Transported Asset Protection Association

Trucking Security Requirements TSR 2023

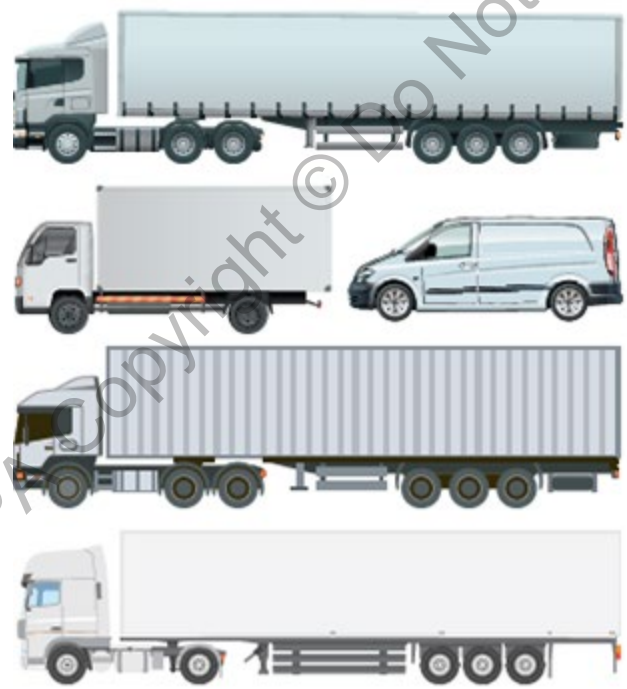
TAPA Standards

TAPA Americas
5030 Champion Blvd,
G-11 #266 Boca Raton,
Florida 33496
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

TSR 2023



TRUCKING SECURITY REQUIREMENTS

Table of Contents

Table of Contents

1.Introduction

1.1 Purpose of this TSR Document

This Trucking Security Requirements (TSR) document is the official TAPA Standard for secure trucking services. It is a common global Standard that can be used in business/ security agreements between Buyers and Logistics Service Providers (LSPs) and/ or other Applicants seeking Certification.

In the development of this Standard, TAPA recognizes the multiple differences in how trucking services are provided globally, regionally, and even within companies, and that the TSR 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.

Scope

The TSR may apply to the following:

- All cargo required to be transported in accordance with the TAPA TSR
- Leased or owned vehicles, trailers or containers utilized for the transportation of cargo by one or more road segments.
- LSP/ Applicant operated, or subcontracted vehicles, trailers or containers utilized for the transportation of cargo by one or more road segments.

Audience

Typical users of the TAPA Standards include:

- Buyers
- LSPs/ Applicants
- Law Enforcement or other government organizations
- Professional Supply Chain Organizations
- Insurers

1.2 Resources to Implement the TAPA TSR

The resources to meet the requirements of the TSR shall be the responsibility of the LSP/ Applicant and at the LSP's/ Applicant's own expense, unless as negotiated or otherwise agreed upon by Buyer and LSP/ Applicant.

1.3 Protecting LSP Policies and Procedures

Copies of security policies and procedures documents will only be submitted to Buyer in accordance with signed disclosure agreements between LSP/ Applicant and Buyer and shall be handled as confidential information.

2.About

2.1 TAPA's Purpose

Cargo crime is one of the biggest supply chain challenges for manufacturers of valuable, high risk products and their logistics service providers.

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 providers, 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 through the use of real-time intelligence and the latest preventative measures.

2.2 TAPA's Mission

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.

2.3 TAPA Contact Information

TAPA consists of three regions (Americas, Asia Pacific, and EMEA) to provide service to all its global members. For more information, please go to:

- Americas:
  www.tapaonline.org
- Asia Pacific:
  www.tapa-apac.org
- EMEA
  www.tapaemea.org

3. TAPA Standards

3.1 TAPA Security Standards

The following global TAPA Security Standards have been created to ensure secure transportation and storage of high-value theft-targeted cargo:

- The Facility Security Requirements (FSR) represents minimum Standards specifically for *secure warehousing, or in-transit storage,* within a supply chain.
- The Trucking Security Requirements (TSR) focuses exclusively on transport by truck and represents minimum Standards specifically for *transporting products via road* within a supply chain.

TAPA global Security Standards are reviewed and revised as needed every three years.

This document addresses the TSR only and explains TAPA TSR Certification in Section 6.

3.2 Implementation

Successful implementation of the TAPA Security Standards is dependent upon LSPs (Logistics Service Providers)/ Applicants, Buyers (owners of the cargo), and TAPA Authorized Auditors working together.

4. Legal Guidance

4.1 Scope

The TSR is a Global Standard and all sections of the Standard are mandatory unless an exception is granted through the official waiver process. (See Section 8.).

4.2 Translation

In geographical areas where English is not the first language, and where translation is necessary and applicable, it is the responsibility of the LSP/ Applicant and its agents to ensure that any translation of the TSR, or any of its parts, accurately reflects the intentions of TAPA in the development and publication of these Standards.

4.3 The "TAPA" Brand

"TAPA" is a registered trademark of the Transported Asset Protection Association and may not be used without the express written permission of TAPA through its officially recognized regions. TAPA Standards and associated material are published through, and by TAPA, and may not be revised, edited, or changed by any party without the express written permission of TAPA. Misuse of the TAPA brand may result in removal of certification or legal action.

4.4 Limits of Liability

By publication of these Standards, TAPA provides no guarantee or assurance that any cargo theft events will be prevented, whether or not the Standards are fully deployed and properly implemented. Any liability that may result from a theft of cargo in transit, or any other loss of cargo in transit under the TSR Standards will be for the account of the LSP/ Applicant and/ or the Buyer in accordance with the terms and conditions in their contract with each other and any laws or statutes which may apply within the subject jurisdiction.

