



#### Document Section:

<b>Doc Type:</b>	Security Manual	<b>Status:</b>	Published
<b>Doc No:</b>	SM 06	<b>Effective Date:</b>	03-08-2012
<b>Revision No:</b>	4.0	<b>Created By:</b>	All Saafri
<b>SectionName:</b>	Loss Prevention		
<b>Title:</b>	Management Review and Continual Improvement		

#### Document Section:



The compliance and performance with regards to the SSG-SMS as well as improvement and legal compliance is the ultimate responsibility of the top management of Schenker Singapore, the SMS Committee. This responsibility is exercised through the management review process within the boundaries of SSG-SMS. Reviews shall include assessing opportunities for improvement and the need for changes to the security management system, including the Security Policy and Security Objectives, Threats and Risks.

Records of the management reviews shall be retained. Input to management reviews shall include:

- a) Results of audits and evaluations of compliance with legal requirements and with other requirements to which the organization subscribes,
- b) Communication from external interested parties, including complaints,
- c) The security performance of the organization,
- d) The extent to which objectives and targets have been met,
- e) Status of corrective and preventive actions,
- f) Follow-up actions from previous management reviews,
- g) Changing circumstances, including developments in legal and other requirements related to its security aspects,
- h) Recommendations for improvement.

The outputs from management reviews shall include any decisions and actions related to possible changes to Security Policy, objectives, targets and other elements of the security management system, consistent with the commitment to continual improvement.

There shall be a documented procedure established for management review. (Reference P-QUA-SCH-05-02 Management Review)


**Document Section:**

<b>Doc Type:</b>	Security Manual	<b>Status:</b>	Published
<b>Doc No:</b>	SM 01	<b>Effective Date:</b>	13-08-2013
<b>Revision No:</b>	5.0	<b>Created By:</b>	Ali Saafri
<b>SectionName:</b>	Loss Prevention		
<b>Title:</b>	Introduction to Security Management System		

**Document Section:**

✦ -	
1.0	Introduction
1.1	In close alignment with the Schenker AG Global Security Management System, Schenker Singapore incorporated this Security Management System and shall adopt Schenker Asia Pacific's Mission Statement.
1.2	Schenker Asia Pacific Mission Statement
	Safe, secure and efficient logistics for customer value and society continuity by protecting our company's employees, assets, information, integrity and reputation
1.3	Security has always been an important aspect in Schenker Singapore. The need for security in Schenker Singapore has increased and this affects the flow of goods, facilities and all staff. The progress is further driven by the development of different security programs emerging from authorities and organizations in combination with the Schenker's ambition to meet and anticipate customers' increasing security demands.
1.4	The Schenker Singapore Security Management System (SSG-SMS) has three objectives:
1.4.1	Provide safety and security for customer goods and related data
1.4.2	Comply with legal and regulatory demands on security
1.4.3	Provide safety and security for staff, information and assets
1.5	To fulfill the objectives the SSG-SMS is focused on a structured approach that governs the security work worldwide in Schenker Singapore in accordance with the method presented in a Plan-Do-Check-Act which is an iterative four-step problem-solving process. The general work process in SSG-SMS is defined by four keys.
Plan:	Design or revise business process components to improve results
Do:	Implement the plan and measure its performance
Check:	Assess the measurements and report the results
Act:	Decide on changes needed to improve the process
1.6	The fundamental idea behind this work process is to:
1.6.1	Break down barriers between departments
1.6.2	Management should learn their responsibility, and take on leadership
1.6.3	Improve constantly
1.6.4	Institute a program of education and self-improvement
1.7	SSG-SMS's objectives together with the Plan-Do-Check-Act process will lead to:
1.7.1	That security work will continue throughout the entire corporation without any gaps or internal barriers. The SSG-SMS security objectives will thereby be fulfilled.
1.7.2	The establishment of responsibility for management on different levels, this allows management to take leadership and develop the security work according with the SSG-SMS structure
1.7.3	A culture of continuous improvement by guidance of the Plan-Do-Check-Act process.
1.7.4	A general security work process facilitating a coherent and suitable security system for guidance of the actors in Schenker Singapore.
2.0	The structure of this Manual
SM 01: Introduction to Security Management System	

This chapter contains a general description of the security effort within Schenker Singapore. The scope and the general work process description are presented. The structure of the entire SSG-SMS document is denominated where all chapters and appendices are presented with regards to availability, usability and content. The different elements in the SSG-SMS are explained and general requirements for security in Schenker Singapore are outlined.

#### SM 02: Security Policy

The foundation for the Schenker Singapore security concept is the Security Policy. In this Chapter the Security Policy and the coverage is presented and explained. The framework of the Security Policy is built on three pillars which are described in this chapter. The consistent usage of best practise strategy combined with the continuous improvement process is the uniting factor for the entire SSG-SMS.

