FSR 2026 Guidance Document

References: TAPA FSR 2026 Standard

FSR CFD 2026

TAPA Global Standard

TAPA Facility Security Requirements - Certification Framework Document 2026

TAPA Americas

1353 Riverstone Pkwy,
Ste 120-320
Canton, GA 30114 USA

www.tapaonline.org

TAPA Asia Pacific

10 Anson Rd, #33-15
International Plaza,
Singapore 079903

www.tapa-apac.org

TAPA EMEA

Kanaalpark 140
2321 JV Leiden
The Netherlands

www.tapaemea.org

FSR/CFD Table of Contents

1. Purpose of this Certification Framework Document

This TAPA FSR Certification Framework Document is the official TAPA guidance for Authorized Auditors and LSPs/ Applicants to conduct audits to meet the TAPA FSR 2026 Standard and to obtain certification for all applicable facilities. The certification process is intended to be both functional and practical in economic and operative terms.

The document has been developed exclusively for the TAPA Organization with the intent to achieve conformance and certification to one or more of the following FSR certification options.

2. Scope

To provide additional flexibility and encourage TAPA certifications, TAPA has developed three options to support certification:

a) Single-site Certification by Independent Audit Body (IAB). Each facility is independently certified to the current FSR revision.

b) Multi-site Certification by IAB. Facility operators of 3 or more sites can achieve a Multi-site Certification (a single certificate) for all sites registered in the certification scheme.

c) Self-audit Certification by Authorized Auditors (AA) by LSP/ Applicant or IAB. Each facility is independently self-certified by the operator to Level C of the current FSR revision.

3. Application of the TAPA FSR Certification Framework Document

In the development of this TAPA FSR Certification Framework Document, TAPA recognizes the differences in how storage services are provided globally, regionally, and even within companies, and that the various TAPA Standards may apply to all, or part of the services provided by an LSP/ Applicant. Depending on the complexity and size of the supply chain, compliance with TAPA Standards may be achieved through a single LSP/ Applicant or Multiple LSPs/Applicants and qualified subcontractors.

This Certification Framework Document may apply to the following:

a) Any or all storage locations within the global supply chain, depending on risk and/or Buyer or LSP/ Applicant requirements;

b) LSP/ Applicant owned or operated facilities;

c) Buyer-owned or operated facilities.

Typical users of this Certification Framework Document include:

a) Buyers/ Manufacturers/ Distributors

b) LSPs/ Applicants

c) IABs

d) Law Enforcement or other Government Organizations

e) Professional Supply Chain Organizations.

f) Insurers.

4. TAPA Requirements for Certification and Audit

Facilities are classified into one of three Security Levels, based on the level of protection needed:

a) Level A = Elevated Security Protection

b) Level B = Moderate Security Protection

c) Level C = Standard Security Protection

LSPs/ Applicants or Buyers may initially achieve certification at Level C, and then progress up to Level B or A, as improvements are made. Additionally, as negotiated between Buyer and LSP/ Applicant, facilities located in high-risk areas may be classified at Level A, while all other facilities are classified at Level B or C. In all cases, it is the responsibility of the Buyer to negotiate the Security Level directly with the LSP/ Applicant, depending on their specific cargo and risks.

Organizations may choose the following three options (Table 1) to demonstrate compliance and be certified to TAPA Security Standards.

The LSPs/Applicants shall ensure either an IAB or AA, is engaged to complete the audit and certification process.

Before the certification audit commences, LSPs/ Applicants must:

a) Inform the IAB or AA which Security Level they are seeking in their certification process.

b) Have their own LSP Authorized Auditor (LSP AA) in place.

LSP AA outsourced option:

a) If there is no LSP AA available within the company then they have the right to subcontract to a 3rd party, if the 3rd party meets all the training and certification criteria as outlined by TAPA. The 3rd party must have obtained an AA certification.