5. Contracts and Subcontracting

5.1 Contracts

The safe and secure transportation, storage, and handling of the Buyer's assets is the responsibility of the LSP/ Applicant, its agents and subcontractors throughout the collection, transit, storage, and delivery, as specified in a release or contract.

Where the TSR is referenced or included in the contract between the LSP/ Applicant and the Buyer, it shall also be referenced in the LSP's/ Applicant's security program.

LSP/ Applicant shall provide the Buyer with evidence of TSR Certification and, where appropriate, evidence that TSR requirements have been met. Further, any alleged failure by the LSP/ Applicant to implement the TSR requirements shall be resolved according to the terms of the contract negotiated between the Buyer and the LSP/ Applicant.

5.2 Subcontracting

Subcontracting of loads includes a contractual requirement that the subcontracting carrier meets all noted TSR Standards.

6. TAPA TSR Certification

6.1 TSR Classification levels

Three Classification levels (for vehicles reported in the Vehicle Register) are specified in the TSR:

- Level 1 = Elevated Security Protection
- Level 2 = Moderate Security Protection
- Level 3 = Basic Security Protection

A combination of classification levels may be used in the certification process. Where Buyers require a minimum classification level for their operations, it is the responsibility of the Buyer to negotiate the classification level required directly with the LSP/ Applicant.

Organization may choose the following four 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:

- Inform the IAB or AA which Security Level they are seeking in their certification process.
- Have their own LSP Authorized Auditor (LSP AA) in place.

LSP AA outsourced option:
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 has obtained a AA certification.

6.2 Pre-Certification

As multiple options are available to obtain certification, a customized audit template available from TAPA is required to be completed to provide the certification audit requirements.

6.3 Modular Requirements

Road vehicle transportation services can involve complex operational and business arrangements. To mitigate security threats, owners of cargo (Buyers) and providers of transportation services (LSP/ Applicant) need multiple options available to specify and maintain minimum but mandatory acceptable security requirements. To address this complexity, TAPA has developed TSR as a modular Standard to allow the industry to select the appropriate transportation mode for their needs.

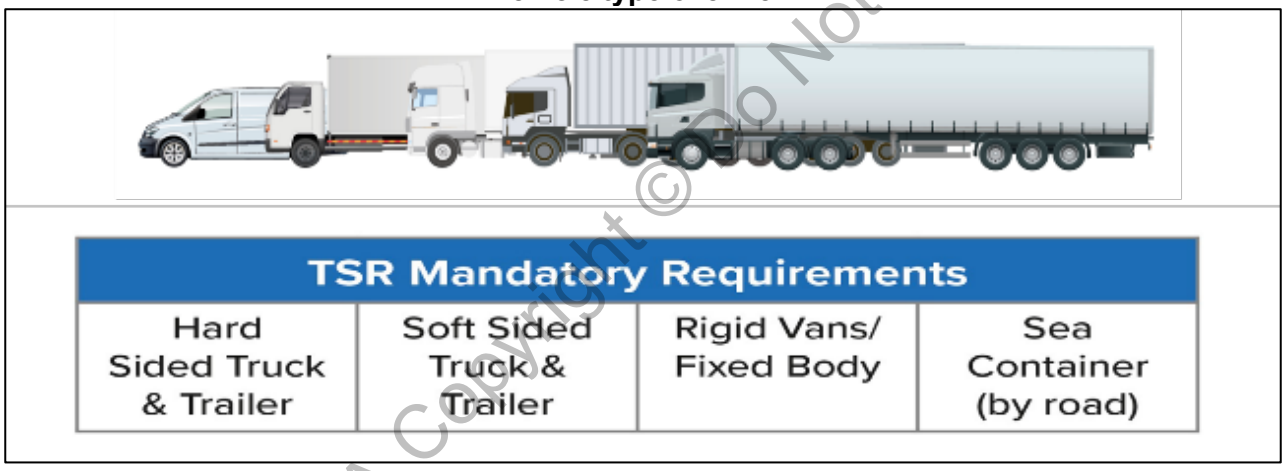
6. TAPA TSR Certification

Achieving the desired and appropriate TSR security certification for road vehicle transportation services may require using a combination of TSR modules and classification levels.

Table 1

Ref#	Module	Description	Level	Auditor Type
6.3.1	Hard sided Truck	Truck + rigid body trailer	1, 2, or 3	IAB AA
6.3.2	Soft sided Truck	Truck + curtain sided trailer	3	IAB AA
6.3.3	Rigid Vans/ Fixed Body Trucks	Van or truck with dedicated cargo compartment	1, 2, or 3	IAB AA
6.3.4	Sea Container	Road transport segment only	1, 2, or 3	IAB AA

Vehicle type overview



IAB Certification (Levels 1, 2, and 3)

If the audit is completed successfully, the IAB issues a certificate indicating the applicant is now TAPA TSR Certified with listings of the appropriate certification levels, operations and locations. The IAB will notify TAPA of the audit results by providing a copy of the certificate issued and other relevant information as formerly agreed between TAPA and the IAB.

6.4 Optional Enhancements

TSR includes optional enhancements that are deemed a higher level of protection which can be used in addition to the modules. Optional enhancements are intended to be selected by the LSP/ Applicant and/ or their Buyer as additional requirements for their operational security needs. When optional enhancements are selected in the pre-certification assessment to be part of the certification audit, all requirements become mandatory.