#### SM 03: Security Risk Assessment & Planning

The continuous improvement process being an essential part of the SSG-SMS is presented and explained in this chapter. This includes presentation of the targets and the usability of the process.

#### SM 04: Implementation, Operation & Responsibilities

This chapter contains a general description about authority, responsibility and accountability with regards to the SSG-SMS and the general security efforts within Schenker Singapore. The needed competence, training and awareness for personnel are also presented in this chapter as well as communication and documentation. The need to establish control of documents, data and operations is obvious.

#### SM 05: Checking & Corrective Action

This chapter addresses the vital issue of checking that all Schenker Singapore issued security measures are in place and take appropriate corrective actions to fulfil the objectives of the SSG-SMS. In general, this chapter contains the Check and Act steps in the Plan-Do-Check-Act (PDCA-process).

#### SM 06: Management Review

This responsibility is exercised through the management review process within the boundaries of SSG-SMS. Reviews shall include assessing opportunities for improvement and the need for changes to the security management system, including the Security Policy and security objectives and threats and risks.

#### SM 07: Appendix: Documentation Matrix of ISO28000 and ISO9001

This Matrix provides reference specific documents which need to be referred to as well as generic documents which may be used by the respective Schenker Singapore Organizations.

### 3.0 Confidential and available parts of the Schenker Singapore security management system

	Public available	Schenker Singapore internal	Schenker Singapore classified
Table of Contents	Yes	Yes	Yes
SM 01	No	Yes	Yes
SM 02	Yes	Yes	Yes
SM 03	3.1	Yes	Yes
SM 04	No	Yes	Yes
SM 05	No	Yes	Yes
SM 06	No	Yes	Yes
SM 07 - Appendix	No	No	Yes

### 4.0 Scope

4.1 Based on the Corporate GSMS and SAP-SMS, SSG-SMS aims to provide all Schenker sites within Singapore with a mutual and common structured approach to establish security. The SSG-SMS appoints limitations and inclusions of expectations, responsibilities, and objectives.

4.2 The SSG-SMS is a coherent instruction in order to achieve a good and serving security system. The SSG-SMS establish a structured method to proactive restrain and prevent potential security breaches to become a full scale security incident. It shall also provide instructions to minimize negative business consequences.

4.3 The global aspect of security within Schenker Singapore has increased due to customer demands and the increasing risk for terrorist attacks on world trade. The SSG-SMS provides Singapore response regarding security to secure the entire Schenker Singapore Organization within Schenker AG's network.

## 5.0 Outline for Schenker Singapore Security

5.1 The foundation of the Schenker Singapore security management system is directly linked to the Schenker AG GSMS. The dependence of the two security management systems is expressed in the below figures. In this figure are the key elements of the system visualized. The SSG-SMS relates to Schenker Singapore and shall be seen as one vital part of all services and function within the company that provides customer value.

### 5.1 The Schenker AG security foundation

### 5.2 The Schenker Singapore security foundation

5.3 To monitor, control and develop all security related features in Schenker Singapore, the SSG-SMS uses four elements.

5.3.1 The Singapore Security Mapping Tool (SSMT), which provide the entire Schenker Singapore with up-to-date information about the security status in all Schenker Singapore sites. The information in the SSMT is considered classified and only available on a need-to-know-basis.

5.3.2 The governing structure is found in the Schenker Singapore Security Policy which is the visionary and the governing part for the SSG-SMS. The Security Policy is built on three pillars.

5.3.3 The development and corrective measures, reflected in SSMT, and based on the guiding principles in the Security Policy, with the aim to establish a culture of continual improvement.

5.3.4 The SRA Sub-Committee is composed of key personnel with different competence, responsibilities and authority that provide Schenker Singapore security through the SSG-SMS with knowledge and business understanding.

5.4 The core of the Schenker Singapore security is that all involved personnel contributes overall business efficiency, safety and security in a structured continuous improvement process which seeks to establish the best practice security solutions for customer and authority demands.

## 6.0 Schenker Singapore Security Management System Elements

6.1 The Plan-Do-Check-Act process is described in the SSG-SMS in five steps, which is an additional step to the classic Plan Do Check Act process, but the philosophy is still the same.

The five steps in the SSG-SMS process are:

6.1.1 Policy

6.1.2 Security risk assessment & planning

6.1.3 Implementation and operations

6.1.4 Checking & corrective actions

6.1.5 Management review

6.2 The four steps in the Plan Do Check Act process are easy to spot whilst the fifth step, the plan-step (P) is split into two steps in the SSG-SMS, policy and security risk assessment & planning. All five steps are equally important to fulfil in order to achieve the objectives of the SSG-SMS. The general work process is illustrated in the below figure.

### Security Management System Elements

6.3 The five elements or process steps in the SSG-SMS will together govern the continuous work to achieve the objectives of the SSG-SMS.

