

## Global Security Verification Report

### Facility Name: SHANGHAI YALIAN INTERNATIONAL LOGISTICS CO.,LTD

Country:	China	Assessment Stage:	Annual
Date of Verification:	22-May-2020	Report Number:	A4843901
Last Verification Date:		Site ID:	F_IAR_84274
Auditor Primary:	lincoln lin	Service Provider:	Intertek
Auditor Secondary:	NA		

### OVERALL FACILITY SCORE

81%



### PERFORMANCE INDEX BAR

The Bar is used to measure and benchmark the facility's score against the other population of audit results in the database. The overall score represents a % deduction in the number of findings across the entire checklist based on importance weight.



### Participating Facilities: 349

The C-TPAT Security Criteria and Guidelines indicate that "Must" is a requirement of the program participation. "Should" means that the procedure is considered to be an industry "best practice."

### PERFORMANCE SUMMARY

Section Name	Score	Must - High	Must - Low	Should - High	Should - Low
Security Vision and Responsibility	100%	0	0	0	0
Risk Assessment	85%	0	2	0	0
Business Partners	100%	0	0	0	0
Cyber Security	79%	0	2	1	0
Conveyance and Instruments of International Traffic Security	93%	0	0	1	0
Seal Security	100%	0	0	0	0
Procedural Security	100%	0	0	0	0
Agricultural Security	100%	0	0	0	0
Physical Security	86%	0	0	3	1
Physical Access Controls	100%	0	0	0	0
Personnel Security	100%	0	0	0	0
Education, Training and Awareness	82%	0	1	1	0
OverAll	81%	0	5	6	1

Intertek's GSV integrates multiple global supply-chain security initiatives, including C-TPAT (Customs Trade Partnership Against Terrorism), PIP (Partners in Protection) and AEO (Authorized Economic Operators).

# Global Security Verification Report, SHANGHAI YALIAN INTERNATIONAL LOGISTICS CO.,LTD

## A. FACILITY PROFILE

### A1. FACILITY INFORMATION

Facility Name:	SHANGHAI YALIAN INTERNATIONAL LOGISTICS CO.,LTD	Contact Name:	Mr. Zhao Wanli
Facility Legal Name:	Shanghai YaLian International Logistics Co., Ltd.	Contact Title:	MANAGER
Audit Location:	No.27, Jinwen Road, Pudong New Area, Shanghai	Email:	379073879@qq.com
City:	Shanghai	Country:	China

### A2. EMPLOYEE INFORMATION

#### NUMBER OF EMPLOYEES

Range	Actual Total	Permanent	Temporary	Foreign	Migrant
101-300	155(100%)	4(3%)	151(97%)	0(0%)	151(97%)

List of Nationalities: NA

### A3. BUSINESS OVERVIEW

Industry:	Transportation and Warehousing	Warehouse customs bonded:	No
Key/Main Product:	Warehouse and transportation	Free trade zone:	No
Facility land size:	15922	Total facility floor size:	15922

Total Nr of Buildings	Distribution	Production	Warehouse	Container Yards	Others
2	0	0	1	1	0

### A4. EXPORT LOGISTICS

#### PERCENTAGE OF GOODS EXPORTED TO US

By Air	By Sea	By Rail	By Truck
0	1	0	0

#### FACILITY RESPONSIBLE FOR THE RELATIONSHIP WITH THE FOLLOWING TYPE OF LOGISTICS

Air:	Sometimes	Consolidators:	Sometimes
Sea:	Sometimes	Freight Forwarders:	Sometimes
Rail:	Never	NVOCC:	Never
Land Carriers:	Always	Other 3rd party logistics providers:	Never
The companies used vary routes:	Yes	The companies used Global Positioning Satellite (GPS):	Yes

# Global Security Verification Report, SHANGHAI YALIAN INTERNATIONAL LOGISTICS CO.,LTD

The companies used employ security guards: **No**

The companies used truck convoys: **No**

The companies used provide vehicle escort: **No**

## A5. GENERAL INFORMATION

### Brief description of the facility:

The facility was established in 2013 and was occupying 15922 square meters lot area. The facility rent part of one partial of 2-storey building for warehouse and office. The facility was only provide warehouse and transportation service. Currently, there were 155 employees consisting of 27 females and 128 males.