Table 2

Ref#	Optional Enhancement	Description	Audit Type
6.4.1	Monitoring	Vehicle tracking, alarms and response	TAPA IAB AA
6.4.2	Locking Systems	Locks and systems to protect cargo compartment	TAPA IAB AA
6.4.3	Rail Transfer/ Tracking	Additional validation checks and control measures of vehicles, trailers and/ or sea containers at handover to third party Rail Terminal Operators	TAPA IAB AA
6.4.4	Escorts	Vehicle armed or unarmed escorts subject to local law	TAPA IAB AA
6.4.5	IT and Cyber Security Threat	Mitigation to reduce IT and cyber threats to personnel, networks, vehicles and cargo in road transport	TAPA IAB AA
6.4.6	Cargo Compartment Alarm Device	Protection and alarm devices for the cargo compartment walls	TAPA IAB AA

If the audit is completed successfully, the IAB is to include in the original TSR certificate a listing of the appropriate optional enhancements and for which TSR Certification is it relevant for.

6.5 Self - Certification

Self-Certification (Level 3 Only)

TSR Self-Certification is intended to be a simplified entry level option for TAPA Standards. The person completing the certification audit must be an AA directly associated with the LSP/ Applicant. TAPA will validate the audit submission and issue certificates for a successful audit result.

Only 1 classification level for one operation can be included in a self-certification.

TSR Optional Enhancements are not permitted to be included in TSR Self Certification options.

Level 3 Self-Certifications must be performed by an Authorized Auditor (AA). An AA can be an internal employee/ associate, who has completed training against the current version of the TAPA Standard, passed the relevant exam and is registered by TAPA as a TSR AA.

Table 3 explains the Self-Certification options. All requirements are mandatory.

Table 3

Ref#	Module	Description	Level	Auditor Type
6.5.1	Hard sided Truck	Truck + rigid body trailer	3	LSP/ Applicant AA
6.5.2	Soft sided Truck	Truck + curtain sided trailer	3	LSP/ Applicant AA
6.5.3	Rigid Vans/ Fixed Body Trucks	Van or truck with dedicated cargo compartment	3	LSP/ Applicant AA
6.5.4	Sea Container	Road transport segment only	3	LSP/ Applicant AA

6.6 Vehicle Audits

The AA must physically inspect an adequate number of vehicles. TAPA recognizes that taking vehicles off the road for inspection can be expensive and time- consuming for the LSP/ Applicant.

Thirty days in advance, the LSP/ Applicant must provide to the AA the vehicle register of vehicles to be certified. From this list, the AA chooses a sample of vehicles to be inspected that contains three times the actual number to be inspected. The LSP/ Applicant may then select from this sample list the actual vehicles to be inspected.

To minimize the expense, and yet maintain the validity of the audit process, the following functions must occur:

- LSP/ Applicant must ensure a minimum of three (3) vehicles are included and maintained in their TSR scheme to be eligible for TSR Certification.
- The LSP/ Applicant is required to maintain a Vehicle Register of all vehicles registered under the TSR.
- The Vehicle Register must include any new vehicles added to the fleet since certification/ re-certification.

Size Categories and Inspection Requirements for TSR LSP/ Applicant

The category is an indication of the quantity of vehicles in an LSP's/ Applicant's scheme but can be a combination of different TSR Levels or all the same TSR Level. The intention is to allow LSP/ Applicants to introduce additional vehicles and change classification levels in a flexible but controlled manner.

Table 4: Audit Sample Size: Vehicles

Fleet Size	Number of Vehicles Registered in Vehicle Register	Number of Vehicles to be Audited
Small	3-30	3 of the registered vehicles
Medium	31-100	The greater of 3 or 7% of all registered vehicles
Large	101-300	7% of all registered vehicles with a maximum of 15
Over-Large	301 - above	7% of all registered vehicles with a maximum of 25

6.6.1 Vehicles added to the Vehicle Register after the certification must be included in the annual Self-Audit submission. The sample set is adjusted to accommodate any new increases or reductions.

6.6.2 The sample set of vehicles inspected must include any new vehicles added to the fleet since certification/ re-certification.

6.6.3 The concept of mutual recognition will apply. A TAPA TSR Certified LSP/ Applicant or trucking company may utilize the services of another TAPA TSR Certified company and previous audit results and status will be mutually recognized. No re-audit of a subcontractor's vehicles or services covered by an existing TAPA TSR Certification will be required.

6.6.4 A TAPA TSR Certified LSP/ Applicant or trucking company may "adopt" road transportation vehicles from another subcontractor or subsidiary. This option is intended to allow owner drivers or small operators to be included in the TSR Certification of a larger operator. Each adopted vehicle must be entered into the certification holder's own vehicle register. A formal agreement between the TSR Certified LSP/ Applicant and the subcontractor or subsidiary must in place and define the measures being taken to ensure ongoing conformance of the personnel and vehicles used in the certification. Adoption effectively means the TAPA TSR Certified LSP/ Applicant is wholly responsible for the adopted vehicles' compliance to the TSR.

6.6.5 The AA may request a new inspection if additional vehicles have been added to the Vehicle Register. The total number of vehicles in the Vehicle Register is taken at the time of the yearly Self-Audit. The AA's decision-making criteria for scheduling a new inspection shall include the following:

6.6.5.1 There is an upwards change in the size category (small, medium, large or overlarge) of the LSP/ Applicant, and/ or more than 20 vehicles have been added to the Vehicle register when compared to the previous year's.