7.0 Analysis of the three Pillars being the foundation of the Schenker Singapore Security Management System

7.1 Pillar: Personnel Awareness and Attitude

- 7.1.1 All personnel involved in Schenker Singapore shall have the necessary awareness training about potential threats against the entire business process within Schenker Singapore. Security awareness will provide all personnel with a correct reaction, when a security breach occurs. The security awareness will together with understanding and acknowledgement of the Schenker Singapore Security Policy establish security awareness.
- 7.1.2 The attitude of personnel part of Schenker Singapore is expected to be positive and thereby contributing to a better working environment. The security training of personnel is vital for obtaining a positive attitude.
- 7.1.3 The attitude of individuals is a result of observational learning from their environment. This means that all personnel are contributing to the attitude towards a good security culture. This requires behaviour transparency and mutual recognition of minimum security requirements for all personnel in Schenker Singapore.
- 7.1.4 Trust is a relationship of reliance. Trust means a perception of honesty, competence and similar values. The creation of trust needs all three determinants but trust can be lost if one of these three determinants is violated. The different levels of management are required to take the leadership role to achieving the objectives in the SSG-SMS. This leadership is based on competence, responsibility, attitude and effective use of the Plan Do Check Act-process method. The leadership role has a severe influence on personnel's awareness and attitude towards not only the SSG-SMS but all business processes and contributes in reaching the Schenker Singapore Mission Statement.
- 7.2 Pillar: Procedures and Best Practice
- 7.2.1 All processes within Schenker Singapore are governed by the usage of procedures. These procedures are specifications of series of actions, acts or operations which have to be executed in the same manner in order to always obtain the same result at the same circumstances. The security aspect is a vital part of all processes why security must be present in all procedures. The design and evaluation of procedures are conducted with the use of the best practice philosophy.
- 7.2.2 Best practice signify that there is a technique, method, process, activity, incentive or reward that is more effective at delivering a particular outcome than any other technique, method, process, etc. The concept of best practice aims to reduce problems and unforeseen complications, than otherwise would emerge. Best practice defines both the most efficient (least amount of effort) and effective (best results) way of accomplishing a task, based on repeatable procedures that have proven themselves over time for large numbers of people. With this said, best practice does not imply inflexible, unchanging practice. Best practice is based around continuous learning and continual improvement.
- 7.2.3 In order to obtain, develop and implement the usage of best practice in Schenker Singapore, it is of vital importance to ensure a positive and successful benchmarking and best practice transfer effort. This process is conducted in three steps.
- 7.2.3.1 The best practice transfer effort is a people-to-people process
  - 7.2.3.2 Learning and transfer is an interactive, ongoing, and dynamic process that cannot rest on a static body of knowledge.
  - 7.2.3.3 Benchmarking stems from a personal and organizational willingness to learn.
- 7.3 Pillar: Physical and Data Security
- 7.3.1 Physical security is visualised with smart usage of different types of security breach preventive measures. These countermeasures aims primary to prevent security breaches in Schenker Singapore installations. The basic effort in physical security is to increase the perceived effort and/or the perceived risk for the potential perpetrator. By carefully prepared combination of physical security efforts that makes it harder and riskier for potential perpetrators to succeed in creating security breaches, will this pillar contribute to the SSG-SMS's objective.

**Document Section:**

<b>Doc Type:</b>	Security Manual	<b>Status:</b>	Published
<b>Doc No:</b>	SM 00	<b>Effective Date:</b>	27-08-2013
<b>Revision No:</b>	4.0	<b>Created By:</b>	Ali Saafri
<b>SectionName:</b>	Loss Prevention		
<b>Title:</b>	Table to contents		

**Document Section:**

✚ -	
Security Manual Content	
SM 00	Table of contents
SM 01	Introduction
SM 02	Security Policy
SM 03	Security Risk Assessment & Planning
SM 04	Implementation, Operation & Responsibilities
SM 05	Checking & Corrective Action
SM 06	Management Review and Continual Improvement
SM 07	Appendix 1: Documentation Matrix of ISO28000 and ISO9001


**Document Section:**

<b>Doc Type:</b>	Security Manual	<b>Status:</b>	Published
<b>Doc No:</b>	SM 07	<b>Effective Date:</b>	03-08-2012
<b>Revision No:</b>	4.0	<b>Created By:</b>	Ali Saafri
<b>SectionName:</b>	Loss Prevention		
<b>Title:</b>	Appendix 1 - Documentation Matrix of ISO28000 and ISO9001		