### Brief description of loading process for shipment:

All cargos were delivered to the port by their own truck.

### Brief description of sealing process:

All seals were bought by themself which meet ISO/PAS 17712 compliant. Seal number would be recorded in log. Photo of container and seal would also be recorded.

### Brief description of direct shipments to port process:

All cargos were delivered to the port by their own truck.

### In-country transport services detail:

All cargos were delivered to the port by their own truck.

### Required transit time between audited facility to the port / the next supply chain:

Required transmit time from facility to Waigaoqiao port is about 0.5 hour, to Yangshan port is about 2 hours.

### CCTV details:

Yes, There are 159 CCTV cameras installed in strategic areas. 139 cameras monitor is secured in the office by office employee, the recording is kept since Feb 26, 2020. But 20 cameras that instleed at outside of the building include gate are monitor by the realtys guards, and the records were only kept about 25 days.

### Security guard force details:

Facility had 6 security guards under in-house employees manning the facility 24/7, and 6 realty's security guards.

# Global Security Verification Report, SHANGHAI YALIAN INTERNATIONAL LOGISTICS CO.,LTD

## B. RESULT DETAILS

The following section includes all findings noted during the on-site audit.

### Security Vision and Responsibility 100%

RATING	Must - High	Must - Low	Should - High	Should - Low	Total
NEW NON-COMPLIANCES	0	0	0	0	0

No findings noted

### Risk Assessment 85%

RATING	Must - High	Must - Low	Should - High	Should - Low	Total
NEW NON-COMPLIANCES	0	2	0	0	2

### New Non- Compliances

ID #	Finding	Rating
O0101	Security risk assessment of the company site conducted but the weaknesses identified are not recorded and/or corrected in a timely manner.	Must - Low
% of occurrence at other facilities None		Past occurrences at this facility None
Auditor Comments Weaknesses identified were not recorded in the Security risk assessment.		
Minimum Security Criteria CTPAT Members must conduct and document the amount of risk in their supply chains. CTPAT Members must conduct an overall risk assessment (RA) to identify where security vulnerabilities may exist. The RA must identify threats, assess risks, and incorporate sustainable measures to mitigate vulnerabilities. The member must take into account CTPAT requirements specific to the member's role in the supply chain.		

### New Non- Compliances

ID #	Finding	Rating
O0105	The company does not adopt the "5 Step Risk Assessment Process Guide" in conducting a security risk assessment of their supply chain(s).	Must - Low
% of occurrence at other facilities None		Past occurrences at this facility None
Auditor Comments The company didn't adopt the "5 Step Risk Assessment Process Guide" to conduct risk assessment.		
Minimum Security Criteria CTPAT Members must conduct and document the amount of risk in their supply chains. CTPAT Members must conduct an overall risk assessment (RA) to identify where security vulnerabilities may exist. The RA must identify threats, assess risks, and incorporate sustainable measures to mitigate vulnerabilities. The member must take into account CTPAT requirements specific to the member's role in the supply chain.		

### Business Partners 100%

RATING	Must - High	Must - Low	Should - High	Should - Low	Total
NEW NON-COMPLIANCES	0	0	0	0	0

# Global Security Verification Report, SHANGHAI YALIAN INTERNATIONAL LOGISTICS CO.,LTD

No findings noted

## Cyber Security

79%



RATING	Must - High	Must - Low	Should - High	Should - Low	Total
NEW NON-COMPLIANCES	0	2	1	0	3

### New Non- Compliances

ID #	Finding	Rating
O0166	Scheduled vulnerability scans of computer network are not done.	Must - Low
% of occurrence at other facilities None		Past occurrences at this facility None
Auditor Comments The network IT infrastructure was not tested regularly		
Minimum Security Criteria CTPAT Members utilizing network systems must regularly test the security of their IT infrastructure. If vulnerabilities are found, corrective actions must be implemented as soon as feasible.		

