



SCAN Supplier Education Series - Risk Assessments

SCAN Foreign Origin Committee & SCAN Program Management Team

March 2025

Disclaimer: This training makes no claim or warranty that the recipient is security compliant in any private or public domain.

Training Course Overview

- Why Risk Assessments are Vital
- What is a Risk Assessment
- How to Conduct a Risk Assessment
- SCAN Criteria for Risk Assessments
- Examples of a Risk Assessment Report

Why Risk Assessments are Vital



Why Risk Assessments are Vital

- The risk assessment process is critically important as it allows Business Partners to understand their supply chains, where the vulnerabilities lie within those supply chains, and determine what to do to mitigate any risks identified.
- From practical and analysis perspective, high non-compliance rate of risk assessment observed during audit and improvements made during CAPA process. Training on this topic will help improve compliance.
- Out of the top five questions with incorrect responses, the top two questions are from the risk assessment category.

Q#	Question Category	Questions
8	Risk Assessment	Is the facility risk assessment shared with business partners and contractors?
12	Risk Assessment	Define the facility's crisis plan. (Select all that apply)

What is a Risk Assessment



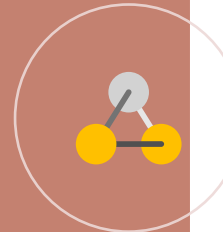
What is a Risk Assessment

A Risk Assessment involves analyzing external threats against company procedures to identify where vulnerabilities exist, and what procedures can be implemented or improved upon to reduce such risk. All international supply chains should be evaluated, including both direct and indirect business partners.

A Risk Assessment includes ensuring (through process improvement, retraining, working with business partners, etc.) that issues identified through analysis and audits as vulnerabilities are successfully addressed.



A Risk Assessment consists of several components, including a **Threat Assessment, Cargo and Data Flow, Vulnerability Assessment, and audits of security procedures.**



A Risk Assessment should also include how security procedures would be affected by natural and man-made disasters, to include how backup systems will address these vulnerabilities. Such issues include power outages; weather events such as hurricanes; earthquakes; civil unrest; and terrorist events.



Note:

Expensive technology is not mandatory, for in the end security relies upon the human component. This is why effective personnel screening and security training are critical issues.

What is a Risk Assessment

A Threat Assessment involves identifying threats to a supply chain that exist within a country or region, that are external and outside the control of the factory, or a factory's business model.

Threat Assessment: An assessment of a criminal or terrorist presence within a jurisdiction integrated with an assessment of potential targets of that presence and a statement of probability the criminal or terrorist will commit an unlawful act. The assessment focuses on the criminal's or terrorist's opportunity, capability, and willingness to fulfill the threat.

1 – Low Risk — No recent activity/intelligence information.

2 – Medium Risk — No recent incidents/Some intelligence/information on possible activity.

3 – High Risk — Recent incidents and intelligence/information.

What is a Risk Assessment

A Vulnerability Assessment involves identifying weaknesses in a company's security procedures and supply chain which could be used to the advantage of terrorists and other criminals identified in the Threat Assessment.

- ✓ Internal audits and security reviews can be important instruments for identifying vulnerabilities. For example, an internal audit of the company itself (such as an internal audit during the annual security profile review, security questionnaires, and site visits conducted during business partner screening), could go into the overall vulnerability assessment. Corrective actions based on the findings of internal audits and business partner reviews can be implemented as part of the Action Plan.



What is a Risk Assessment

An Action Plan consists of taking identified and documented vulnerabilities to develop and implement procedures and/or improvements to reduce those vulnerabilities.

- ✓ An audit is a periodic documented review to ensure the procedures the company has in place are being conducted and followed through, as part of regular, everyday procedures, and that records are completed and properly filed. Audits may reveal security deficiencies, however, do not replace, rather enhance, a company's Vulnerability Assessment.



Be written and documented



Include communication with
business partners



Include alternative locations
if the facility can't be used

How to Conduct a Risk Assessment

-Five Step Risk Assessment





Five Step Risk Assessment

Components of the Five Step Risk Assessment

1. Mapping cargo flow and identifying **business partners (both direct or indirect)**
2. Conducting a threat assessment
3. Conducting a vulnerability assessment
4. Preparing an action plan
5. Documenting the risk assessment process

*Please click [HERE](#) For more details and information on the **Five Step Risk Assessment Guidance**.