**Document Section:**

✦ - Documentation Matrix of ISO28000 and ISO9001					
Clause	ISO28000 requirements	ISO28000 Manual	ISO28000 Procedure	QEHS manual	QEHS Procedure
4.1	General requirements	SM 01	NA	NA	NA
4.2	Security management policy	SM 02	NA	NA	NA
4.3.1	Security risk assessment	SM 03	P-SER-SCH-431-01 SRA	NA	NA
4.3.2	Legal, statutory and other security regulatory requirements	SM 03	P-SER-SCH-432-01 Legal, statutory and other security regulatory requirements	NA	NA
4.3.3	Security management objectives	SM 03	P-SER-SCH-431-01 SRA	NA	NA
4.3.4	Security management targets	SM 03	P-SER-SCH-431-01 SRA	NA	NA
4.3.5	Security management programme	SM 03	P-SER-SCH-431-01 SRA	NA	NA
4.4.1	Structure, authority and responsibilities for security management	SM 04	P-SER-SCH-441-01 SMRA organisation chart	QM 06 Responsibility and Authority  QM 07 Organisation Chart-Top Management	NA
4.4.2	Competence, Awareness and Training	SM 04	NA	QM 26 Training	P-QUA-HR-06-03 Training  P-QUA-HR-06-04 On Job Training (OJT)
4.4.3	Communication	SM 04	P-SER-SCH-443-01 Communication	NA	NA
4.4.4	Documentation	SM 04	NA	QM 13 Document and Data Control	P-QUA-SCH-04-04 Document and Data Control
4.4.5	Document and data control	SM 04	NA	QM 13 Document and Data Control  QM 24 QEHS Records	P-QUA-SCH-04-04 Document and Data Control
4.4.6	Operation control	SM 04	NA	NA	P-QUA-LP-07-01 Loss prevention
4.4.7	Emergency preparedness response and security recovery	SM 04	NA	QM 34 Emergency Management	P-QUA-LP-07-02 Bomb threat management  P-EHS-SCH-447-001 Emergency preparedness and response  P-QUA-FAC-07-04 Emergency response procedure  P-QUA-FAC-07-05 Contingency planning

4.5.1	Security performance measurement and monitoring	SM 05	P-SER-SCH-451-01 Security performance measurement and monitoring	NA	NA
4.5.2	System evaluation	SM 05	NA	NA	NA
4.5.3	Security related failures, incidents, non conformances and corrective and preventive action	SM 05	P-SER-SCH-453-01 Incident reporting	NA	NA
4.5.4	Control of records	SM 04	NA	QM 24 QEHS Records	P-QUA-SCH-04-03 Control of Records  P-QUA-SCH-04-04 Document and Data Control
4.5.5	Audit	SM 05	NA	NA	P-QUA-SCH-08-01 Internal Audit
4.6	Management review and continual improvement	SM 06	NA	NA	P-QUA-SCH-05-02 Management Review





#### Document Section:

<b>Doc Type:</b>	Security Manual	<b>Status:</b>	Published
<b>Doc No:</b>	SM 04	<b>Effective Date:</b>	03-08-2012
<b>Revision No:</b>	4.0	<b>Created By:</b>	Ali Saafri
<b>SectionName:</b>	Loss Prevention		
<b>Title:</b>	Implementation, Operation and Responsibilities		

#### Document Section:

✚ -	
<b>1.0 Implementation, Operation and Responsibilities</b>	
1.1	This chapter address how Schenker Singapore SMRA Sub-Committee is organised and how responsibilities are allocated. Implementation and operational responsibilities are described on the basis of how the security network within Schenker Singapore is organised.
1.2	Top management responsibilities
1.2.1	The responsibility and authority for all security issues are within the Schenker Singapore board. The Country Security Manager is responsible and authorized to act within the authority of the Schenker Singapore board.
<b>2.0 Operational Structure for Security Management</b>	
2.1	Organizational structure
2.1.1	The top management organization structure shall be documented in QM 07 - Organisation Chart - Top Management
2.1.2	SMRA Sub-Committee structure shall be documented in P-SER-SCH-441-01 - SMRA Sub-Committee structure, authority and responsibilities.
2.2	Communication structure
2.2.1	Due to the large number of Schenker Singapore employees and activities in a number of facilities, it is important that communication is well channelled in order for information, directives to reach the proper receivers and for important feed-back to be channelled backwards. The Schenker Singapore Management Organizational Structure is supported by appointed persons who shall be the primary sources of received and sent information.
2.3	Security Steering Committee
2.3.1	Security Management System (SMS) Committee
2.3.1.1	The SMS Committee is made up of appointed persons in the Schenker Singapore Management Organizational Structure.
2.3.2	Security Management Risk Assessment (SMRA) Sub-Committee
2.3.2.1	Schenker Singapore incorporated a Security Management Risk Assessment (SMRA) Sub-Committee which ensures the continuity of managing and controlling an approved security risk management process on behalf of the Schenker Singapore Organization.
2.3.2.2	The SMRA Sub-Committee is made up of Schenker Singapore employees and potentially Subject Matter Experts (SME) that have a detailed knowledge of the Organizations security systems and sub-systems and a thorough understanding of the impact of those systems.
2.3.2.3	Each member will be appropriately selected by the SMS Committee including the SMRA Sub-Committee.
2.3.2.4	The SMRA Sub-Committee has been formed to ensure that the Organization remains compliant with security standards.
2.3.2.5	The SMRA Sub-Committee is tasked to identify, analyze, evaluate and treat security related risks using the internally approved SRA tools and methodology. Assessment of the effectiveness of the existing security systems is also incorporated. Findings and recommendations are recorded and communicated effectively for regular review and continual improvement.
2.3.2.6	Review is done periodically every two months or when there are major changes occur in the operation or in the Organization that affect the threats to security.
2.3.2.7	To report security risks, findings and recommendations to SMS Committee, the SMRA Sub-Committee will utilize security risk assessment worksheets that detail among others the critical assets, risk analysis, recommended new controls.
2.3.2.8	The SRA risk register is considered a 'live working document' that can be used to add new risk or for base line reference and re-assessment of existing risks.

