TAPA EMEA
Transported Asset Protection Association

FSR

Facility Security Requirements

Multi-Site Guidance V1

TAPA EMEA
Pastoor Ohllaan 39
3451 CB Vleuten
The Netherlands

www.tapaemea.org
info@tapaemea.org
Tel. +31 619 5734 61

TAPA does not represent nor warrant that the information contained in this document will prevent any loss, damage or injury to a person or property, because of burglary, theft, hold-up, fire or other cause, or that the information will in all cases provide the protection for which it is intended. If the reader chooses to use any information in this document, they assume all risk and liability for doing so.

CONTENTS

FSR 2023

FACILITY SECURITY REQUIREMENTS

TAPA
Transported Asset Protection Association

Certification Framework and Requirements

TAPA
Transported Asset Protection Association

TAPA Facility Security Requirements Certification Framework Document – 2023

A TAPA FSR 2023 Guidance Document

References: TAPA FSR 2023 Standard

TAPA Americas
1353 Riverstone Pkwy,
Ste 120-320, Canton
GA 30114 U.S.A.
www.tapaonline.org
Tel. (561) 617-0096

TAPA Asia Pacific
1 Paya Lebar Link, #04-01, Paya
Lebar Quarter,
Singapore 408533
www.tapa-apac.org
Tel. (65) 6914 0892

TAPA EMEA
Pastoor Ohllaan 39
3451 CB Vleuten
The Netherlands
www.tapaemea.org
Tel. +31 19573461

1. Introduction to the Multi-site certification option

The FSR Standard includes an FSR Multi-site certification option designed to support companies seeking to certify three or more facilities .

FSR Certification Multi-site is an option being introduced into the TAPA Standard based on member and industry requests. T APA was tasked to have a certification system that allowed 1 certificate to cover multiple sites and yet maintain confidence that the standards are being consistently applied.

Independent Audit Body (IAB) Multi-site certification establishes minimum security standards as well as operational and cost efficiencies between multiple sites. It also promotes the sharing of best practices and supports a 'team' approach to obtaining and maintaining compliance with the FSR Standard for risk mitigation and loss prevention.

For companies with multiple FSR certifications, choosing FSR Multi-site should reduce the overall cost by allowing multiple sites to be listed under one parent certification, while still upholding the intentions and integrity of the Standard.

Successful implementation of the FSR Standard is dependent upon service providers, TAPA-approved auditors, and buyers of services working together to accurately interpret, adopt, and audit against these requirements.

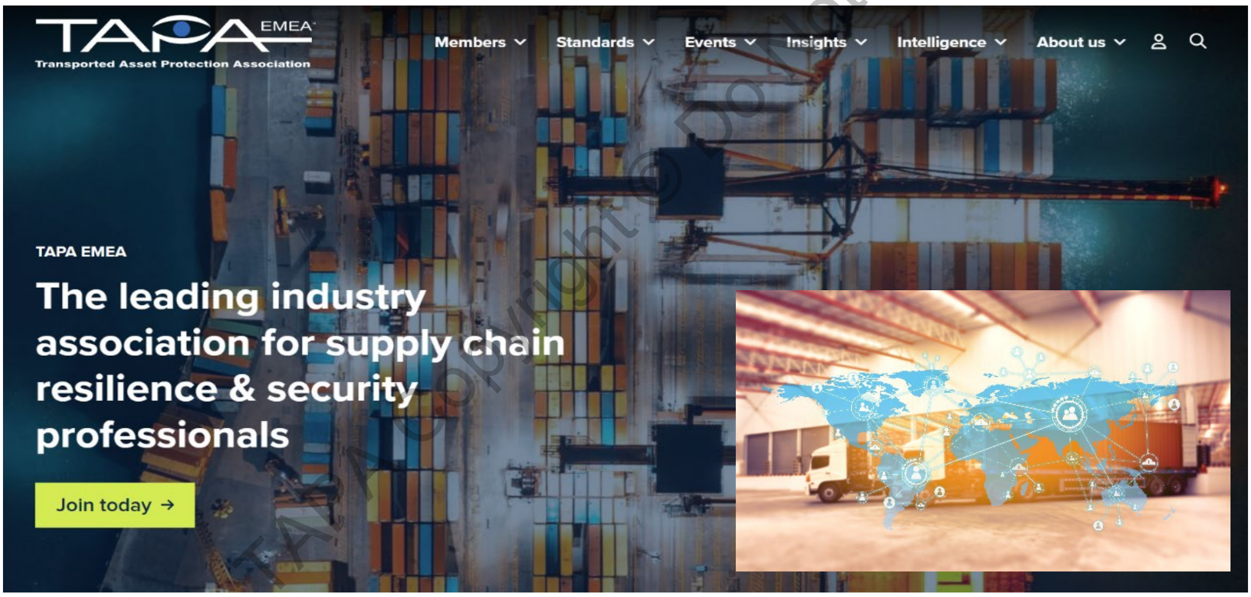
The Multi-site option is intended for organizations: That utilize the FSR standard in 3 or more facilities, but typically it starts to make sense for organizations with 10 or more facilities.