### New Non- Compliances

ID #	Finding	Rating
O0186	Users with access to IT systems are not provided with individual accounts. Multiple users are sharing same account.	Must - Low
% of occurrence at other facilities None		Past occurrences at this facility None
Auditor Comments Checking two computers, one was administrator account.		
Minimum Security Criteria Individuals with access to Information Technology (IT) systems must use individually assigned accounts. Access to IT systems must be protected from infiltration via the use of strong passwords, passphrases, or other forms of authentication and user access to IT systems must be safeguarded.		

### New Non- Compliances

ID #	Finding	Rating
O0201	The company IT network data are not backed up once a week or as appropriate.	Should - High
% of occurrence at other facilities None		Past occurrences at this facility None
Auditor Comments The computer information were backed up once a month.		
Minimum Security Criteria Data should be backed up once a week or as appropriate. All sensitive and confidential data should be stored in an encrypted format.		

## Conveyance and Instruments of International Traffic Security

93%



RATING	Must - High	Must - Low	Should - High	Should - Low	Total
NEW NON-COMPLIANCES	0	0	1	0	1

# Global Security Verification Report, SHANGHAI YALIAN INTERNATIONAL LOGISTICS CO.,LTD

## New Non- Compliances

ID #	Finding	Rating
O0244	Management personnel does not conduct random searches of conveyances.	Should - High
% of occurrence at other facilities None	Past occurrences at this facility None	
Auditor Comments Management personnel did not conduct random searches of conveyances.		
Minimum Security Criteria Based on risk, management personnel should conduct random searches of conveyances after the transportation staff have conducted conveyance/Instruments of International Traffic inspections.The searches of the conveyance should be done periodically, with a higher frequency based on risk. The searches should be conducted at random without warning, so they will not become predictable. The inspections should be conducted at various locations where the conveyance is susceptible: the carrier yard, after the truck has been loaded, and en route to the United States border.		

## Seal Security 100%

RATING	Must - High	Must - Low	Should - High	Should - Low	Total
NEW NON-COMPLIANCES	0	0	0	0	0

No findings noted

## Procedural Security 100%

RATING	Must - High	Must - Low	Should - High	Should - Low	Total
NEW NON-COMPLIANCES	0	0	0	0	0

No findings noted

## Agricultural Security 100%

RATING	Must - High	Must - Low	Should - High	Should - Low	Total
NEW NON-COMPLIANCES	0	0	0	0	0

No findings noted

## Physical Security 86%

RATING	Must - High	Must - Low	Should - High	Should - Low	Total
NEW NON-COMPLIANCES	0	0	3	1	4

## New Non- Compliances

ID #	Finding	Rating
O0381	The company does not have an automatic intrusion detection or alarm system installed in sensitive/controlled access areas.	Should - High

# Global Security Verification Report, SHANGHAI YALIAN INTERNATIONAL LOGISTICS CO.,LTD

% of occurrence at other facilities None	Past occurrences at this facility None
Auditor Comments The facility had not installed automatic intrusion detection or alarm system in sensitive/controlled access areas.	
Minimum Security Criteria Security technology should be utilized to monitor premises and prevent unauthorized access to sensitive areas.	

## New Non- Compliances

ID # O0402	Finding There is no alternative or back-up power source for alarm, lighting and CCTV systems.		Rating Should - Low
% of occurrence at other facilities None		Past occurrences at this facility None	
Auditor Comments No back-up power source for CCTV systems was installed in the facility.			
Minimum Security Criteria Security technology systems should be configured with an alternative power source that will allow the systems to continue to operate in the event of an unexpected loss of direct power.			

## New Non- Compliances

ID # 00405	Finding CCTV alarms are not used to alert a company to unauthorized access into sensitive areas.		Rating Should - High
% of occurrence at other facilities None		Past occurrences at this facility None	
Auditor Comments The CCTV had no alarm function.			
Minimum Security Criteria If camera systems are deployed, cameras should monitor a facility’s premises and sensitive areas to deter unauthorized access. Alarms should be used to alert a company to unauthorized access into sensitive areas.			