2.3.2.9 The SMRA Sub-Committee will report to the Security Management System (SMS) Committee on a regular basis who are responsible for the overall management, review and maintenance of the Schenker Singapore Security Management System in compliance with the set security specifications.

2.3.2.10 It further has the responsibility of guiding Organization with regard to security processes, which includes submissions of proposals to develop and improve the SSG-SMS, make recommendations and submissions of reports to the Schenker Singapore SMS with the aim to:

- 2.3.2.10.1 improve and enhance security procedures, measures and systems
- 2.3.2.10.2 be responsible for the overall design, maintenance, documentation and improvement of the organization's security management system;
- 2.3.2.10.3 identifying and monitoring the requirements and expectations of the organization's stakeholders and taking appropriate and timely action to manage these expectations;
- 2.3.2.10.4 advising on the availability of adequate resources;
- 2.3.2.10.5 considering the adverse impact that the security management policy; objectives, targets, programmes, etc. may have on other aspects of the organization;
- 2.3.2.10.6 ensuring any security programmes generated from other parts of the organization complement the security management system;
- 2.3.2.10.7 communicating to the organization the importance of meeting its security management requirements in order to comply with its policy;
- 2.3.2.10.8 ensuring security-related threats and risks are evaluated and included in organizational threat and risk assessments, as appropriate;
- 2.3.2.10.9 ensuring the viability of the security management objectives, targets and programmes.
- 2.3.2.10.10 maintenance of the related Master Documents concerning security standards
- 2.3.2.10.11 assist in Security Risk Assessments
- 2.3.2.10.12 conduct internal audits to assess the effectiveness of Security Management System in place

2.3.2.11 A procedure shall be written to describe the requirements, roles and responsibilities of the SMRA Sub-Committee.

## 2.4 Product Management, Air, Land, Logistics, Ocean

2.4.1 The PM functions are actively participating in the continuously development of a security regime for the Organization through the steering committee as well as via the SMRA Sub-Committee. The PM functions are responsible for that security measures in line with instructions outlined the SSG-SMS and specific for their modal responsibility are implemented and carried out in cooperation and coordination with security functions. Additional mode specific security responsibilities are, inter alia;

- 2.4.1.1 Develop guidelines, give advice and information to support security implementation
- 2.4.1.2 Monitor compliance with SSG-SMS
- 2.4.1.3 Assist in training activities
- 2.4.1.4 Support in security audit activities
- 2.4.1.5 Ensure compliance with SSG-SMS for contractual agreements
- 2.4.1.6 Proactive approach in developing, testing and implementing mode specific customer security requirements

## 2.5 IT Department

2.5.1 The department is responsible for information and data security and has the task to develop appropriate tools to that purpose.

## 2.6 Sales & Marketing

2.6.1 Sales & Marketing are actively participating in the continuously development of a security regime for the Organization through the SMRA Sub-Committee. Sales & Marketing process tenders and support the implementation of security related requirements linked to business agreements in business units, regions, countries and branches. Specific security responsibilities in connection with customers are, inter alia:

- 2.6.1.1 Collection of customer requirements;
- 2.6.1.2 Transfer of customer requirements;
- 2.6.1.3 To support implementation of security requirements for new business
- 2.6.1.4 Customer interface to security issues when starting up new business
- 2.6.1.5 Support in audit activities required by customers
- 2.6.1.6 Ensure compliance with SSG-SMS for contractual agreements
- 2.6.1.7 Marketing existing security products
- 2.6.1.8 Assist in training activities