6.6.5.2 AA can inspect up to 7% of the vehicles that have been added to the Vehicle Register.

6.6.5.3 AA and LSP/ Applicant to agree the actual vehicles due for inspection in advance.

6.6.5.4 LSP/ Applicant will ensure reasonable efforts are made to facilitate the AA's truck inspection.

6.6.6 Both the Buyer and TAPA reserve the right to conduct their own audits to confirm that all appropriate vehicles in the Vehicle Register meet the requirements of the TSR.

6.7 General Information

Regardless of the business relationships, TSR certified operations must use road transport vehicles that are formally included within one or more parties' TSR certification scheme. Some companies may choose to certify their entire fleet. Others may certify only part of the fleet for certain uses.

A multisite management option and the integration of more than one TSR location is an option available in the TSR 2023 revision and must be coordinated between the interested parties, the IAB, and the regionally responsible TAPA teams in individual cases or if necessary.

The LSP/ Applicant shall ensure the appropriate auditor, trained/ qualified on the current TSR, is engaged to complete the audit and certification process. See Table 1 for options.

Before the certification audit is scheduled/ commences, LSP/ Applicant must inform the AA which classification levels they are seeking in their certification process.

An informal summary of the findings/ results should be shared with the LSP/ Applicant during the audit closing conference. The 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 AA and LSP/ Applicant.

Costs for TAPA certification are the responsibility of the LSP/ Applicant, unless otherwise negotiated with the Buyer(s).

6.8 Re-Certification

The TAPA TSR certificate 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 (see Corrective Action/ SCAR in Section 7).

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 TSR 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.

An LSP/ Applicant or Buyer may request re-certification if either party considers the Classification level to have changed.

7. Audit Follow Up

7.1 Corrective Action/ SCAR

If TSR 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 AA within ten (10) business days, documenting the action to be taken and the date the action will be completed. SCAR completion dates may be negotiated between the AA and the LSP/ Applicant. However, unless the Regional TAPA Waiver Committee approves a waiver, corrective action implementation shall not exceed sixty (60) days from notification to the LSP/ Applicant.

In all cases, the LSP/ Applicant shall submit progress updates/ reports on all outstanding SCARs to the AA. Any SCAR not completed before its 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 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: It is not necessary for the AA to re-audit the company in order to close a SCAR. Evidence of SCAR closure (i.e., achieving compliance) may be presented to the AA in the form of written correspondence, web meetings or conference calls, photographs, etc.

7.2 Compliance Monitoring

Self-Audits

The LSP/ Applicant will ensure they have an internal process in place in order to monitor compliance, in years two and three, in between formal audits conducted by an AA.
The interim Self-Audits must reflect the TSR requirements.

7.1.1 Interim Self Audit's must be carried out by LSP's/ Applicant's own or subcontracted AA.

7.1.2 All AAs must have taken and passed the applicable exam for the TAPA Standard and version they are required to audit against.

7.1.3 For TAPA TSR certifications issued by an IAB: The interim Self-Audit must be documented on the TAPA audit form and submitted to the **IAB** within 30 days of the anniversary date of the original IAB certification.

7.1.4 For Self-Certifications: The interim Self-Audit must be documented and submitted to **TAPA** within 30 days of the anniversary date of the original Self-Certification.

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.

Self-Assessments for Vehicles

Ongoing Assessment

The LSP/ Applicant must have documented evidence that all subsequent Self-Assessments (fixed or rolling program, covering all vehicles listed in the TSR Vehicle Register) are completed at least once every 12 months by the LSP/ Applicant. Associated records are retained for audit purposes.

Table 5: Audit & Compliance Monitoring Schedule

Action	Frequency	A	B	C
Certification Audit (IAB/ AA Certification Audit)	Every three (3) years	✔	✔	✔
LSP/ Applicant Self-Certification Audit	Every three (3) years			✔
Self-Audits (interim compliance checks)	Annually at 1st and 2nd Anniversary	✔	✔	✔
LSP/ Applicant Subcontractor Audit	In accordance with Buyer- LSP/ Applicant contract	✔	✔	✔

Buyer Visits to LSP/ Applicant

The Buyer and the LSP/ Applicant recognize the importance of working in partnership to reduce risk within the supply chain. Both parties agree to schedule Buyer visits with reasonable notice; e.g., 10 business days, with scope and parameters mutually agreed upon in advance and/ or in accordance with the Buyer-LSP/ Applicant contract. Loss investigations; i.e., thefts, damage, etc., shall be performed in accordance with the Buyer- LSP/ Applicant contract.

7.3 TAPA Complaint Investigation and Resolution

If TAPA receives a formal complaint concerning the performance of a certified LSP/ Applicant, TAPA (subject to validation) may require that the LSP/ Applicant contract for a re-audit at the LSP's/ Applicant's expense. If the LSP/ Applicant fails the audit, or refuses to comply with this process, their certificate may be withdrawn.

8. Waiver

8.1 Overview

A waiver is a written approval granted to either exempt a company from a specific TAPA requirement or to accept an alternative compliance solution. The waiver request must be completed using the current official version of TAPA Waiver Request Form. The form can be accessed via the TAPA website. A waiver may be requested if an LSP/ Applicant cannot meet a specific requirement in the TSR 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 (TAPA Waiver Request form). 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.

8.2 Waiver Business Process

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

Table 6: 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 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 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 TSR.

If Waiver Is Granted

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

Table 7: 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.

9. Appendixes

See refer to the appendixes for the requirements for the choice of certification category.