2. About TAPA

Cargo crime is one of the biggest supply chain challenges for manufacturers of valuable and high-risk products and their logistics service suppliers.
The threat is no longer only from opportunist criminals. Today, organized crime rings are operating globally and using increasingly sophisticated attacks on vehicles, premises, and personnel to achieve their aims.

TAPA is a unique forum that unites global manufacturers, logistics suppliers, freight carriers, law enforcement agencies, and other stakeholders with the common aim of reducing losses from international supply chains. TAPA's primary focus is theft prevention using real-time intelligence and the latest preventative measures.

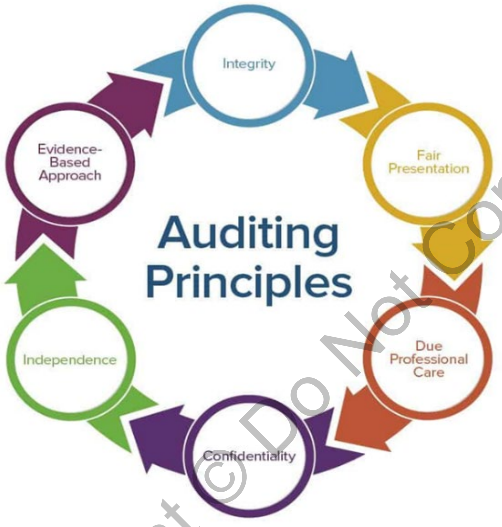
TAPA's Mission:


TAPA EMEA Transported Asset Protection Association
Members
Standards
Events
Insights
Intelligence
About us
TAPA EMEA
The leading industry association for supply chain resilience & security professionals
Join today →

TAPA's mission is to help protect members' assets by minimizing cargo losses from the supply chain. TAPA achieves this through the development and application of global security standards, recognized industry practices, technology, education, benchmarking, regulatory collaboration, and the proactive identification of crime trends and supply chain security threats.

3. What is a FSR Multi-site Certification?

- A Multi-site certification (M-SC) system utilizing the TAPA FSR standard
- A single security management system
- A program for building trust in a robust security management system with appropriate validation controls in place
- Ensure efficiencies and quality are consistently maintained
- Cost-effective benefits
- Transferable processes



Multi-site site FSR certification has the option of combining levels A, B, or C.

It is intended for organizations that utilize FSR in 3 or more facilities, have a single management system in place for security, and must have the capability to provide a central function to oversee the ongoing conformance to the TAPA Standards. The benefits for the M-SC are fewer audits, lower IAB fees, and a single security management system. Lower costs allow for the inclusion of more sites, centralized resource efficiencies, and common standards and practices at all sites.

How?

After you have taken the FSR training and passed the exam you have already taken the first step. The next step is to do your homework and assess each of your sites and ensure they will meet the FSR requirements before the certification audit is scheduled. If some sites cannot be ready in time, you can add them to the Multi-site certificate at a later date.

You should also contact one of the TAPA-approved IABs to agree on an audit scope and pricing agreement. Although you may be trained by TAPA, is there anyone else in your organization (backup) who will be supporting the certification and will also be required to be trained?