## 2.7 Human Resources

2.7.1 Schenker Singapore Human Resources responsibility relates to Schenker personnel and is supporting country Organizations in the development of guidelines for employment of personnel with regards to vetting and fulfilment of security requirements whether these are of a legislator origin or customer driven. The department is acting as a focal point with regards to specific matters for screening of personnel against lists of denied parties. Development and maintenance of a global "Code of Conduct" for Schenker personnel on security behaviour is the responsibility of Schenker Singapore Human Resources and to support country HR in monitoring the compliance of security requirements directed at Schenker personnel. Specific security responsibilities for Human Resources Department are, inter alia:

- 2.7.1.1 Supportive for training activities

- 2.7.1.2 Active involvement in developing training material
- 2.7.1.3 Facilitate vetting activities
- 2.7.1.4 Support the development of security guidelines for employees

## 2.8 Other Organizational Stakeholders

2.8.1 Departments not mentioned elsewhere in the SSG-SMS are required to assist in security related issues when these interact in the department's area of responsibility but is driven by a department specifically outlined in the SSG-SMS. Each department with a specific responsibility laid down in the SSG-SMS is required to cooperate and coordinate security related issues with any stakeholder at Schenker Singapore being concerned by a security issue of whatever reason.

## 3.0 Competence, Training and Awareness

3.1 An important cornerstone of the Schenker Singapore security program is the proper level of attitude and awareness giving personnel the incentive to react on security shortages discovered on all levels and for all processes in the Schenker Singapore Organization. The SSG-SMS is only fitted to its purpose as the knowledge that others have of the system why training is essential to that respect. Personnel must receive security training commensurate with job descriptions varying from awareness training to function specific training. Qualified training leads to high competence which will facilitate Schenker Singapore fulfilment of compliance with security demands initiated either by Authorities or by customers.

## 4.0 Emergency Preparedness Response and Recovery

4.1 Any incident that occurs within Schenker Singapore which has an impact on the security integrity, property and safety of the organisation shall require Emergency Response and Recovery. It could be a fire in the building, an act of terrorism, an epidemic outbreak, a natural disaster or anything that requires a significant amount of effort and resources to resolve.

4.2 Procedures entailing Emergency Response, Contingency Planning, Disaster Recovery Plan and Bomb Threat Management Plan shall be written.

## 5.0 Loss Prevention

5.1 The purpose of this procedure is to provide a formalized method of communicating the procedures, guidelines and other relevant information within Schenker Singapore with regard to Cargo Loss Prevention and its many functions. The document forms the mandatory minimum Cargo Loss Prevention standards within Schenker Singapore. The procedure is valid for all transport modes, warehousing and logistic services.

## 6.0 Denied Parties (Sanction List)

6.1 UN resolution 1373/2001 and 1390/2002 and EC Regulations No 2580/2001 and No 881/2002 state that "funds and other financial assets or economic resources of certain individuals, groups, undertakings and entities, including funds derived from property owned or controlled, directly or indirectly, by them or by persons acting on their behalf or at their direction shall not be made available." The all-embracing purpose with legislation based on the resolutions and regulations is to prevent or minimize the risk of terrorist attacks. For Schenker Singapore this implies that measures need to be implemented to secure its part of the supply chain. The purpose of the data comparison is to identify all parties/persons with a direct or indirect business relation to Schenker Singapore in order to guarantee that no current relations exists between Schenker Singapore and those listed or that Schenker Singapore does not enter into a business relationship with parties/persons on the sanction lists. The work with denied parties or sanction list is mandatory for all Schenker Singapore companies.

6.2 An internal "Denied Parties Manual" has been developed for the work to be carried out by appointed Schenker staff. The manual is found at Corporate Intranet/Risk Management.

## 7.0 Control of Documents and Records

7.1 No part of the SMS Manual, related Policies and Procedures may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording and / or otherwise without the prior consent of the SMS Management Representative.

7.2 The SMS Management Representative / Document Controller shall be responsible for the overall control and coordination of the SMS Manual, related Policies and Procedures for distribution and amendments. Controlled copies of the SMS Manual, Security Policies and Procedures are kept in the eQMS (electronic SMS Management System) in the folder of the SMS Manual.

7.3 Uncontrolled copies of the SMS Manual, related Policies and Procedures may be distributed to customers or interested parties and shall thereon after not be updated.

**Document Section:**

<b>Doc Type:</b>	Security Manual	<b>Status:</b>	Published
<b>Doc No:</b>	SM 05	<b>Effective Date:</b>	19-08-2013
<b>Revision No:</b>	5.0	<b>Created By:</b>	Ali Saafri
<b>SectionName:</b>	Loss Prevention		
<b>Title:</b>	Checking and Corrective Action		

**Document Section:**

✚ -

**1.0. Checking & Corrective Action**

All checking and corrective actions of security related matters must be preformed in a structured way in order to ensure credibility.

**1.1 Security performance measurement and monitoring**

Security performance must be monitored and measured in an objective manner. This can be achieved in different ways through i.e. collection of statistics from in-house systems, self audits and from customer complains.