Appendix A: Hard Sided Truck

Appendix B: Soft sided Truck

Appendix C: Rigid Vans/ Fixed Body Trucks

Appendix D: Sea Container

10. Enhanced Options

10. TSR Enhanced Options

Section	*Monitoring – Enhanced Option*
A	***Mandatory Requirements***
A.1	Alarm Monitoring Center Roles, Responsibilities and Capabilities
A.1.1	The Alarm monitoring center (AMC) must be adequate for its intended purpose and be pre-approved for use by the LSP/ Applicant or Buyer. 1. AMC is approved and registered as a lawful business operation as required by local country requirements. * 2. AMC shall have the appropriate licenses to operate as an alarm monitoring/ receiving center. *Notes:* *a. *The LSP/ Applicant can utilize an external AMC (contracted) or an internal AMC (own staff). However, all requirements are applicable to external or internal managed AMC operations. Exceptions to this requirement need the approval of TAPA as per the standard waiver process. LSP's/ Applicant's and their customer's support for the waiver must be submitted with the waiver.* *b. Where more than 1 AMC is required to be involved in alarm monitoring and event response, the secondary AMC must have a contract in place with the primary AMC be included in the certification and meet the monitoring enhancement requirements. The appropriate AMCs should test their coordinated activation and response procedures at least annually.*
A.1.2	AMC must be a permanent facility and of strong construction. 1. AMC should be adequately protected with physical security measures in place (access control, door locking, intruder alarms, CCTV, badge and visitor procedures) to protect employees, information and operations from any negative external natural or man-made influence, including a criminal attack. 2. AMC to have a minimum of one duress alarm button installed in monitoring room, connected to reliable external security company or LEA. Escalation procedure includes immediate call of security company/ LEA and password / duress code for monitoring staff. Process to be documented and tested every three months. 3. The AMC will have robust and reliable connections to water and electrical power.
A.1.3	The location and operation of the AMC is to be risk assessed at least annually. 1. The risk assessment is to be documented and reviewed by AMC management. 2. The risk assessment shall include an evaluation of countermeasures, action plans, crisis management and business continuity plans for all identified risks and emergencies.
A.1.4	The AMC must have adequate procedures to safeguard its staff and ability to maintain operations. 1. Operation of the AMC shall be governed by site operating procedures that require annual review and updating as appropriate.

10. Enhanced Options

Section	Monitoring – Enhanced Option
A	*Mandatory Requirements*
	2. Escalation procedures for activation of duress alarm implemented and includes immediate contact with external security company and/ or LEA. Password and/ or duress code for monitoring staff feature enabled. Process to be documented and tested every three months. 3. A system of tests of vehicle monitoring alarms to evaluate strengths and weaknesses in the management of alarms and systems shall be completed at least twice each year. 4. A documented maintenance plan for all critical systems. 5. The roles and responsibilities of the AMC monitoring operators shall not be diluted by adding non-AMC related duties. 6. Management and staffing levels must be assessed as adequate to perform the required roles and responsibilities.
A.1.5	Documented AMC staff training program in place and records of training in place. Must cover: 1. New hire orientation training 2. Technical system functionality training 3. Annual schedule of training and retraining requirements of all relevant emergency and standard operating procedures 4. Protocols for communications with LSP/ Applicant 5. Confidentiality of data and protecting intellectual property
A.1.6	Own and agency staff vetting procedures to include checks on employment history, gaps in employment, criminal convictions, job terminations in similar/ same industry, job related qualifications (within constraints of local law).
A.1.7	AMC has robust vehicle pre-departure procedures. 1. Ensure adequate system checks are performed to validate signaling and monitoring devices are in working order. 2. Procedures in place for dealing with faults and notification to appropriate own/ LSP/ Applicant management. *Note:* *Communication checks with drivers and their escorts if present are advised*
A.1.8	The AMC must have procedures in place to ensure alarm activation events are processed timely and effectively 1. Able to timely respond to multiple events simultaneously. 2. Events must be categorized and target time to respond set for each category. Highest priority alarms must be responded to within 2 minutes of activation. 3. AMC has response protocols to monitor of all required vehicles, sensors and alarms as required by the LSP/ Applicant. A record of alarm activations and GPS alert signals received, and the actions taken must be recorded. 4. If AMC or LSP/ Applicant provided vehicle monitoring systems are used, the AMC must have unique identifiable access for secure login. 5. Procedures and contact details in place to escalate vehicle alarms to the appropriate responders.

10. Enhanced Options

Section	*Monitoring – Enhanced Option*
A	***Mandatory Requirements***
	These must include: a. The vehicle driver b. National and/ or local LEA Also, where provided and applicable c. AMC central or local resources d. AMC contracted service partners e. Vehicle escort provider f. LSP central or local resources 6. AMC to have access to contact details of appropriate LEA in every country and for every leg along the route (not only generic emergency number of countries) and intervention partners capable to support in any type of emergency. 7. A daily review of monitoring quality, alarm receiving, and escalation protocols is performed and recorded. 8. Any system faults or deficiencies must be recorded, and evidence of correction recorded. 9. Any operational errors or failure to follow procedure must be explained, a record of the event maintained and any corrective actions taken. 10. Alarm management KPIs and statistics to be available for audit by AMC management and pre-authorized LSPs/ Applicants. 11. All historical data for route alarms and actions taken must be available for at least 30 days. *Notes:* *a) A system to classify all alarms should be in place. Highest priority being any life/ injury threatening alarms.* *b) The alarm state must be escalated or de-escalated as appropriate.* *c) Procedures to contact the driver during an alarm event must be in place.* *d) Code words or phrases to validate the driver's situation may be required but must not put the driver's safety at risk.*
A.1.9	AMC procedures shall ensure the capability to handle communication in multiple languages: 1. Capability to talk to vehicle drivers and/ or emergency services in a language that is mutually spoken or through an interpreter or an effective mechanism/ device. 2. AMC language communication options must be available for the routes of the vehicles being monitored. 3. AMC language communication options must be clearly described in an appropriate procedure or protocol. Must include an exception process when mutual language communications are not possible.
A.1.10	AMC uses unique identification and tracking capability for each vehicle.
A.1.11	AMC will track location of vehicles in real time or at intervals that have been pre-agreed with the LSP. *Note: Process to ensure LSP/ Applicant requirements are implemented and maintained to be in place*