Table 1: FSR Certification Options

Type	Options	Level	Auditor Type
IAB Audit	Single-site Certification	A, B or C	TAPA IAB AA
IAB Audit	Multi-site Certification	A, B or C	TAPA IAB AA
Self-Audit	Self-Certification	C	LSP/ Applicant AA or IAB AA, executing a self-audit on behalf of the LSP/Applicant

4.1. Single-site Certification

The single-site scope shall be clearly defined and the IAB will perform an audit based on the scope for the single site. In this situation, the TAPA IAB certifications are site/facility specific. If the TAPA Security Standards audit requirements are all met, the LSP/ Applicant shall be deemed to have passed the audit and the IAB will issue a certificate indicating the LSP's/ Applicant's particular site is now certified to the applicable TAPA Security Standard and level (A, B or C). The IAB will provide TAPA with audit results in the form of copies of certificates issued or notification of failed audits.

4.2. Multi-site Certification

The Multi-site Certification requires the LSP/ Applicant to put in place a single security management system intended to provide confidence and assurance that all sites included in the management system are meeting the requirements of the applicable Standard. The elements required are;

a) An identified Central Function.

b) All sites identified and listed in the certification.

c) Subject to continuous surveillance and internal audits.

4.2.1. The Central Function

The Central Function can, but does not have to be, the headquarters of the LSP/Applicant. However, it must;

a) Be accountable for the single management system.

b) Have the responsibility to ensure that all its sites within the management system are meeting the requirements of the FSR Standard.

c) Have the right to issue corrective and preventative actions when needed at any site.

d) Have a documented formal agreement or policy in place detailing the roles and responsibilities of Central Function and the sites.

4.2.2. The sites

All sites included in the single security management system shall have a relationship amongst each other which can be a legal or contractual relationship with the Central Function of the organization. The relationship cannot be extended to subcontractor sites or facilities being included in the Multi-site Certification System of the Central Function.

4.2.3. Auditing the Central Function

The Certification system audit of the Central Function requires:

a) The selection and use of a TAPA Approved IAB for certification auditing of the security management system.

b) That the IAB audits the Central Function of the LSP/ Applicant annually and its conformance to the single security management system which shall include but is not limited to:

1. Central Function security management system records procedures, policies are sampled.
2. Records available for sites registered in security management system that include hard and/or soft copy audit results and non- conformance management.

c) That the IAB shall issue a TAPA FSR Multi-site certificate to the LSP/ Applicant meeting all the conformance requirements.

d) That the Multi-site certificate shall contain the valid from/ to dates, the number of sites registered in the security management system, security levels at the time of audit and any waivers that may have been granted.

e) The certificate will be valid for 3 years. Years 2 and 3 audits do not require a new certificate to be issued unless the single security management system has significantly changed.

f) The Multi-site certificate shall list all the sites that are part of the management system and the levels of standard that are part of the system.

g) It is not permitted to have sites operating to different versions of the FSR. All sites listed under the certificate will conform to the FSR version specified on the official Multi-site certificate.

h) Should an LSP/ Applicant want to upgrade to the latest version on the FSR before expiry of their existing certificate, then a new certification audit shall be required.

4.2.4. Auditing the sites

Physical sampling audits of the sites will require;

a) That all sites registered in the Central Function single security management system be available for auditing when selected. Note: Any site selected for audit in a 3-year cycle of the certification will not be re-audited.

b) Sites will be physically audited against a sampling basis (Table 2).

c) The sampling consideration will be based on a random selection of 10% of the registered sites per annum.

Multi-Site Certification:

The Interim audits of the Central Function and the sites which are sampled can be done either by a physical visit of the IAB or remotely by the IAB.

Table 2: Multi-site Certification Sampling

	Year 1	Year 2	Year 3
Sample size	10% + CF*	10% + CF*	10% + CF*

*CF – Central Function that is carrying out the central role of managing the security management system

4.2.5. Inclusion of New Sites

The LSP/ Applicant can request the IAB for inclusion of new sites or a new group of sites to join an already certified Multi-site organization, on or before the annual cycle of the IAB site sampling. The IAB shall include these additional sites into the total sites for selection when selecting the sample to be audited.

The LSP/ Applicant shall ensure all new sites have been self-audited and meet the required security level before requesting their addition to the management system. This process must be documented and available to the IAB on request.

If the IAB audit is completed successfully, the IAB re-issues certificates to the Central Function with the new sites included.

4.2.6. Removal of Sites

The LSP/ Applicant can remove sites from the single security management system by removing them from the listing of sites and formally informing the IAB. The IAB shall revoke the individual site certifications and adjust and reissue the Multi-site certificate. The IAB shall note the removal of sites

in the total sites for selection when selecting the sample to be audited.