## New Non- Compliances

ID # 00422	Finding Recordings (e.g., tapes or electronic files) are not kept for a minimum of 30 days or according to client specific requirement, whichever is longer.		Rating Should - High
% of occurrence at other facilities None		Past occurrences at this facility None	
Auditor Comments The records of cameras that installed at outside of the building were kept since Apr 27, 2020, about 25 days.			
Minimum Security Criteria If cameras are being used, recordings of footage covering key import/export processes should be maintained for a sufficient time for a monitored shipment to allow an investigation to be completed.			

<b>Physical Access Controls</b>	<b>100%</b> 
---------------------------------	---

RATING	Must - High	Must - Low	Should - High	Should - Low	Total
NEW NON-COMPLIANCES	0	0	0	0	0

# Global Security Verification Report, SHANGHAI YALIAN INTERNATIONAL LOGISTICS CO.,LTD

No findings noted

## Personnel Security

100%



RATING	Must - High	Must - Low	Should - High	Should - Low	Total
NEW NON-COMPLIANCES	0	0	0	0	0

No findings noted

## Education, Training and Awareness

82%



RATING	Must - High	Must - Low	Should - High	Should - Low	Total
NEW NON-COMPLIANCES	0	1	1	0	2

### New Non-Compliances

ID #	Finding	Rating
O0477	There is no written security awareness program covering awareness of current terrorist threat (s), smuggling trends, and seizures in place to ensure employees understand the threat posed by terrorist at each point of the supply chain.	Must - Low
% of occurrence at other facilities None		Past occurrences at this facility None
Auditor Comments Security awareness training didn't cover current terrorists and smuggling trends.		
<b>Minimum Security Criteria</b> Members must establish and maintain a security training and awareness program to recognize and foster awareness of the security vulnerabilities to facilities, conveyances, and cargo at each point in the supply chain, which could be exploited by terrorists or contraband smugglers. The training program must be comprehensive and cover all of CTPAT's security requirements. Personnel in sensitive positions must receive additional specialized training geared toward the responsibilities that the position holds. One of the key aspects of a security program is training. Employees who understand why security measures are in place are more likely to adhere to them. Security training must be provided to employees, as required based on their functions and position, on a regular basis, and newly hired employees must receive this training as part of their orientation/job skills training. Members must retain evidence of training such as training logs, sign in sheets (roster), or electronic training records. Training records should include the date of the training, names of attendees, and the topics of the training.		

### New Non-Compliances

ID #	Finding	Rating
O0485	The company does not perform emergency response mock drills.	Should - High
% of occurrence at other facilities None		Past occurrences at this facility None
Auditor Comments Emergency response mock drill was not conducted by the facility.		
<b>Minimum Security Criteria</b> CTPAT Members should have measures in place to verify that the training provided met all training objectives.		



## **C. BEST PRACTICES AND RECOMMENDED BEST PRACTICES**

CBP describes Best Practices as innovative security measures that exceeds the CTPAT criteria and industry standards. For C-TPAT purposes, a best practice must meet all five of the following requirements, all of which are subject to verification: (1. Senior management support; 2. Innovative technology, process or procedures; 3. Documented process; 4. Verifiable evidence; and, 5. A regular system of checks, balances and accountability.)

### **Existing Best Practices:**

#### **1. Business Partners**

- Not applicable

#### **2. Cyber Security**

- Not applicable

#### **3. Conveyance and Instruments of International Traffic Security**

- For conveyance entries/exits, logs are maintained with name of the guard.
- Photos of authorized employees are publicized to access the restricted areas posted in the work area to detect any unauthorized entry/access.

#### **4. Seal Security**

- Not applicable

#### **5. Procedural Security**

- Loaded containers/trailers' final inspection is conducted.

#### **6. Agricultural Security**

- Not applicable

#### **7. Physical Security**

- Vehicles are prohibited/prevented from parking near perimeter fencing.

#### **8. Physical Access Controls**

- Security guards receive specific training in C-TPAT.