10. Enhanced Options

Section	*Monitoring – Enhanced Option*
A	***Mandatory Requirements***
A.1.12	AMC documented procedures for receiving and responding to vehicle monitored devices shall be in place. These should include: 1. Driver cabin intrusion alarm 2. Fixed and mobile duress alarm 3. Unauthorized Stop 4. Where trailer utilized. Disconnection of the Trailer 5. Unauthorized cargo compartment door opening 6. Route deviation (geofencing alarm) 7. Voice communication loss 8. Tracking signal loss 9. Tracking device tampering 10. Battery status alarm
A.1.13	The AMC shall be able to demonstrate that it can adequately deal with the LSP's/ Applicant's and/ or their clients customized requirements for monitoring, responding and notification to alarm activations. *Note: It is sufficient for the AMC to provide examples of customized plans to support conformance to this requirement.*
A.1.14	The AMC shall maintain listing of locations where the AMC has the capability to provide a local response team to attend an incident in addition to an LEA response or where LEA cannot respond. The incident response capability will be documented in AMC procedures. Locations not listed will be deemed to not have a local response team capability.
A.1.15	AMC has a credible business resilience and continuity plans in place that ensures: 1. AMC has completed a risk assessment and produced a report that addresses business continuity plans to cover a range of emergencies. These shall include but not be limited to fire, flood, denied access to the AMC, cyber-attack. 2. Local battery backup systems in place that shall be sufficient to power critical AMC monitoring and communication equipment for at least 10 mins. 3. AMC has measures in place to ensure uninterrupted power supply to servers and monitoring equipment. Site standby power supply shall be by a generator or generators supported by an UPS according to EN 62040-1 or an equivalent standard. The generators shall be provided with a fuel supply on site sufficient to operate the generator for at least 24 hours. 4. Procedure in place to ensure the AMC can defend against a cyber-attack on its critical data systems. Actions to recover systems identified in the event of a successful cyber-attack.
A.2	LSP/ Applicant Roles and Responsibilities
A.2.1	A formal agreement between the LSP/ Applicant and the AMC must be in place. The agreement must include references to: 1. An overview of the LSP's/ Applicant's operational needs.

10. Enhanced Options

Section	*Monitoring – Enhanced Option*
A	***Mandatory Requirements***
	2. AMC and LSP/ Applicant service levels 3. A list of procedures or protocols to be covered in the agreement. 4. Information/ data that must be or cannot be shared. 5. LSP/ Applicant authority to conduct audits of the AMC operations. 6. AMC permitted communications with LSP/ Applicant, LSP's/ Applicant's clients and LSP's/ Applicant's service partners.
A.2.2	A process to review and make timely changes to the formal agreement between the LSP/ Applicant and the AMC must be in place. This should cover: 1. How to implement small operational corrections to the business requirements. 2. Identifying and implementing major changes to the business requirements due to operational need or risk driven events and threats.
A.2.3	The driver shall have documented procedures available and provided by the LSP/ Applicant. Requiring: 1. Vehicle cargo compartment door alarms activated and working. 2. Immediately prior to loading, all installed tracking devices activated and working. 3. All alarm events that the driver should recognize and respond to. These should include: a. Driver cabin intrusion alarm b. Fixed and mobile duress alarm c. Unauthorized Stop d. Where trailer utilized. Disconnection of the Trailer e. Unauthorized cargo compartment door opening f. Route deviation (geofencing alarm) g. Voice communication Loss h. Tracking signal loss i. Tracking device tampering j. Battery status alarm
A.2.4	LSP/ Applicant shall provide specific route details and information that the AMC must monitor for compliance. These shall include. 1. Detailed or general route plans. 2. Driver name and contact details. 3. Any authorized parking areas for overnight or rest stops. 4. Vehicle details (incl. License Plate No.). 5. Expected time of loading/ departure. 6. Expected time of arrival/ unloading. *Note: A process to provide this information shall be documented and available for inspection if required.*

10. Enhanced Options

Section	Locking Systems – Enhanced Option	1. Hard sided Truck & Trailer Req's	2. Soft sided Truck & Trailer Req's	3. Rigid Vans/ Fixed Body Trucks	4. Sea Container Road Transport
B	***Mandatory Requirements***				
B.1	Internal or protected door hinges on cargo compartment doors.	✔	N/A	✔	N/A
B.2	Cargo compartment doors cannot be opened independently, first door must hold the second door in place.	✔	N/A	✔	N/A
B.3	Cargo compartment fitted with internal rear door lock-down system, operated remotely.	✔	N/A	✔	N/A