4.2.7. Change of Status to Existing Sites

The LSP/ Applicant can adjust the security level of existing sites included in the security management system. A request to change the status must be formally sent to the IAB. Sites that are downgraded will be automatically accepted to the lower security level. Sites that are to be upgraded will either be included in that year's sampling audits or require an audit by the IAB if the sampling audits have already been completed or cannot be completed within 60 days.

4.2.8. Transition from Single-site to Multi-site

LSPs/ Applicants that wish to combine any existing single sites into an existing Multi-site security management system must ensure the sites are fully compliant with the same FSR version as listed on the Multi-site certificate. Multi-site cannot incorporate different versions of the FSR standard.

4.3. Self-certification (Level C only)

Self-Certification is only applicable to Level C single-site. Self-Certification (Table 3) must be performed by an LSP/ Applicant AA or alternatively an IAB AA, executing a self-audit on behalf of the LSP/Applicant. An LSP/Applicant AA can be an internal employee/ associate, trained against the current version of the TAPA FSR and registered and authorized by TAPA as an AA or outsourced person/s under contract to perform this role. Regardless of which type of auditor is used to conduct the Self-Certification, the completed Audit Form must be submitted to TAPA to receive the Level C certification.

Table 3: Self-Certification Options

Option	Description	Level	Auditor Type*
Self-Certified	Self-Certification	C	LSP/ Applicant AA or alternatively an IAB AA, executing a self-audit on behalf of the LSP/Applicant

*The audit is carried out using the current TAPA audit template and providing sufficient information/ evidence to provide assurance to TAPA that they are meeting the requirements of the applicable TAPA Security Standard. Self- Certification is site/facility specific. If the TAPA audit requirements are all met, the LSP/ Applicant shall be deemed to have passed the audit and will be certified to level C of the applicable Security Standard for that specific facility location.

In Self-audit certifications, "N/A" entries must always be supported by documented evidence.

5. Re-certification

All TAPA FSR Security Certifications shall be valid for a period of three (3) years with no extension permitted. To prevent any lapse in certification, a re-certification audit must be performed prior to the expiration date of the current certificate. Completion of any SCARs must also occur within the original 60-day allotted period and prior to the current certificate's expiration date.

Therefore, to assure adequate planning and preparation, it is recommended that the LSP/ Applicant schedule the re-certification audit three (3) months before the current certificate expiration date. If the TAPA Security Standard's certificate is issued within the aforementioned three-month period, the date of the new certificate will be the expiration date of the current certification. If corrective actions are not closed prior to the expiration date, and there is no waiver granted, the certification will expire.

Either the LSP/ Applicant or Buyer may request re-certification if either party considers the Classification Level to have changed. Costs for TAPA re-certification are the responsibility of the LSP/ Applicant, unless otherwise negotiated with the Buyer(s).

6. Audit Follow Up

The LSP/Applicant will ensure that they have an internal process in place to monitor compliance, in years between formal audits (see Tables 4, 5 and 6) conducted by an IAB AA or LSP/ Applicant AA as appropriate.

6.1. Corrective Action / SCAR

An informal summary of the findings/results should be shared with the LSP/ Applicant during the audit closing conference. The IAB or AA shall inform the LSP/ Applicant of audit results within ten (10) business days following the completion of the audit. Any delays in issuing the audit results must be promptly communicated to the LSP/Applicant and negotiated between the IAB or AA and LSP/Applicant.

If any of the requirements are not met, as discovered during the audit, the AA submits a Security Corrective Action Requirement (SCAR) to the relevant LSP/ Applicant. The LSP/ Applicant shall respond to the IAB or AA within ten (10) business days, documenting the actions to be taken and the date the action will be completed. SCAR completion dates may be negotiated between the IAB or AA and the LSP/Applicant. However, SCAR completion dates shall not exceed sixty (60) days from the date of notification to the LSP/ Applicant unless the Regional TAPA Waiver Committee approves a waiver. The LSP/ Applicant cannot seek to exclude a site with an open SCAR from the total list of sites in the Multi-site certification scheme.