#### **9. Personnel Security**

- Not applicable

#### **10. Education, Training and Awareness**

- Not applicable

### **Recommended Best Practices:**

#### **1. Business Partners**

- The facility should conduct periodic table-top exercises to address security breaches within the supply chain and, if one doesn't already exist, create a "quick response team" to investigate suspicious activities discovered during cargo transportation.
- The facility should perform periodic audits of business partners accompanied by a third-party security firm (these audits may be performed without advance notice). The firm should provide a written assessment of business partners' adherence to C-TPAT minimum security criteria. If non-compliance is discovered, it could be sufficient grounds for terminating the business relationship.
- The facility should provide periodic security awareness training to all of the contractors.

#### **2. Cyber Security**

- The facility should equip computers with biometric retina scanners for authentication and identification purposes.

# Global Security Verification Report, SHANGHAI YALIAN INTERNATIONAL LOGISTICS CO.,LTD

- The facility should install software on employees' laptops that allows management to delete information from hard drives from a remote location.
- The facility should require computer users to sign an agreement of liability for the use of the company's information systems, and renew these agreements each time a password change is initiated.

## 3. Conveyance and Instruments of International Traffic Security

- The facility should use a dock locking arm to anchor the container chassis to the loading dock.
- The facility should use tamper-indicative security labels bearing an actual photo of the seal and a serial number, attached to the hinges and between the two doors of the vehicles.

## 4. Seal Security

- In addition to using a bolt seal, attach a cast iron J-bar device to the locking bar that requires a specialized tool for removal.
- The facility uses multiple ISO/PAS 17712 certified high security seals on all shipments bound to the U.S.

## 5. Procedural Security

- The facility should schedule all deliveries at distribution centers in advance using an online automated tool, and ensure that upon arrival, drivers provide security guards with shipment-linked delivery numbers for verification.
- The facility should use tamper-evident tape with serial numbers to seal cartons, and verify the serial numbers against the packing list when loading and at the final destination.

## 6. Agricultural Security

- The facility should consider using alternatives to wood packaging material. The following products are not subject to USDA regulation: Plywood or press board; Plastic pallets; Oriented strand board; Hardboard; Parallel strand lumber; Synthetic foam; Metal frames; Inflated dunnage; Masonite veneer

## 7. Physical Security

- If the facility is located adjacent to a lake or body of water that forms part of its perimeter, it should install an optical fence above and below the water line to detect waterborne intruders.
- The facility should install a double-layered perimeter fence, creating a secure zone between the two fence lines. Ensure that both fences are equipped with electronic monitoring capabilities, and that the outer fence incorporates underground concrete to deter tunneling.
- The facility should maintain multiple alarm systems that include door contacts, heat and vibration sensors, and seismic movement detectors.
- The facility should position security guard that view towers at each corner of the facility perimeter with sightlines that permit views of activity inside and outside the facility. Make sure the towers are manned at all times.

## 8. Physical Access Controls

- The facility should ensure that as employees enter the facility, their photos are displayed on an electronic access system monitor so that the security guard in the area can verify that the individual entering matches the photo displayed on the monitor.
- The facility should ensure that the exterior doors of buildings are equipped with two- person key systems that require a company manager and security guard to unlock the facility.
- The facility should Issue all visitors thermal-activated visitor ID badges featuring expiration marking/coloring that appears after eight hours.

## 9. Personnel Security

- Drug screening checks should be conducted.
- The facility should conduct exit interviews as a routine part of the employee termination process, with a counselor on hand to evaluate the likelihood that a terminated employee could pose a retaliation threat.
- The facility should have a fingerprinting document of the identity of all new hires, and provide an employee list to national authorities on an annual basis for additional screening.

## 10. Education, Training and Awareness

- A security awareness assessment should be given annually to a random sample of employees to gauge their understanding of the company's general security policy.

## **Global Security Verification Report, SHANGHAI YALIAN INTERNATIONAL LOGISTICS CO.,LTD**

- The facility should conduct a semi-annual security awareness training seminar for all U.S. based suppliers, customers, and other business partners.
- The facility should provide online training portal.
- The facility should require new employees to complete a multiple-module security training program. Web-based training should emphasize recognition of internal conspiracies, maintaining cargo security, facility access control, and mail handling procedures. Publish security updates via an intranet.

