quality or integrity of products.

INTERPRETATION

Adequate process parameters

The alarm settings for process parameter recording equipment shall be adequate for the process being monitored.

Records shall be checked and maintained for a minimum of shelf life + 1 year as they could be required for use in a due diligence defence.

Where automatic temperature recording systems are not used, the manual checks must be continued during non-working periods (e.g. weekends and public holidays). The frequency of manual checks shall be such that the product cannot deteriorate between checks. This will depend on how sensitive the products stored are to temperature variation and how frequently the temperature-controlled storage rooms (cold stores) are accessed. During periods when doors are kept shut (e.g. at night), the frequency of checks may be reduced. As a guide, unless otherwise justified, the frequency should be every 2 hours for chilled products and every 4 hours for frozen products.

Effective date: 10 August 2026