In all cases, the LSP/Applicant shall submit progress updates/reports on all outstanding SCARs to the IAB or AA. Any SCAR not completed before the due date shall be escalated by the LSP's/ Applicant's Security Representative to the LSP's/Applicant's Management. The reason(s) for noncompliance shall be documented and communicated to the IAB or AA. LSP's/ Applicant's failure to address a SCAR may result in the withholding of the TAPA certification. The LSP/ Applicant has the right to appeal directly to TAPA if the certification is withheld. TAPA shall arbitrate the dispute between the LSP/ Applicant and the AA and retains the right to issue a binding resolution to the dispute.

Note 1: It is not necessary for the IAB or AA to re-audit the facility in order to close a SCAR. Evidence of SCAR closure (i.e., achieving compliance) may be presented to the IAB or AA in the form of written correspondence, web meetings or conference calls, photographs, etc.

Note 2: For Multi-site security management system certification, any SCARs not closed or subject to an approved extension may result in the suspension or revocation of the LSP's/ Applicant's Multi-site certification status and therefore all sites will no longer be considered certified.

6.2. Compliance Monitoring

Interim Self-Audits by the LSP/ Applicant must be completed as per Tables 4, 5 and 6: Audit & Compliance Monitoring Schedules. The interim Self-Audit requirement applies to all sites in all certification options and must be documented on official TAPA Audit Forms and submitted to the IAB or for self-certification to TAPA within 30 days of the anniversary date of the current certification.

Interim Self Audit's must be carried out by LSP's/ Applicant's own AA. All AAs must have taken and passed the applicable exam for the TAPA Standard and version they are required to audit against.

Failure to comply will result in suspension of the original certification until the interim Self-Audit is properly completed. Gaps identified must be documented, assigned a due date for completion of corrective action(s), and tracked to closure within 60 days.

Audit & Compliance Monitoring Schedules

Table 4: Single-site certification

No.	Compliance Activity	Frequency	Levels of Application		
6.2.1.	Single-site Certification Audit (IAB/ AA Certification Audit)	Every three (3) years	Ⓐ	Ⓑ	Ⓒ
6.2.2.	Single-site Interim Self-Audit (LSP/ Applicant AA)	Annually at 1st and 2nd Anniversary	Ⓐ	Ⓑ	Ⓒ

Table 5: Multi-site certification

No.	Compliance Activity	Frequency	Levels of Application		
6.2.3.	Multi-site Central Function Certification Audit (IAB/ AA Certification Audit)	Every three (3) years	Ⓐ	Ⓑ	Ⓒ
6.2.4.	Multi-site Central Function Audit (IAB/ AA)	Annually at 1st and 2nd Anniversary	Ⓐ	Ⓑ	Ⓒ
6.2.5.	Multi-site Initial Self Audit (LSP/Applicant AA for all sites in a Multi-Site Certification)	Pre-certification 1st year	Ⓐ	Ⓑ	Ⓒ
6.2.6.	Multi-site Interim Self-Audits (LSP/ Applicant AA for all sites in a Multi-Site Certification)	2nd and 3rd year	Ⓐ	Ⓑ	Ⓒ
6.2.7.	Multi-site Sampling Audits (IAB/ AA for 10% of sites in a Multi-site Certification)	2nd and 3rd year	Ⓐ	Ⓑ	Ⓒ

Table 6: Self- certification

No.	Compliance Activity	Frequency	Levels of Application		
6.2.8.	LSP/ Applicant Self-Certification Audit	Every three (3) years			©
6.2.9.	Interim Self-Audits (LSP/ Applicant AA for Self-Certification only)	Annually at 1st and 2nd Anniversary			©

7. Waivers

7.1. Overview

A Waiver is a written approval granted to exempt a facility from a specific TAPA requirement and to accept an alternative compliance solution. A waiver may be requested if an LSP/ Applicant cannot meet a specific requirement in the FSR and can justify alternative measures. Waivers are valid for the period of the certification.

All waiver requests for a specific security requirement (either in part or whole) must be submitted via a TAPA Waiver Request form to the Independent Audit Body (IAB) / Authorized Auditor (AA) by the LSP/ Applicant. The requesting LSP/ Applicant takes full responsibility for the accuracy of information provided in the waiver request.