10. Enhanced Options

Section	Rail Transfer/ Tracking – Enhanced Option
C	Mandatory Requirements
C.1	Risk Assessment
C.1.1	The LSP/ Applicant must complete risk assessments of the departure and arrival rail terminals to be used. Security threats are to be identified and the LSP/ Applicant and/ or Rail Terminal Operator(s) mitigation actions to minimize threats that could result in freight loss must be recorded. The risk assessment shall include as a minimum: 1. The Risk Assessment process must be documented and require LSP/ Applicant management to make informed decisions about any vulnerabilities and if mitigation is sufficient. 2. Must be conducted/ updated at least annually. 3. Assessment of common threats shall include: a. Theft of cargo, containers or vehicles. b. Theft or duplication of information that could be useful for a deception event. c. Unauthorized access to terminal facilities and external areas. d. Cargo tampering. e. Effectiveness of Security systems. f. Procedures to deter/ prevent fictitious pickups of cargo g. Security continuity during workforce shortages or natural disasters, etc. *c. Note: This information shall be available to the Buyer if requested.*
C.2	HVTT Procedures
C.2.1	LSP/ Applicant and Rail Terminal Operator(s) will have a formal agreement in place for handling any FTL vehicles, trailers or containers declared to the Rail Terminal Operator by the LSP/ Applicant as “HVTT or vulnerable loads”.
C.2.2	LSP/ Applicant will agree, document and implement operating procedures with the Rail Terminal Operator(s). These will include: 1. Departing terminal handover (LSP/ Applicant) a. Vehicle/ trailer/ Container checks on arrival at the terminal. b. Integrity checks – Seals and locks intact, no evidence of tampering. 2. Documentation correct and signed c. Pre-departure checks (Rail Terminal Operator). d. Safe storage and monitoring prior to placement on train. e. Integrity checks – Seals and locks intact, no evidence of tampering. 3. Rail in-transit procedures (Rail Terminal Operator) f. Procedure in place to communicate lengthy delays and diversions to LSP/ Applicant. g. Mitigation options defined in case of security incidents, train operator’s staff shortage/ illness, train breakdown, strikes, accidents, bad weather.

10. Enhanced Options

Section	*Rail Transfer/ Tracking – Enhanced Option*
C	**Mandatory Requirements**
	h. Vehicle/ trailer/ Container checks on arrival at the terminal. i. Integrity checks – Seals and locks intact, no evidence of tampering. 4. Arriving terminal checks and handover (LSP/ Applicant) j. Vehicle/ trailer/ Container checks on arrival at the terminal. k. Integrity checks – Seals and locks intact, no evidence of tampering. l. Documentation correct and signed. m. Pre-alert process to next destination defined and in place. 5. The LSP/ Applicant will have a procedure agreed with the Rail Terminal Operator for communicating emergencies and escalation of events. This procedure must be in operation 24/7. 6. The LSP/ Applicant will ensure training procedures are in place and adequate to cover the roles and responsibilities of LSP's/ Applicant's own operation. 7. The LSP/ Applicant will ensure the Rail Terminal Operator's own training procedures are in place and sufficient to cover the roles and responsibilities of the Rail Terminal Operator(s) own operation.
C.3	Investigations
C.3.1	The LSP/ Applicant shall have an agreement with the Rail Terminal Operator on the minimal level of cooperation and information sharing that will be required between LSP and the Rail Terminal Operator. This shall include, but not be limited to: 1. Time limits for Rail Terminal Operator to report missing or lost freight to the LSP. 2. Known details of loss and investigation status are provided in a first alert. (location, modus operandi, investigations status and where engaged, details of LEA response. 3. Mutual decision making process for closing freight loss incident as resolved or unresolved. *Note: Details of this agreement must be provided to the Buyer if requested.*
C.4	Use of Tracking Equipment
C.4.1	Where LSP/ Applicant or Rail Terminal Operator's electronic tracking systems are required and used to track the LSP's/ Applicant's vehicle, trailer or container during transport by rail or storage within the rail terminal a procedure to cover monitoring and response actions must be agreed between the LSP/ Applicant and the Rail Terminal Operator. *Note: Details of this agreement must be provided to the Buyer if requested.*

10. Enhanced Options

Section	Escorts – Enhanced Option
D	***Mandatory Requirements***
D.1	Escort Company Service Levels
D.1.1	A formal agreement between the LSP/ Applicant and the Escort provider must be in place. The agreement must include references to: 1. An overview of the LSP's/ Applicant's operational needs. 2. Escort providers and LSP/ Applicant service levels. 3. A list of procedures or protocols to be covered in the agreement. 4. Information/ data that must be or cannot be shared. 5. LSP/ Applicant authority to conduct audits of the Escort provider's operations. 6. Escort provider's permitted communications with LSP/ Applicant, LSP's/ Applicant's clients and LSP's/ Applicant's service partners.
D.1.2	A trained and recognized internal resource or external security company must be utilized for escort of road transport vehicles. *Note: Where external, this service must be carried out by a professional organization with relevant certification from local Security Guarding and/ or national authorities.*
D.1.3	An escort service must be available to the LSP/ Applicant. Documented procedures to be available and readily implemented to use will include: - 1. Escort vehicles must be: a. Well maintained as per manufacturer's and regulatory requirements. b. Fully fueled and have completed detailed pre-departure checks before being approved to accompany the transportation vehicle. c. Have a one push and/ or voice activated duress alarm device fitted to the vehicle. A portable device with the same functionality and purpose carried by security personnel, linked to home base/ AMC is an acceptable alternative. d. Real time voice communication available with the transportation vehicle's driver, the escort company home base and the third-party AMC (where tracking/ monitoring equipment is installed on vehicles to be escorted).
D.1.4	An overt and/ or covert escort service must be available to the LSP/ Applicant. Overt escort vehicles will have appropriate markings indicating they are a private security vehicle. Covert escort vehicles will have no visible makings.