The risk assessments described below are only guides, and all companies should establish a process that conforms to the needs of their business model, and should not simply adopt a generic, externally provided model. CTPAT Partners must conduct a risk assessment at least annually to remain in the CTPAT program.

Five Step Risk Assessment

Step	Process	Description	Method
1	Map Cargo Flow and Business Partners	Identify ALL parties involved in the following processes: 1. Procurement/Purchasing 2. Production 3. Packing 4. Storage 5. Loading/Unloading 6. Transportation 7. Document Preparation	1. Request information from supply chain partners 2. Review documentation (Bills of Lading, manifests, invoices, etc.) 3. Determine routing from site visits/audits of the supply chain.
2	Conduct Threat Assessment	Identify and rate the risk of threat (low, medium, high) for the country and region for each international supply chain, using the following (at a minimum): Terrorism (political, bio, agro, cyber) Contraband Smuggling, Human Smuggling, Organized Crime, Conditions fostering above threats.	1. Investigate using open-source internet information (government and private organizations) 2. Representative/contacts “on the ground” at Origin should be interviewed 3. Discuss with Law enforcement (foreign/domestic), local state, federal/national 4. Ask if they belong to Trade and security organizations 5. Assigned CTPAT SCSS
3	Conduct Vulnerability Assessment	For all business partners in the international supply chain (directly contracted or sub-contracted): 1. Identify the work function process they perform 2. Verify partners meet applicable minimum-security criteria 3. Rate partners compliance (low, medium, high)	1. SVI Number/CTPAT Membership 2. Membership in Mutual Recognition Program 3. Ask to review security surveys 4. Site visits by company representative completed? 5. Site visits by overseas personnel/agents? 6. Review company Business reports 7. Request company’s Security certifications covering CTPAT minimum security criteria 8. Ask if third party supply chain security assessments were completed



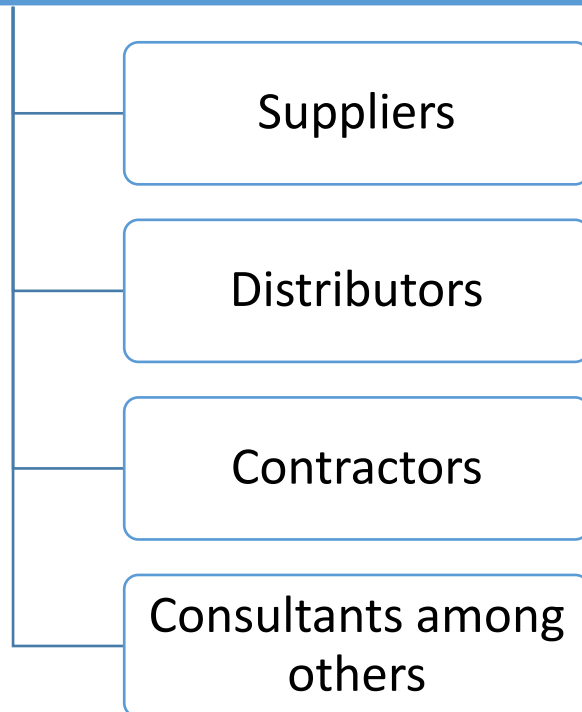
Five Step Risk Assessment

Step	Process	Description	Method
4	Prepare Action Plan	Establish a corrective action plan to address gaps or vulnerabilities found in business partner's security programs.	<ol style="list-style-type: none">1. Record weaknesses2. Identify corrective actions3. Provide timeline and assign responsibility4. Verify actions completed
5	Document How Risk Assessments are Conducted	A description of the company's approach, policies, and procedures for conducting an international supply chain security risk assessment.	<ol style="list-style-type: none">1. Document company's policy for conducting international supply chain security risk assessment2. Document procedures to conduct international supply chain security risk assessments

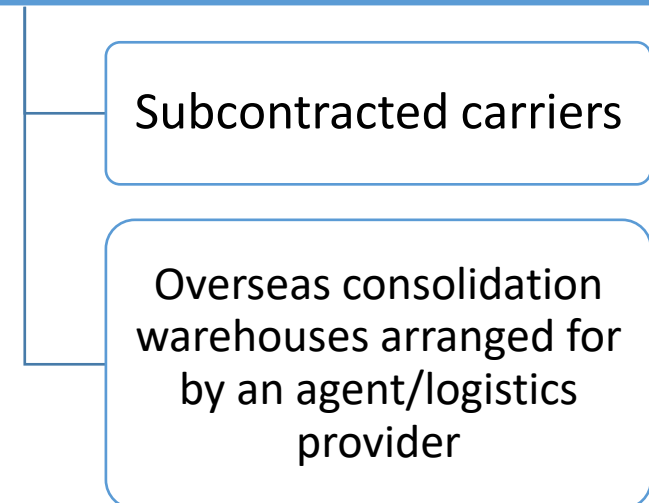
Five Step Risk Assessment – Who are the Business Partners

A business partner may be any party that provides a service to fulfill a need within a company's international supply chain.