D. PERFORMANCE TREND ANALYSIS

Section Name	Current NA	Last NA	First NA	Change (Current-Last)	Change (Current-First)
--------------	------------	---------	----------	-----------------------	------------------------

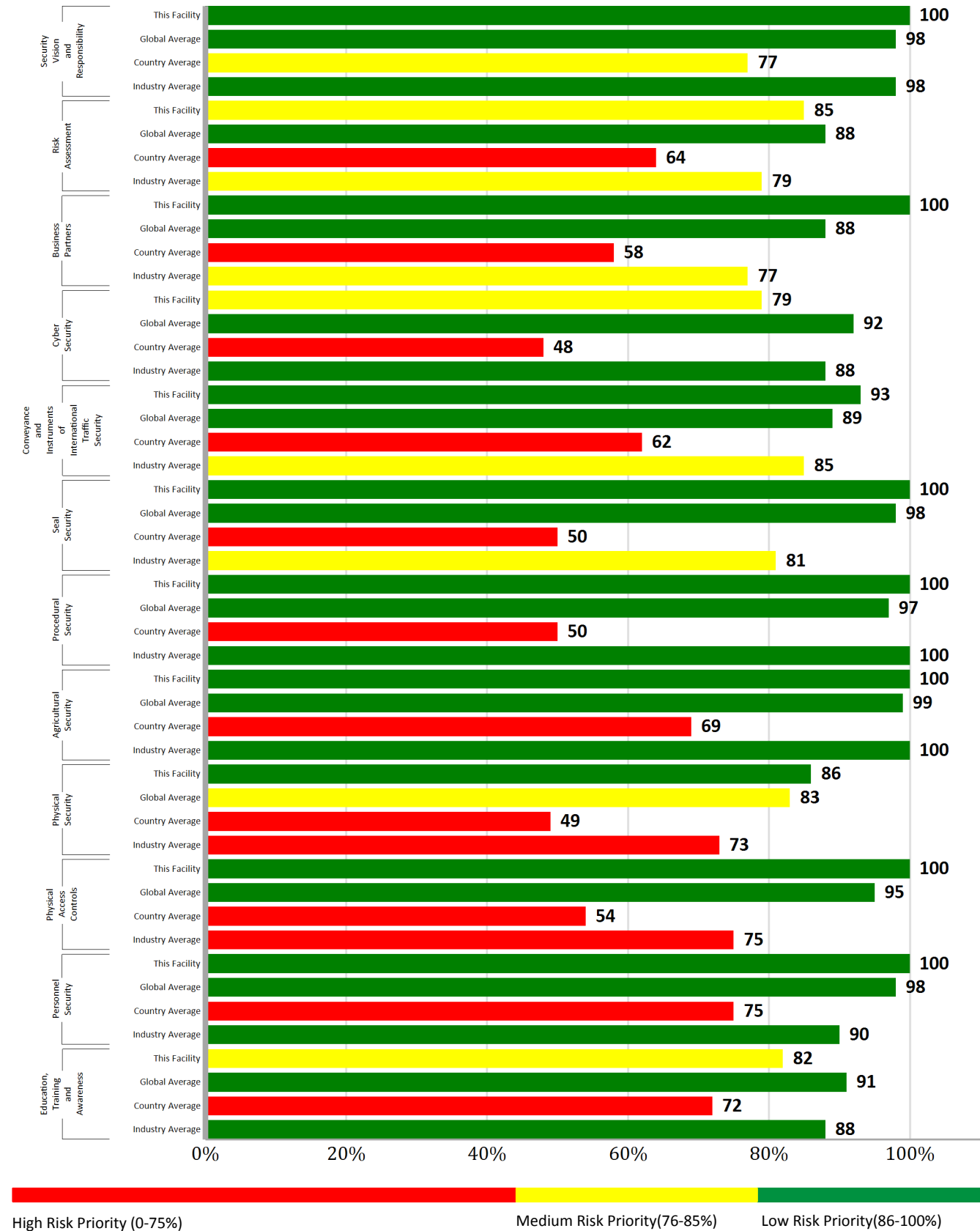
 Advancers    Constant    Decliner

## E. KEY STRENGTHS AND CHALLENGES

Criteria	Facility Strengths: Facility performance ranks in the top percentile of the population and/or has implemented a best practice process	Global Freq. of Compliance %
Compliant	The company demonstrates effective asset management over assets containing sensitive information through regular controlled inventories. Effective media sanitization and disposal should be in accordance with NIST Guidelines or other appropriate industry guidelines.	90%
Compliant	Business partner's security assessment is reviewed periodically.	91%
Compliant	The company has written procedures governing how identification badges and access devices are granted, changed, and removed.	92%
Compliant	Seal numbers are electronically printed on the bill of lading or other shipping documents.	92%
Compliant	The company works with their transportation providers to track conveyances from origin to final destination point. Specific requirements for tracking, reporting, and sharing of data should be incorporated within terms of service agreements with service providers.	94%
Compliant	Information Security management system policies and procedures are reviewed annually, or more frequently as business risks or circumstances dictate. Changes and updates from the review are made as needed.	94%
Compliant	The company demonstrates policies and procedures to ensure that all technology is properly licensed and there are no counterfeit or improperly licensed technology is in use.	94%
Compliant	Gates are manned and/or monitored.	95%
Compliant	The Supply Chain Security Program is regularly reviewed and review is documented.	95%
Compliant	Visitor and employee vehicles are prohibited/prevented from parking near cargo conveyances.	95%

Criteria	Facility Challenges: Facility performance ranks in the bottom percentile of the population	Global Freq. of Compliance %
Should - High	The company does not have an automatic intrusion detection or alarm system installed in sensitive/controlled access areas.	68%
Should - High	Recordings (e.g., tapes or electronic files) are not kept for a minimum of 30 days or according to client specific requirement, whichever is longer.	55%