10. Enhanced Options

Section	*Escorts – Enhanced Option*
D	*Mandatory Requirements*
D.2	Escort Personnel
D.2.1	Escort personnel must be professionally trained and competent. The minimum requirements include: 1. While on assignment wearing the standard uniform of the escort provider and/ or high visibility vests so they are readily identifiable as security personnel. 2. Carry official company and personal ID to satisfy enquiries from LEA or other regulatory authorities. 3. Passed an employment and/ or aptitude test ensuring their suitability for the intended role and the ability to perform all required duties. 4. Having training and retraining records on all aspects of the role being performed covering: Emergency response, security escort patrol protocols, alarm/ fault response, communication with law enforcement agencies and management. 5. Hiring process requires vetting/ screening/ background check.
D.3	Escort Company Procedures
D.3.1	A process to review and make timely changes to the formal agreement between the LSP/ Applicant and the Escort Provider must be in place. This should cover: 1. How to implement small operational corrections to the business requirements 2. Identifying and implementing major changes to the business requirements due to operational need or risk driven events and threats.
D.3.2	The carrying of firearms is permissible only when all the following conditions are met and when a robust policy covering these conditions is available and in place. 1. Local laws allow the carrying of firearms and the escort resource is fully compliant to all regulatory requirements. 2. Evidence available indicating cargo owners and LSP/ Applicant agree to the escorts carrying firearms. 3. Escort company has a risk assessment promoting the need to carry firearms and the conditions when they can or cannot be used. 4. All escort company personnel involved in the procurement, maintenance, storage, staff training and carrying of firearms meet the local legal and regulatory requirements. Evidence of this to be provided to the Authorized Auditor.

10. Enhanced Options

Section	IT and Cyber Security Threat – Enhanced Option
E	***Mandatory Requirements***
E.1	The LSP/ Applicant must have security policies for IT and cyber threat. The policies can be documented in separate or a combined document. The policies must explain: - 1. The actions of the LSP/ Applicant to identify and respond to threats. 2. The policies and procedures in place to protect, detect, test, and respond to security events. 3. The methods for the recovery of IT systems and/ or data. 4. The communications protocol to Buyers/ Clients to mitigate supply chain impact within 24 hours of knowledge of incident. 5. How the policies are reviewed annually and updated as appropriate.
E.2	The LSP/ Applicant must have a training program providing information security awareness training to employees. This training must: - 1. Cover the roles and responsibilities that computer users have in maintaining security and the associated benefits. 2. Have a system in place that ensures records of persons receiving training are maintained and retained for a minimum of2 years.
E.3	The LSP/ Applicant must have a written policy in place for ensuring Cyber Security measures are in place with subcontractors and / or vendors that ensure: 1. LSP's/ Applicant's Cyber Security requirements are communicated to subcontractors and / or vendors and embedded in agreements. 2. Where subcontractors and / or vendors do not recognise or refuse to adopt LSP's/ Applicant's Cyber Security requirements, measures are documented and in place that mitigate the risks to the LSP's/ Applicant's Cyber Security requirements and their customers.
E.4	The LSP/ Applicant must have a plan in place for Power Interruption Mitigation that maintains power for at least 48 hours for critical IT systems, i.e., power supply or backup generator.
E.5	LSP's/ Applicant's Information Systems must have licensed anti-virus and anti-malware software installed. The anti-virus and anti-malware software must contain the latest updates.
E.6	LSP/ Applicant must have appropriate I.T. Disaster Recovery Plan (DRP) for recovering from compromised system attacks, including but not limited to, all necessary data and software back-up and recovery arrangements.
E.7	LSP's/ Applicant's Information Systems must be backed up. Such backups must be tested routinely, and backup data must be encrypted and transferred to a secondary, off site location.

10. Enhanced Options

Section	*IT and Cyber Security Threat– Enhanced Option*
E	***Mandatory Requirements***
E.8	LSP/ Applicant must implement a policy for all user accounts to manage and control access to Information Systems by using unique individual identifiers and strong passwords. Procedures in place to ensure: 1. Password compliance audit program in place. 2. An initial unique password must be assigned to each new account at the time of creation. 3. Initial passwords cannot contain the user's name, identification number or otherwise follow a standard pattern based on user information. 4. Passwords will be communicated to users in a secure manner, and only after validating the identity of the user. 5. Users must be required to change passwords on initial login. 6. Passwords must be changed at least every 90 days.

10. Enhanced Options

Section	Cargo Compartment Alarm Devices – Enhanced Option	1. Hard sided Truck & Trailer Req's	2. Soft sided Truck & Trailer Req's	3. Rigid Vans/ Fixed Body Trucks	4. Sea Container Road Transport
F	*Mandatory Requirements*				
F.1	The cargo compartment is properly equipped/ protected to detect a breach of the cargo compartment through the side walls, roof, front, and back. Such technology must include alarm loops or integrated netting. *Note: Motion detection or light sensors can´t replace the physical installation of the above-mentioned alarm devices.*	✔	N/A	✔	N/A
F.2	The cargo compartment tracking device or the vehicle tracking/ telematic system(s) must be able to send/ transmit any cargo compartment breach alarm in real time to the monitoring center (AMC).	✔	N/A	✔	N/A
F.3	Documented response protocols for cargo compartment breach alarm in place, updated and tested at least every six months.	✔	N/A	✔	N/A
F.4	Training of drivers and AMC personnel on application of related response protocols. This training must be provided before driving a load of HVTT goods and thereafter every two (2) years.	✔	N/A	✔	N/A

Publishing and copyright information

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

Publication history

First published in August 2023

First (present) edition published in August 2023

This Publicly Available Specification comes into effect on 15th September 2023