Direct Business Partners



Indirect Business Partners



How to Select and Monitor Business Partners

If the partners are CTPAT Members or AEO-certified (U.S. Authorized Economic Operator (AEO) program), collect the respective certificate and verify it with the foreign Customs administration's website. And continue to monitor the validity of certificates

Classify the weakness based on the level of risk involved, set different timelines and collect evidence

Complete Social compliance program including forced, imprisoned, indentured, or indentured child labor



Screen new business partners and monitor current partners, including money laundering and terrorist funding by verifying business licenses, checking business references, credit reports etc.

Exercise due diligence to make sure partners to meet or exceed CTPAT'S MSC via a statement of compliance.

- Onsite/Immersive audit
- Questionnaire
- Compliance statement

Update security assessments of business partners annually, or as circumstances/risks dictate. Higher risk supply chains would be expected to have more frequent reviews than low risk ones.


How to Select and Monitor Business Partners

- The business partner screening process must consider whether a partner is a Customs-Trade Partnership Against Terrorism (**CTPAT**) Member or a Member of an approved Authorized Economic Operator (**AEO**) program with a Mutual Recognition Arrangement (**MRA**) with the United States (or an approved MRA). A copy of the AEO certificate or a SCAN Audit Report is acceptable proof for meeting program requirements for business partners.
- Members must obtain evidence of the certification and continue to monitor these business partners to ensure they maintain their certification.
- Current United States MRAs include New Zealand, Canada, Jordan, Japan, South Korea, the European Union (27 Member states), Taiwan, Israel, Mexico, Singapore, the Dominican Republic, Peru, the United Kingdom, and India.



How to Select and Monitor Business Partners


- Example of a SCAN Security Audit Report



BRANCH

SCAN SECURITY AUDIT (ONSITE)

Report # EAC-2024-12-0118-CAPA-V4
Audit Submitted Dec 06, 2024
Compliance Score 96%
Audit Type EXTERNAL



Location Information

SCAN ID
Point of Contact Name
Point of Contact Email
Order Date *Not provided*
Other Ordering Member ID *Not provided*
Custom Comments *Not provided*
SCAN Members linked to factory
Vendor Name - Entered by SCAN Member *Not provided*
Vendor Email Address - Entered by SCAN Member *Not provided*

Contact Name	Phone	Email
		JohnH@agri-fab.com

Location AGRI-FAB
Primary Location Yes
Critical Location No
Assigned Auditor
Schedule Date

Audit Summary

Pre-CAPA

Audit Submitted	Compliance Score Pre-CAPA	Risk Index
Dec 02, 2024	86%	Guarded

Compliance by Category

Category	Score	Target
Agricultural Security	100%	100%
Business Partner Requirements	52%	100%
Conveyances and Instruments of International Traffic	83%	100%
Cyber and Information Technology Security	100%	100%

How to Select and Monitor Business Partners

- Example 1 of AEO Certificate

证书编号
Certificate No.



认证企业证书
AEO CERTIFICATE

认证企业名称
AEO Name

认证企业编号
AEO Code

认证企业类型
AEO Type

认证日期
Date of Authorization

发证机关
Issuing Authority

发证日期
Date of Issue

02月04日

高级认证企业

20

How to Select and Monitor Business Partners

- Example 2 of AEO Certificate



Indian Customs

Authorised Economic Operator (AEO)
Programme



Central Board Of Indirect Taxes & Customs

AEO Certificate Details View

<u>Company Name:</u>	
<u>Company Address</u>	
<u>IEC Number</u>	
<u>AEO Tier</u>	T1
<u>Zone</u>	
<hr style="border-top: 1px dashed black;"/>	
<u>Certificate Number</u>	INAA
<hr style="border-top: 1px dashed black;"/>	
<u>Certificate Issue Date</u>	
<u>Certificate Validity Date</u>	
<hr style="border-top: 1px dashed black;"/>	
<u>Certificate Present Validity Date</u>	01/01/2025 5
<u>Certificate Present Validity Status</u>	Valid

©2018 Central Board of Indirect Taxes & Customs, India

Five Step Risk Assessment – Security Risk Rating

Each partner is responsible for establishing its own overall security risk rating system based on its business model. The goal is to have a ranked output to see where your company should focus resources to reduce/mitigate risk.