**1.1.1 Performance measures**

The primary type of security performance measurement is quantitative and is based on reports or other information sources.

**1.1.2 Monitoring security performance**

The monitoring of the security performance is an ongoing process. The aim is to identify emerging risks and address them by executing the security & risk assessment process.

**1.1.3 Measurement of compliance with supply chain security programs**

The usability of the SSG-SMS is closely linked to the compliance with different supply chain security programs. The measurement of system compliance is a proactive process that is fulfilled through assessment of the security programs content in relation to the current status of the SSG-SMS.

**1.2 Schenker AG security fulfilment – Global Security Mapping Tool**

1.2.1 The Global Security Mapping Tool will provide Schenker Singapore in line with Schenker AG with an Intranet-online program providing the results of the level of security at each Schenker Singapore site.

1.2.2 The information will be supervised and updated on a regular basis and as a minimum, twice per year. The Global Security Mapping Tool shows also the planning of future security installations and implementation of processes with the aim to further increase security at a Schenker Singapore site. The information can be used by local management for investment planning. Responsible for maintaining and updating the records are the Company Security Managers assisted by Site Security Managers.

**1.3 Incident reporting system**

1.3.1 An Incident Report System shall be developed for incident reporting with regards to security related incidents and escalation to Schenker AG. If there for some reason is a security related incident which not involves a claim for a customer, supplier or third party the incident shall be reported to the Country Security Manager.

1.3.2 Security related failures needs to be investigated in order clarify the involved chain of events that contributed to the failure. Following the investigation and the results from the investigation, measures must be taken to prevent further occurrences by appropriate corrective and preventive actions.

**1.4 Audits**

1.4.1 The operational control of security performance and security status is partly established by the use of audits, internally as well as externally driven. The backbone of operational control is the Schenker Singapore Security Mapping Tool identifying the full security status for each Schenker Singapore site. The use of the tool implies a continuous auditing process within the entire Schenker.

The self-auditing activities necessary for fulfilling the Schenker Singapore Security Mapping Tool shall be complimented with regular internal audits via the use of checklists.

1.4.2 Internal audits shall be carried out on a regular basis and cover all security related procedures and physical security being implemented and installed as well as awareness amongst personnel received through training and training records. Deficiencies that are discovered must be recorded and attended to without delay. Where possible, audits shall be conducted by personnel independent of those having direct responsibility for the activity being examined.

1.4.3 A security audit may be integrated into audits for e.g. quality, environmental, safety, dangerous goods, compliance issues related to the usage of the ISO framework.

## **1.5 Questionnaires**

1.5.1 The primary information source for monitoring the current security status in country Organizations and sites is the Schenker Singapore Security Mapping Tool. The security data contained in the system may be used for fulfilling customer requests for filling in questionnaires addressing the security status in a Schenker Singapore company or site. Such requests shall however be analysed by the Company Security Manager and if necessary be approved by the local management before carried out. Normally such customer requests are channelled through Sales & Marketing, which has a coordination responsibility. The data contained in the Schenker Singapore Security Mapping Tool may also be used for internally initiated questionnaires.

**Document Section:**

<b>Doc Type:</b>	Security Manual	<b>Status:</b>	Published
<b>Doc No:</b>	SM 03	<b>Effective Date:</b>	03-08-2012
<b>Revision No:</b>	4.0	<b>Created By:</b>	Ali Saafri
<b>SectionName:</b>	Loss Prevention		
<b>Title:</b>	Security Risk Assessment and Planning		

**Document Section:**

✦ -	
<b>1.0</b>	<b>Security Risk Assessment &amp; Planning</b>
1.1	Security responsible persons of the SMRA Sub-Committee shall be guided by the SSG-SMS and the Schenker Singapore Security Mapping Tool, establish and maintain Security Risk Assessment & Planning (SRA) procedures. The procedures shall provide the structured method for identification and assessment of security threats and security management-related threats and risks. Further on, the process governs the working process of identification and implementation of necessary SSG-SMS countermeasures to fulfill the Schenker Singapore Mission Statement.
1.2	The SRA shall consider the risk (likelihood and all potential consequences) to the following security risk sources such as:
1.2.1	Criminal actions
1.2.2	Terrorist actions
1.2.3	Malicious damages
1.2.4	Security threats that may cause operational problems
<b>2.0</b>	<b>Security objective</b>
2.1	The three objectives of the SSG-SMS shall be in line with the concept of continual improvement, quantified and communicated within Schenker Singapore and reviewed by the SMRA Sub-Committee before added to the SSG-SMS. The different objectives address different stakeholder's needs and demands for fulfilling the security efforts. The objectives present three different objectives:
2.2	<u>The Customer Objective:</u>
2.2.1	The increasing customer demands on both effectiveness and security is the driving force in this view point.
2.3	<u>The Legal and Regulatory Objective:</u>
2.3.1	Different authorial supply chain security programs together with associational security initiative provide a distinct and applicable foundation for all security work related to Schenker Asia Pacific's mission statement.
2.4	<u>The SMRA Sub-Committee Objective:</u>
2.4.1	Together with the other two objectives, the SMRA Sub-Committee's need for safety and security will provide the objective in order to make the security effort complete.