Now you can schedule your sequence of audits with your IAB. You may have corrective actions and waivers to process, but once completed you will be awarded your certificate.

Example of a Multi-site Certification:

1 Central function, 12 sites with 6 A Level, 3 B Level, and 3 C Level
Note: *Already self-certified sites (Level C) cannot be included in Multi-site*

Why can the FSR self-certification (Level C) not be included in a Multi-site certification?

FSR Self-certification is only permitted for the FSR C level and is considered to be the entry or minimally acceptable level of compliance to the standard.
The Multi-site option is more complex in terms of the need for a security management system, the use of different security levels, and the mandatory use of the TAPA-approved IAB to ensure a higher level of scrutiny is used before awarding a Multi-site certificate.
Therefore, FSR self-certification is only permitted for single-site operations.

What is the schedule for the Independent Audit Body?

Auditing Central function – every year
12 sites – auditing 10% sample every year
The Annual Review of the 12 self-audits must be submitted by the LSP's Central function and reviewed/ checked prior to the certification process by the IAB and before the central audit function audit takes place.

In case of non-compliance, a Security Corrective Action Requirements (SCARs) needs to be activated by the LSP's Central function

The Central function must manage the SCARs (non-compliances)
SCARs completion dates shall not exceed sixty (60) days
SCARs not actioned on the due date at 1 or more sites may result in suspension/delay of the certificate being issued

What audits are required to achieve an FSR Multi-site certification?

1.
Initial audits (self-audits) should be assigned by the IAB for the first year followed by Interim audits in years 2 and 3. The Central Function is required to complete and submit an audit for each facility that is included in the certificate. **The audit documents of each facility, that is included in the certificate, must be completed and compliant prior to the actual visit of the IAB.** The IAB should review this material as evidence of compliance and ensure the audits were adequate and any corrective actions have been .

2.
Central Function audit. This is required to be completed each year and is completed by the IAB. The audit will focus on your company's security management system. Company policy, procedures, and compliance evidence should all be validated by the IAB

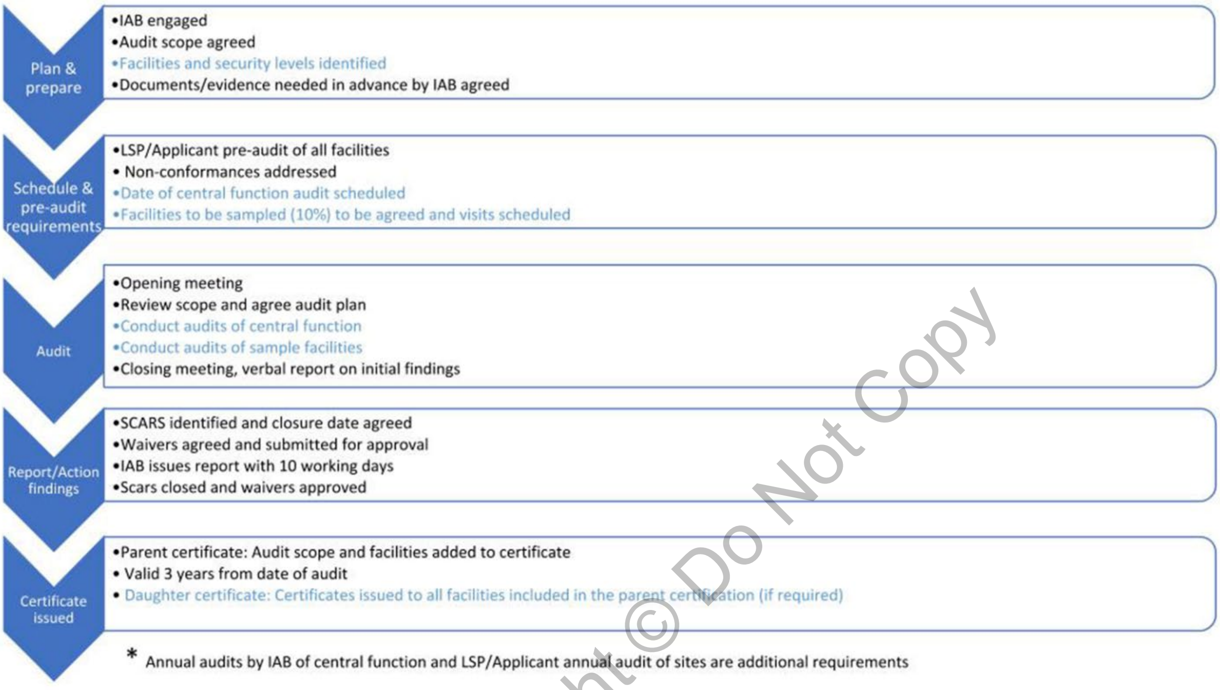
3.
Sampling audit. The IAB is required to inspect at least 10% of sites included in the Multi-site. If it's 20 sites in total, then in the first year 2 sites would normally be selected by the IAB for sampling. In years 2 and 3, another 2 sites for each year would also be sampled.