Businesses may use various methodologies for rating risk within their international supply chains. The Five Step Risk Assessment Guide (Five Step Guide) uses the following simple risk ratings throughout:

1. Low risk;
2. Medium risk;
3. High risk.

Risk index = possibility index * Consequence severity index
风险指数 = 可能性指数 * 后果严重指数

Score	Possibility Index 可能性指数
1	It's unlikely. It's a total accident
2	Very unlikely, you can imagine
3	Maybe, but not very often
4	Quite likely
5	It happens once a year or more

Score	Consequence Severity Index 后果严重指数
1	A slight risk, acceptable
2	General danger, need to be careful
3	Significant risk and need to be corrected
4	Highly dangerous, need immediate rectification
5	It's too dangerous to continue

Risk index 风险指数

5	10	15	20	25
4	8	12	16	20
3	6	9	12	15
2	4	6	8	10
1	2	3	4	5

- 1-4 分 : Low priority, acceptable risk
- 5-15 分 : Medium priority, need to take control
- 16-25 分 : High priority, need to have intensive control

SCAN Criteria for Risk Assessments





CTPAT MSC vs. SCAN Criteria

The SCAN audit questions are structured around the requirements stated in the Customs Trade Partnership Against Terrorism (**CTPAT**) Minimum Security Criteria (**MSC**).

SCAN as an organization of US and Canada based importers with a common goal of facilitation of international supply chain security compliance enthusiastically endorses the efforts of U.S. Customs and Border Protection (**CBP**) to refresh and update the CTPAT MSC.

SCAN has performed over **34,000** supply chain security audits in the past 10 years and has a repository of **31,000** locations (one location may have multiple completed audits). SCAN members participated in the Advisory Committee On Commercial Operations (**COAC**) that provided input and feedback during the drafting and review of new MSC.



SCAN Criteria on Risk Assessment

Q#	Category	Audit Questions	Guidance
7	Risk Assessment	Does the facility have a risk assessment that identifies vulnerabilities in the business plan?	<p>A risk assessment is a written document that highlights vulnerabilities identified while assessing your operation. The risk assessment must include, at a minimum:</p> <ul style="list-style-type: none"> • All possible vulnerabilities/risks that could impede the completion of business unique to the particular facility • Preventative actions to address known vulnerabilities/risks to minimize and/or prevent disruption of business • Corrective actions to address both known and unknown vulnerabilities/risks to return to business after disruption
8	Risk Assessment	Is the facility risk assessment shared with business partners and contractors?	<p>It is a good business practice to share your risk assessment with both your business partners, suppliers, and vendors to allow for coordination of corrective actions and business continuity planning. The risk assessment must include at a minimum:</p> <ul style="list-style-type: none"> • List of all primary vendors and suppliers • How these vendors/suppliers are impacted by possible vulnerabilities/risks • What role vendors/suppliers play in facility's preventative/corrective actions • Date of when risk assessment will be or was shared



SCAN Criteria on Risk Assessment

Q#	Category	Audit Questions	Guidance
9	Risk Assessment	Does the facility risk assessment include vulnerabilities specific to contracted service providers such as contractors, seasonal employees etc.?	Vulnerabilities involving contractors are a critical consideration. A risk assessment identifying areas of vulnerability that are controlled by contracted service providers is needed.
10	Risk Assessment	Is the facility risk assessment updated periodically?	<p>SCAN's expectation is to implement the procedure to review and update the risk assessment at minimum annually. The risk assessment must include at a minimum:</p> <ul style="list-style-type: none"> • Frequency of review/updates • What information is to be reviewed/updated • How updates will be communicated to primary vendors/suppliers and contract service providers (if applicable)