### 3.0 Security targets

3.1 The security targets shall be defined / described with:

- 3.1.1 Up to an appropriate level of detail;
- 3.1.2 Specific, measurable, achievable, relevant and time-based (where practicable);
- 3.1.3 Communicated to all relevant employees and third parties including contractors with the intent that all are made aware of individual obligations;
- 3.1.4 Include a cost benefit analysis

3.2 Different security targets shall be defined on country and site level. Mode specific functions with security targets are defined by the PM functions. The security targets are reviewed annually and include cost benefit analysis and a result report. The different security targets shall be in line with the objectives of SSG-SMS and coordinated with SMRA Sub-Committee.

### 4.0 Legal, statutory and other security regulatory requirements

4.1 The SSG-SMS demonstrate a continuous improvement procedure that:

- 4.1.1 Identifies applicable legal requirements
- 4.1.2 Identifies business related security requirements
- 4.1.3 Determine how various requirements influences SSG-SMS, Schenker Singapore Security Standards, Schenker Singapore Security Mapping Tool and the SRA Sub-Committee.
- 4.1.4 Implement procedures that fulfil the legal and business related security requirements.

4.2 The review of the SSG-SMS compliance with legal and regulatory demands is, from a business perspective, of outermost importance. The compliance review process is therefore closely linked to the top management review of the SSG-SMS. The compliance review process shall include:

- 4.2.1 Evaluation and assessment of the different legal and regulatory demands from both a compliance and business perspective,
- 4.2.2 Communication of the different legal and regulatory demands within the Schenker Singapore,
- 4.2.3 The compliance review process shall be proactive,
- 4.2.4 Contribute to a security culture that embraces the different legal and regulatory demands.

### 5.0 The security risk assessment process

5.1 The core of the SSG-SMS is the security & risk assessment process aimed at continuous improvement. The process shall establish and maintain the practical implementation related to the three pillars of SSG-SMS. The security & risk assessment process shall be used on all levels in Schenker Singapore from site level and cargo carrier unit to management level. A procedure shall be written to describe the Security Risk Assessment Process.

### 6.0 Information Sources

6.1 The security & risk assessment process is only as good and credible as the credibility of the used information and data within the process itself. Different information sources that may be used for such a process are:

- 6.1.1 Statistics from Claims
- 6.1.2 Information from Schenker Singapore Security Mapping Tool
- 6.1.3 Local police crime statistics
- 6.1.4 Uniform Crime Reports or comparable data
- 6.1.5 Previous security & risk assessment process outputs
- 6.1.6 Customer requirement on security
- 6.1.7 Regulatory security demands (C-TPAT, TAPA, AEO, STP etc.)
- 6.1.8 Prior complaints from employees, customers, guests, visitors, etc.
- 6.1.9 Prior civil claims for inadequate security


- 6.1.10 Intelligence from local, state, or national law enforcement agencies about potential threats
  - 6.1.11 Industry-related information about trends
  - 6.1.12 General economic conditions of the area
  - 6.1.13 Presence of a crime magnet (e.g., proximity of a popular night club, continuous presence of vagrants, property in disrepair)
  - 6.1.14 Scientific reports, papers and thesis
-



**Document Section:**

<b>Doc Type:</b>	Security Manual	<b>Status:</b>	Published
<b>Doc No:</b>	SM 02	<b>Effective Date:</b>	06-08-2012
<b>Revision No:</b>	4.0	<b>Created By:</b>	Ali Saafri
<b>SectionName:</b>	Loss Prevention		
<b>Title:</b>	Security Policy		

**Document Section:**

 -

## SCHENKER SINGAPORE PTE LTD

### SECURITY POLICY

The Schenker Singapore (Pte) Ltd security policy provides the foundation for all security-related issues and activities within the organisation, aiming to promote security at the workplace, the collective responsibility of the Management and awareness to all employees.

As part of our security management system framework, we aim to ensure safe, secure and efficient supply chain services by protecting our company's employees, assets, information, integrity and reputation from potential threats. To achieve this objective, we will comply with:

- ISO 28000 : 2007,
- Current applicable legislation, regulatory and statutory requirements and other requirements to which Schenker Singapore (Pte) Ltd subscribes to,
- Schenker Singapore (Pte) Ltd organisational policies.

We are committed to ensure the security of our operations through continual improvement of our security management system.

This policy will be effectively communicated to our Business Partners.