

DRAFT



**Rx-360 Supply Chain Security White Paper:
Audits and Assessments of Third Party Warehousing
and Distribution Facilities**

1 June 2012

INTRODUCTION

Today's global corporations frequently outsource various business functions to organizations that have specialized expertise. While outsourcing can offer improved efficiency and cost savings, it also creates certain risks to product security. The primary risks to products are counterfeiting, diversion, theft and adulteration. While all of these risks exist in both corporate and outsourced facilities, theft and diversion of drug product at and through third party Logistics Service Providers (LSP) are significant risks. LSPs provide a client company with warehousing, distribution and logistics services. This business risk further increases as the industry moves into emerging markets where supply chain visibility is poor, security knowledge and standards are lower, and the risk of criminal activity is higher. The primary defense against these risks is an appropriate security program with expectations and responsibilities conveyed through contracts and confirmed via assessments and audits.

The focus of this white paper is to assist manufacturer clients by providing a framework from which they can select the elements and aspects that are best matched to their risk tolerance and apply it via the system outlined in this document or via their own customized version of the system to maximize the protection of their patients, their brand, and their organization.

The paper will outline the elements of an effective Security Plan. These elements are intended to work together as a system. As an example, often seen is the company that will spend significant resources on background checks for employees, and on electronic access control, only to allow temporary staff unfettered access to the building without conducting a background check, or at least specifying the items which should be checked by the contracting agency and implementing an audit program. In short, the access control program loses effectiveness unless only vetted people are allowed unescorted access.

Next the paper will discuss the mechanisms by which a manufacturer client can identify (or 'map') and prioritize the reviews of their third-party LSPs. This prioritization can be a very simple process or a very complex process dependent upon the extent to which a company outsources these services and the geographies in which they operate. This section discusses the application of risk to the prioritization and the methods an organization with a complex network of outsourced providers can use to assist in the collection of this information. Once the risk levels have been assigned and the mitigation levels have been assessed, the organization's audit prioritization can be put into place and the appropriate resources applied to conduct these reviews.

Finally, the aspects of the audit and the follow-up action, as well as the two companion documents are discussed briefly. This process and these two documents are intended to serve as tools which manufacturer clients can use to develop their own systems, contracts, audits and assessments that meet their risk tolerance levels. As always, these tools should be applied in accordance with applicable laws and regulatory requirements.

SECURITY PLAN ELEMENTS

Overview

LSP security encompasses all aspects of an operation's security program including physical security, access control, records and logs, procedural security, personnel security, cargo security, control of goods, returns and rejected product, reporting and notification, and information protection. These elements must be mapped throughout the entire distribution and storage network. As a result of the complex and varied nature of LSP networks, defining applicable security requirements becomes a customized effort. As such, creating a singular solution is not feasible. Rather, assembling a set of LSP security assessment and auditing standards is a more practical approach. These security standards can then be utilized throughout the selection and contracting process, as well as during the ongoing monitoring of outsourced logistics service providers. They will serve as the baseline security practices from which an organization can develop an optimum security system that encompasses relevant policies, procedures, equipment, and personnel. The following information provides an overview relative to these elements.

General Requirements

Each LSP should have a person appointed as a security manager. This individual must identify and understand the nature of the security risks throughout the supply chain, and thereby apply appropriate financial and managerial controls to mitigate those risks. Security issues such as loss of product must be investigated and the effectiveness of the security measures determined and monitored. The LSP security manager will serve as the primary liaison with the client corporation, law enforcement, and the public, as needed.

The LSP should create a written set of security policies requiring compliance from employees, visitors, suppliers, and contractors. These policies should include access control, employee and visitor identification devices (e.g., ID cards), vehicle security and parking, physical property security, and product integrity and security. The LSP should be restricted from sourcing products or components from anyone besides the manufacturer.

Implementing a security awareness program will help to create a security culture. Topics should include threats to the supply chain, product integrity, recognizing suspicious activity, reporting and notification procedures, and access control.

Physical Security

Physical security is that portion of a security system that protects people, property, goods and assets. This is accomplished by utilizing staffing, equipment and devices to deter an intruder. Electronic security is the electronic means used to control access, intrusion detection, alarm monitoring, communication, reporting and sensor monitoring. Also included in physical security are video

surveillance, lighting, perimeter security and auxiliary power. These aspects, working in concert, make up a comprehensive physical security program.