SCAN Criteria on Risk Assessment

Q#	Category	Audit Questions	Options	Guidance
11	Risk Assessment	<p>Define the facility's cargo movement management process. (Select all that apply)</p> <p>Only select NA if the cargo movement is not managed or facilitated by the facility.</p>	<p>A written cargo process map is available</p> <p>The cargo process map includes transit times from origin to final container yard</p> <p>The cargo process map includes locations where freight may be at rest</p> <p>No written cargo process map is available</p>	<p>The cargo movement management process that includes: the names and contact information for providers, routes cargo takes, transit times and distances and all potential points where freight may be at rest.</p>



SCAN Criteria on Risk Assessment

Q#	Category	Audit Questions	Options	Guidance
12	Risk Assessment	Define the facility's crisis plan. (Select all that apply)	<p>Documented crisis plan available</p> <p>Crisis plan includes reporting crisis-related issues to business partners as necessary</p> <p>Crisis plan includes alternative locations if facility is rendered unusable</p> <p>No documented crisis plan available</p>	<p>It must be included in your crisis plan below listed information:</p> <ul style="list-style-type: none"> • Define types of crises • Information on how the facility responds to each type of crises • How facility communicates crises to affected business partners • Information on alternate locations that would be used should the facility be rendered unusable due to crises

Examples of a Risk Assessment Report



Example – Cargo Flow

Step 1 (Sample) Map Cargo Flow, Identify Partners and Processes

Notes: Ensure partners map out all variations of a supply chain: for example, Full Container Load (FCL) vs. Less than Container Load (LCL); from one factory to various ports of export; from one factory using different modes of transportation (air vs. sea); Any other potential variations that would alter the movement of cargo or the individuals involved in the process.

Always remember: **"freight at rest is freight at risk."**

Sub-contracting increases risk within a supply chain, particularly where security requirements have not been conveyed or verified. Items below in "red" font and an *, indicate a potentially high risk situation.

Business partner	Role/Process	Cargo movement, if applicable	Known details about provider	Days cargo "at rest" this stage	Transport mode	If handles cargo, who selects the provider?
XYZ Manufacturer	Production, Packing, Document Preparation	Point of Departure	Location: City 123, Country Origin; Years doing business with - 22; family owned and operated	0	NA	NA
Export Broker/ FF	Prepares Documentation for Export	N/A	Unknown *	NA	NA	NA

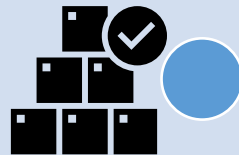
Example – Cargo Flow

Business partner	Role/Process	Cargo movement, if applicable	Known details about provider	Days cargo "at rest" this stage	Transport mode	If handles cargo, who selects the provider?
	Inland Transportation	Picks up cargo from factory and consolidator EFG		0	Truck	Factory
	Unloading, Storage, Loading	Unloads cargo from inland truck carrier, stores LCL, loads with other customers' cargo		2	NA	Factory
	Inland Transportation	Picks up cargo from consolidator and transports to Port of Export		0	Truck	Consolidator's contracted carrier*
	Storage	Receives offloaded container at country of transshipment		10*	NA*	Sea Carrier
	Transportation	Transports cargo from country of transshipment	Location: City, New Country; unknown	10	Vessel	Consolidator
	Storage	Unloads cargo from sea carrier's vessel and stores until domestic transport picks up	Location: City 42, USA ; MTSA/ISPS compliant	1	NA	U.S. Consolidator
	Transportation	Picks up cargo from terminal	Unknown*	0	Truck	U.S. Consolidator

Example – Cargo Flow

Factory

- Maximum 60 minutes loading time



Transport Service Provider Warehouse at ABC.