Each waiver request must then be submitted through the IAB/AA to the TAPA Regional Waiver Committee for approval. It is the responsibility of the IAB/ AA to decide if the request is complete and justifies processing by TAPA; this includes verification of mitigating factor(s) and/or alternative security controls.

Should TAPA officials and/or Buyers challenge that waiver conditions have changed, TAPA will complete a formal investigation, and LSP/ Applicant understands that the waiver may be revoked by TAPA.

7.2. Waiver Business Process

If an LSP cannot meet a specific requirement in the FSR, the waiver process below is implemented.

Table 7: Responsibilities: Waiver Application / Evaluation

Step	Responsibility	Action
1.	LSP/Applicant	Establishes and verifies mitigation measures.
2.	LSP/Applicant	Completes TAPA Waiver Request form and submits it to the IAB/ AA.
3.	IAB/AA	Reviews and verifies integrity of the information contained in the TAPA Waiver Request form.
4.	IAB/AA	Submits TAPA Waiver Request form to the TAPA Regional Waiver Committee.
5.	TAPA Regional Waiver Committee	Reviews Waiver request and either grants or denies the waiver.

If Waiver is Denied:

If the TAPA Regional Waiver Committee does not approve the waiver request, the LSP/ Applicant is required to implement the full security requirements of the FSR.

If Waiver is Granted:

If the TAPA Regional Waiver Committee approves the waiver request, the following actions will be taken:

Table 8: Waiver Approval

Step	Responsibility	Action
1.	TAPA Regional Waiver Committee	Documents and signs the waiver specifics.
2.	TAPA Regional Waiver Committee	Specifies the waiver lifespan (up to a maximum of three years) and sends a copy to the AA.
3.	AA	Notifies the LSP/ Applicant of the outcome of the Waiver Request.
4.	LSP/ Applicant	Complies with the waiver requirements. Failure to do so shall void the waiver approval.

7.3. Waivers for Physical Barriers and for High Value Cage

TAPA will consider a waiver to all or part of the perimeter barrier requirements and/or for the HVC if all the following preconditions are met:

General:

- The Waiver request is submitted using the official TAPA Waiver Request form process and is endorsed by the IAB/ AA.
- The waiver request includes details of any mitigating measures to ensure that vulnerable goods are not at unnecessary risk of theft or loss.
- A risk assessment must be completed and submitted with the waiver request. Any significant vulnerabilities identified in the risk assessment must be separately listed in the waiver request and the actions taken to reduce the risk to an acceptable level.

Perimeter barriers:

- Additional equipment, resources and procedures introduced to assist in the timely detection of unauthorized persons or vehicles, may include but are not limited to additional lighting, CCTV coverage, enhanced people and vehicle ID enforcement procedures, LSP vest or uniform only restricted areas.
- The Visible perimeter signs must be installed in local language indicating “No unauthorized access”, “No unauthorized parking”.
- Visible signs on external dock doors or walls are to be installed instructing drivers, visitors etc. to proceed to appropriate lobby, security control.

- Confirmation that procedures are in place ensuring cargo handling, shipping and receiving yard areas are inspected and compliant with waiver conditions at least weekly.

HVC:

- For HVC Waivers the appropriate mitigation actions to minimize risk (where an HVC is not available) must be considered and documented in the annual Risk Assessment.
- The waiver request includes an attached declaration signed by the LSP/Applicant stipulating that no Buyers require an HVC.

Publishing and Copyright Information

This document is published by the Transported Asset Protection Association (TAPA).

The copyright notice displayed in this document indicates the year in which the document was last issued.

Publication History

First published: September 2026

Present edition published in: September 2026

This Publicly Available Specification (PAS) becomes effective on 15 September 2026.

Status of this Document

This document represents the TAPA Facility Security Requirements Certification Framework Document (FSR CFD) – 2026 Revision and establishes the certification framework for facility security within the TAPA certification process.

The document remains valid until it is replaced, revised, or withdrawn by TAPA.

TAPA may issue future revisions, updates, or amendments to reflect evolving security threats, industry practices, and technological developments.

Use of this Document

Compliance with this specification may be used as part of the TAPA certification process for facilities handling high-value and theft-sensitive cargo.

Organizations implementing this specification are responsible for ensuring that all applicable legal, regulatory, and operational requirements are met in addition to the requirements described in this document.