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

Note: The IAB is capable of using remote auditing techniques; but any auditor conducting remote audits must have either followed the TAPA EMEA Remote Virtual Auditing training (RVA) and/ or is capable/ having experience in the use of remote auditing techniques; photographs, auditing through screen shares, and synchronous and asynchronous videos.

Audit Cycle:

The audit cycle of M-SC is the same as for a single FSR but with some additional tasks:



Plan & prepare
- IAB engaged
- Audit scope agreed
- Facilities and security levels identified
- Documents/evidence needed in advance by IAB agreed

Schedule & pre-audit requirements
- LSP/Applicant pre-audit of all facilities
- Non-conformances addressed
- Date of central function audit scheduled
- Facilities to be sampled (10%) to be agreed and visits scheduled

Audit
- Opening meeting
- Review scope and agree audit plan
- Conduct audits of central function
- Conduct audits of sample facilities
- Closing meeting, verbal report on initial findings

Report/Action findings
- SCARS identified and closure date agreed
- Waivers agreed and submitted for approval
- IAB issues report with 10 working days
- Scars closed and waivers approved

Certificate issued
- Parent certificate: Audit scope and facilities added to certificate
- Valid 3 years from date of audit
- Daughter certificate: Certificates issued to all facilities included in the parent certification (if required)

* Annual audits by IAB of central function and LSP/Applicant annual audit of sites are additional requirements

Points of attention:

Multi-site audits can take longer due to preparation time and reviews of LSP information provided to the IAB.

IAB TAPA account manager/ lead auditor/ central function and/ or other relevant/ included point of contacts should be involved in a good preparation meeting and is critical to a successful audit. Make sure the Central function understands how to complete timely site initial self-audits and how to submit them.

Avoid the use of inexperienced staff to complete and submit self-audits, this can result in audits being rejected or delayed.
Submit initial self-audits before your Central Function audit is scheduled, allowing enough time for the IAB to review and use findings in the CF audit

Identify your pre-audit preparation requirements regarding the actual audit process, documentation, and other evidence, the additional requirements which are required if utilizing the remote audit option, and the potential waivers and need for advance information/evidence.

All audits need to be generated using the official EMEA published audit form template (This template is available on the members page of the TAPA EMEA website). Audits when completed must be submitted to the lead auditor of the IAB and this person has to coordinate further steps with the TAPA EMEA admin team. This can take time for larger operations. Accurate audits mitigate the risk of delays.

The IABs must ensure accurate scoring, relevant comments added, non-conformances addressed, and waivers raised and submitted when applicable.
The LSP's Central function must check report accuracy before submitting.

SCARs/ non-conformances must be addressed in line with FSR requirements. The Multi-site Certificate cannot be issued until SCARs are closed, the same as with the single FSR certificate.

4. General Information

FSR Overview and FSR Certification Framework Document (CFD)

FSR Security Standard

The FSR may apply to the following:

- All storage and handling locations within the global supply chain
- LSP/Applicant-owned or operated facilities
- Buyer-owned or operated facilities

The FSR is a global standard and all sections of the Standard are mandatory unless an exception is granted through the official waiver process.