- Maximum 40 minutes moving time

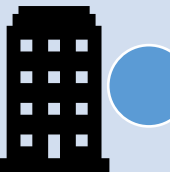
First Rest Point - ABD Gas Station

- Maximum 2 hours moving time



ABF Security Check Gate

- Maximum 3.5 hours without rest



Destination Receiver

Example – Risk Assessment

		Counter-terrorist Security Five Step Risk Assessment and Countermeasures Date: Feb/02/2024						Risk Level: High (16-25) / Midium (5-15) / Low (1-4)	
Item#	Risk Category	Risk Description	Consequence	Likelihood Index	Consequence Severity Index	Risk Index	Risk Level	Preventative and Corrective action	Responsible department
1	Disaster Crisis	Fire, flood, earthquake, typhoon, mudslide, etc.	Plant and equipment damage, personal injury, resulting in interruption of production activities and financial losses of the company	4	5	20	High	Formulate the "Natural Disaster Emergency Plan" and "Post-Disaster Reconstruction Plan", conduct regular drills on the emergency plan and summarize	Shipping
2	Security Vision and Responsibilities	No anti-terrorist security vision and responsibility commitment	Does not comply with C-TPAT MSC minimum safety guidelines	2	2	4	Low	Formulate anti-terrorist security policy objectives and responsibility commitments	Shipping
3	Risk Assessment	no risk assessment	Does not meet risk assessment requirements	2	2	4	Low	Develop risk assessment procedures and conduct risk assessments	Shipping
4	Business Partner	No anti-terrorism investigations of suppliers	Suppliers fail to comply with anti-terrorism requirements	3	3	9	Medium	The audit of new suppliers includes the audit of the anti-terrorism system, and the suppliers are audited regularly and irregularly	Shipping

Example – Risk Assessment

Threat	Vulnerability	Geographic import region	Risk Rating	Mitigation methods	Source of information/EOI	Action plan item
Attempting to enter terrorist or terrorist weapons into the U.S.	Customers	Country A	Medium	Procedures for Screening Business Partners	Client screening protocols	(if you don't do something from the mitigation methods, example for an action item)
	New Customers (new business)	Country B	High	CTPAT/MRA member*	Security questionnaire	
Contraband Smuggling (such as weapons, drugs, cash, or IPR)	Personal Shipments/ onetime shipments	Country C		Outreach to customers to join the CTPAT program*	Onsite audit protocols	
Human Smuggling			High	Request cargo security measures	Client outreach materials	
				Provide training materials/outreach for threat awareness		
				Compliance audits of contractors		
Contamination of Food Supply—bioterrorism	Produce Imports	Country A	Low	Send educational materials to clients for threat awareness and methods of prevention	Client outreach materials	
	Seafood Imports					

Example – Risk Assessment

反恐安全五步风险评估及应对措施表									
评估日期: 2022年5月4日					评估人: 王文静				
序号	风险项目	风险描述	后果	可能性指数	后果严重指数	风险指数	风险等级	应对措施	备注
1	安全愿景与责任	没有反恐安全愿景与责任承诺	不符合C-TPATMSC最低安全准则	2	2	4	低	制定反恐安全方针目标及责任承诺书	
2	安全愿景与责任	没有对反恐安全进行定期评审	不符合C-TPATMSC最低安全准则	2	2	4	低	进行定期评审	
3	安全愿景与责任	没有设定反恐安全联络员	不符合C-TPATMSC最低安全准则	2	2	4	低	任命安全联络员	
4	安全愿景与责任	没有跨部门职能团队	不符合C-TPATMSC最低安全准则	2	2	4	低	任命跨部门的职能团队	
5	安全愿景与责任	高层不重视, 没有安全承诺	不符合C-TPATMSC最低安全准则	2	2	4	低	制定反恐安全承诺书	
6	安全愿景与责任	没有成文的社会责任计划	不符合C-TPATMSC最低安全准则	2	2	4	低	遵守国际劳工准则	
7	风险评估	没有进行风险评估	不符合风险评估要求	2	2	4	低	制定风险评估程序, 进行风险评估	
8	风险评估	风险评估不全面	不符合风险评估要求	3	2	6	中	制定风险评估程序, 进行风险评估	
9	风险评估	风险评估没规定至少一年进行一次	不符合风险评估要求	2	2	4	低	制定风险评估程序, 进行风险评估	
10	风险评估	风险评估未包括货物的移动线路图	不符合风险评估要求	3	2	6	中	制定风险评估程序, 进行风险评估	
11	商业合作伙伴	没有合格供应商名录	无法对供应商进行反恐管	2	3	6	中	建立合格供应商名录	
12	商业合作伙伴	没有对供应商进行反恐调查	供应商未按反恐要求执行	3	3	9	中	1、新供应商稽核时包括反恐体系稽核2.定期、不定期地对供应商进行反恐	
13	商业合作伙伴	没有和供应商签订反恐协议	供应商不了解反恐要求	2	2	4	低	所有供应商签订反恐协议	
14	商业合作伙伴	没有和承包商签订反恐协议	承包商不了解反恐要求	2	2	4		包含食堂、建筑公司协议期内服务单位需签订反恐协议	



Thank you

Any questions, please contact via SCAN@scriskolutions.com.