Must - Low	The company does not adopt the "5 Step Risk Assessment Process Guide" in conducting a security risk assessment of their supply chain(s).	53%
Should - High	CCTV alarms are not used to alert a company to unauthorized access into sensitive areas.	38%
Should - High	The company does not perform emergency response mock drills.	30%
Should - Low	There is no alternative or back-up power source for alarm, lighting and CCTV systems.	30%
Should - High	Management personnel does not conduct random searches of conveyances.	23%
Must - Low	Users with access to IT systems are not provided with individual accounts. Multiple users are sharing same account.	15%
Must - Low	There is no written security awareness program covering awareness of current terrorist threat(s), smuggling trends, and seizures in place to ensure employees understand the threat posed by terrorist at each point of the supply chain.	9%
Should - High	The company IT network data are not backed up once a week or as appropriate.	9%

## F. COMPARISON BENCHMARK



# Global Security Verification Report, SHANGHAI YALIAN INTERNATIONAL LOGISTICS CO.,LTD

## DISCLAIMER

This report is for the exclusive use of the client of Intertek named in this report ("Client") and is provided pursuant to an agreement for services between Intertek and Client ("Client agreement"). No other person may rely on the terms of this report. This report provides a summary of the findings and other applicable information found/gathered during the audit conducted at the specified facilities on the specified date only. Therefore, this report does not cover, and Intertek accepts no responsibility for, other locations that may be used in the supply chain of the relevant product or service. Further, as the audit process used by Intertek is a sampling exercise only, Intertek accepts no responsibility for any non-compliant issues that may be revealed relating to the operations of the identified facility at any other date. Intertek's responsibility and liability are also limited in accordance to the terms and conditions of the Client Agreement. Intertek assumes no liability to any party, for any loss, expense or damage occasioned by the use of this information other than to the Client and in accordance with the Client Agreement and these disclaimers. In case there is any conflict between the disclaimers stated herein and the applicable terms and conditions of Intertek incorporated into the Client Agreement, then these disclaimers shall prevail.