Standards Revision and Approval Process.
The standard is valid for 3 years.

FSR Classification Levels

The classification level is determined by conducting a local risk assessment of the facility. It can also be influenced by customer(s) requiring a minimum security level:

Level A = Elevated Security Protection
Level B = Moderate Security Protection
Level C = Standard Security Protection

Certification Requirement

Multi-site certification can only be achieved through the audit being performed by a TAPA IAB Authorised Auditor (AA)

Type	Options	Level	Auditor Type
IAB Audit	Single-site certification	A, B or C	TAPA IAB AA
	Multi-site Certification	A, B or C	TAPA IAB AA
Self-Audit	Self certification	C	LSP /Applicant AA or IAB AA

Authorized Auditor (AA)

Requirement:
TAPA requires that an LSP/Applicant has a TAPA-trained employee (LSP AA) from their organization in place before FSR certification audits can be performed.

Remark:

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

  In the EMEA region, the following applies:

- A trained LSP AA is not required at all locations or required to attend certification audits, but they must have an active role in the preparation and ongoing compliance of the certified operation (see also Table 4). If the LSP/Applicant cannot appoint a person from their own staff, they may appoint a non-employee from an agency/consultancy under a specific agreement to perform this role exclusively for them. This must not be an agency/consultancy that offers an LSP AA service to multiple LSP/Applicant clients as this conflicts with the services already provided by the TAPA Approved Independent Audit Bodies and fails to meet the intent of the LSP AA role.

Multi-site Certification

For FSR Multi-site certification, the LSP/Applicant is required to have a single security management system in place.
The objective is to ensure all sites included in the management system are meeting the requirements and provide confidence and assurances of the applicable Standard.

The elements required are:
- An identified central function
- All sites identified and listed within the certification
- Subject to continuous surveillance and internal audits

***Note:** LSP/Applicant sites that do not have operational security compliance reporting to the central function, cannot be included within the Multi-site certification. LSP/Applicant sub-contractor sites cannot be included in the LSP/Applicant Multi-site certification.*

Central Function for the Multi-site Certification

Headquarters can either be that of the LSP/Applicant, or external to the LSP/ Applicant.

Accountable for the single security management system for all sites.

Responsible for ensuring all sites within the security management system are meeting the requirements

Issues corrective and preventative actions when needed at any site.

A documented formal agreement or policy in place that clearly explains the roles and responsibilities of central function and the sites

Contracts/ Contractual agreements

The safe and secure storage and handling of the Buyer's assets is the responsibility of the LSP/Applicant as specified in a written agreement or contract.

Outsourced processes

Vicarious agents/storage partners include a contractual requirement that the outsourced or third-party LSP/applicant meets all of the stated FSR standards. *(As mentioned above; external sites cannot be part of Multi-site certification)*

General Topics

Requirements:

There is a central function to manage the security management system for all sites as defined in the scope of the Multi-site certification

- Centralised function must be actively maintaining compliance with the Standards
- Centralised function focus must be on providing support and expertise to the sites as well as requiring sites to meet their obligations

All sites shall have a legal or contractual relationship with the central function

- Corporate policy, a contract, Service Level Agreement, Standard Operating Procedure, Memorandum of Understanding, are all acceptable formats for detailing the centralized function relationship with the sites

- Organization charts are also a good way to provide evidence but should not be used as the only means to achieve and demonstrate compliance

A single security management system is established to ensure that all its sites within the system are meeting the requirements of the applicable TAPA Security Standard

- The roles and responsibilities for maintaining conformance to the Standard must be clear
- Central function and site roles and responsibilities are agreed and in place
- Measures such as audits, addressing non-conformances, training, and maintenance are all examples of areas for including within the single security management system

The central function and its management system shall be subject to internal audits to ensure continued compliance with TAPA Standards

- The organisation may have its own internal auditing methods and/or can adopt TAPA-provided material
  - The key objective is that a cycle of audits and systems for addressing corrective actions are in place

The central function shall carry out audits of in-scope sites to ensure that each site meets the applicable TAPA FSR requirements. The audits must be done with the appropriate TAPA audit templates.
All the individual yearly site audits must be completed and must be available to the auditor prior to the certification process.

- Audit templates are available, check the TAPA EMEA website for the appropriate template or use your own template covering 100% same requirements.
- Site audit records must be available to AA's on request to provide evidence of maintaining compliance

Note: *some companies are not sharing audit doc's etc prior to the audit. This means that the AA can request it during the audit, it is important that these documents are readily available for review.*

The central function shall have the authority and rights to require all sites comply to TAPA FSR Security Standards and to implement corrective and preventative actions as needed

Note: *Where applicable this should be set out in the formal agreement between the central function and the sites*

- The organisation should seek to adapt existing management practices where possible to achieve this requirement
- Central function and sites may disagree on some aspects of compliance, but the central function is responsible for the resolution

The central function shall maintain documented policies and procedures for its security management systems that are applicable for all its sites

- Policies and procedures must be suitable and sufficient to mitigate the organisations security risks
- Central function policies and procedures must complement and not conflict with site-based policies and procedures

The central function shall ensure that the appropriate policies and procedures are updated, communicated, deployed and implemented at all sites as required

- Annual reviews must be conducted on all policy and procedures. The reviews may not require amendments or updates during each review, however, it is important that annual reviews and any changes are captured within the document history section

Policies & Procedures

Requirement:
The policies and procedures shall be maintained and are easily accessible by all sites as required

- Policy and procedures must be available to the relevant personnel
- Policy and procedures must be available on a “need to know” basis

Note: *Policies and procedures can be communicated/ shared or be available in a digital format and/ or company internal manuals/ postings.*

Self-assessment audit report carried out for all sites

Requirement:
The central function will mandate all sites to carry out self-assessments, all self-assessment reports must be submitted to the central function for records and reviews. Records should be maintained for at least two (2) years.

- Self-assessments can be aligned with other auditing requirements
- Self-assessments do not require a site-based auditor to be used but audit results must be reported to the site

The central function must ensure that all SCARs from the self-assessment and audits are appropriately closed to improve its security management systems. Records should be maintained for at least two (2) years.

- A log of SCARs must be available for operational review and audit inspection purposes

All sites shall submit progress updates and reports on all outstanding SCARs to the central function. The central function will escalate to the LSPs/Applicant's management if SCARs are not completed before the due dates. Records should be maintained for at least two (2) years.

- The communication of SCAR updates between the sites and the central function can be formal (templates) or informal (email updates)
- Actions must be taken, and details documented for missed dates and failure to resolve SCARs

Records of inspections, Risk Assessments, CCTV

Requirement:
The central function shall have procedures in place:

- To ensure all sites maintain records of inspections, visitor logs, driver logs and 7-point inspection etc
- That appropriate risk assessment management and subsequent records is at all sites and are maintained
- That all sites review and maintain documents on physical security systems like CCTV/VSS and alarm layout
- Which records are required, where they are stored including retention periods, must be covered in the central function procedure

Access control, Intrusion detection

Requirement:
All intrusion detection alarm and Access Control systems are maintained and tested to ensure their operational effectiveness
The central function and all sites are responsible for maintaining a record log of all intrusion detection and access control testing, maintenance, and incidents.

- This requirement seeks alignment with the central function management responsibilities and the site responsibilities to test, maintain systems, and keep appropriate records

Training Records

Requirement:
All sites maintain proper training records on security management training of its employees. Records should be maintained for at least two (2) years.

- The central function procedure must cover what records are required, how and where they must be stored and the retention periods for each record

Screening and Vetting

Requirement:
All sites perform screening and vetting of records at regular intervals to ensure the integrity and effectiveness of the security management systems to ensure records of reviews including its findings and corrective/preventive actions are maintained

- Many different factors can complicate the creation of the central function procedure such as local laws, privacy/data protection rights, union or workers council agreements. However, the main objective is to create a procedure that is compliant to local requirements and still sets expectations for sites to perform acceptable screening/vetting checks

Management Review

Requirement:
The central function shall conduct regular management reviews to ensure the compliance, effectiveness, and improvement of its security management systems.
The management reviews shall, at a minimum, cover the effectiveness of self-audits, SCARs closures, risk assessments, incidents, and improvement actions
This requirement can be a stand-alone process or be combined with other management review requirements
Note: *A security management system is an auditable framework of standards and policies designed to protect people, goods, infrastructure, equipment, and transportation. The management system must be designed to ensure all locations work to the same standards and policies.*

The central function must maintain records of all management reviews. Records should be maintained for at least two (2) years.

- The central function should have a process in place to store and access the records
- Annual Business Review Meetings within the company is a possible example, as these are documented and shared with the management

5. Frequently Asked Questions

Can you please explain what audits are required to achieve an FSR Multi-site certification?

- Initial audits (self-audits) should be assigned by the IAB for the first year followed by Interim audits in years 2 and 3. The LSP is required to complete and submit an audit for each facility that is included in the certificate. The IAB should review this material as evidence of compliance and ensure the audits were adequate and any corrective actions have been taken.

- Central Function audit. This is required to be completed each year and is completed by the IAB. The audit will focus on the company's security management system. Company policy, procedures, and compliance evidence should all be validated by the IAB

- Sampling audit. The IAB is required to inspect at least 10% of sites included in the Multi-site. If it's 20 sites in total, then in the first year 2 sites would normally be selected by the IAB for sampling. In years 2 and 3, another 2 sites for each year would also be sampled.

I attended the FSR training and was very interested in the Multi-site option. I could see the possibility of cost savings and I liked the benefit of having a centralized management system for TAPA requirements, this works well with my own company's security management system. What would you advise my next steps should be to combine all sites in the certification?

- As you have taken the FSR training you have already taken the first step. The next step is to do your homework and assess each of your sites and ensure they will meet the FSR requirements before the certification audit is scheduled. If some sites cannot be ready in time, you can add them to the Multi-site certificate at a later date. You should also contact one of the TAPA-approved IABs to agree on the audit scope and pricing agreement.

  Although you may be trained by TAPA, is there anyone else in your organization who will be supporting the certification and will also be required to be trained? Now you can schedule your sequence of audits with your IAB. You may have corrective actions and waivers to process, but once completed you will be awarded your certificate.

I'm interested to know more about how non-conformances are to be processed. It's probable many more non-conformances will come up in a Multi-site than in a single-site audit. If it is agreed with the IAB that corrective actions would be completed within 30 days, but I then find for one of the sites that I need more time, can I still get the certificate before this one site non-conformities are addressed?

- Unfortunately, this is not possible. TAPA certification for all standards requires 100% compliance or waivers to be approved. All non-conformances must be addressed before the IAB will pass the audit and issue a certificate.

I currently have multiple sites FSR certified as single sites, some are FSR A and some are FSR B. I also have other sites that are not yet FSR-certified. I'd like to get these remaining sites certified to FSR C. Which option is better, continue with FSR single site or switch to FSR Multi-site?

- This is an assessment that requires some careful consideration on the part of the operator. In principal TAPA would normally advise that the LSP seeks to use Multi-site as the benefits and efficiencies are then fully optimized. However, there may be practical considerations that are considered that suggest some or all of the sites may not be suitable for the Multi-site. These could include sites operated by different legal entities within the same group, no single security management system in place covering all the sites, or some sites not yet compliant with the FSR standard. Please contact TAPA or your IAB if you need any advice

Why can the FSR self-certification not be included in a Multi-site certification?

- FSR Self-certification is only permitted for the FSR C level and is considered to be the entry or minimally acceptable level of compliance to the standard. The Multi-site option is more complex in terms of the need for a management security system, the use of different security levels, and the mandatory use of the TAPA-approved IAB to ensure a higher level of scrutiny is used before awarding a Multi-site certificate. Therefore, FSR self-certification is only permitted for single-site operations.

If you have any further Multi-site Certification-related questions, please do not hesitate to contact our TAPA EMEA Standards team at the following email address:

standards@tapaemea.org

Publishing and copyright information

The TAPA EMEA copyright notice displayed in this document indicates when the document was last issued.

Publication history

First published in November 2023