Access Control

Access control refers to the procedural aspects of ensuring that those personnel who are allowed access to the facility are authorized. An important component of access control is the positive verification of visitor identification and the record keeping associated with those who access the site.

Records and Logs

Record keeping is an important aspect to proper security. Accurate records should be kept regarding current and former employees and contractors, the vetting process records associated with their on-boarding, video surveillance logs, computer system logs, site access logs, driver logs, and destruction and inventory logs.

Personnel Security

Each LSP must have a process in place to conduct extensive background checks and toxicology screening (where allowed by law) on all employees tasked with the handling of pharmaceutical products or relevant information. Prior to employment, all employee checks should include past employment (dating back 5 years with extensive gaps investigated) and criminal records. Toxicology screening would include pre-employment, post-employment (random), and for cause.

Cargo Security

Cargo security measures are controls around the shipping and receiving of products. They include aspects such as loading and unloading procedures, shipment verification, driver verification, standards and briefings, segregation of functions, and the protection of shipment information. They also include use of tamper-evident seals, shipping containers, satellite tracking mechanisms and other brand protection technologies.

Control of Goods in the Facility

Part of a comprehensive security program regarding pharmaceuticals in a warehousing and distribution environment are the procedures by which access to the pharmaceutical goods are controlled and recorded. Access should be based on business need and should be tracked by proper record keeping. Electronic access is one effective means of controlling access to secure areas containing product, but robust procedures are necessary to ensure that electronic access control is effective.

Returns and Rejected Product

Control of reverse logistics is extremely important in preventing fraudulent activity within the supply chain. Products returned should be verified to ensure that quantities are as stated and that the

containers are sealed. In cases where companies are engaging in the acceptance of partial quantity returns, 100% verification of product should be conducted to ensure that the reverse logistics supply chain is not a target for counterfeit and diversion activity.

Reporting and Notification

LSP's should have robust and comprehensive notification policies in place to ensure that the manufacturer client is contacted in the appropriate time frame when incidents do occur. These policies should not only be in place prior to an incident occurring, but the timeframes can be agreed to in contract terms to ensure that compliance is met. Timely notifications in cases of loss, damage, theft, security incidents, employee and contractor background issues, solicitation by unauthorized sellers, order discrepancies, and violations of government regulations are all important to the manufacturer client.

Information Protection

Manufacturer clients should not overlook the aspects of information security in their review of LSP security programs. Many manufacturers have separate programs which address information security of both electronic and traditional aspects, but if not, this area should be addressed as part of a set of comprehensive Supply Chain Security program requirements.

MAPPING, ASSESSMENTS, AND AUDIT PRIORITIZATION

Supply Chain Mapping

The security auditing process begins with a thorough understanding of the organization's entire supply chain network. This mapping exercise is strictly focused on identification of warehousing and logistics facilities as well as paths of movement between facilities. Once this list of providers is catalogued, an organization can use different methods to assess the risk relative to their supply chain facilities. (The methods by which this risk is assigned are many and could alone be the subject of lengthy discussion, but are outside the scope of this paper.)

Risk Assessment

Working with applicable internal and external stakeholders, a list of security risks should be compiled relative to these supply chains, collated, and applied to the logistics outsourcing program. Global perspectives must be considered, as the security threats and appropriate solutions will vary regionally. If the organization does not have a component that is skilled at assigning these risks, there are many providers who can assist with this work.

A risk assessment would then be conducted for each LSP operation and environment, identifying high-risk opportunities for theft, diversion and counterfeiting, and those operations handling high-risk materials. The risk assessment should then be combined with an analysis of the third party LSP's

security program via a self-assessment of the LSP's security by their internal team which is requested by and submitted back to the manufacturer.

Self-Assessment

A Self-Assessment is a formal, systematic process of data gathering related to security measures against corporate requirements and regulatory standards. It provides the foundation and justification for implementation of appropriate security measures. The self-assessment should be comprehensive including all elements of the security program. It should be closely matched to the audit tool to ensure that the proper level of self-examination is possible by the LSP. Some organizations choose to create a questionnaire based on their audit tool for this purpose specifically.

Once the risk assessment relative to a facility is complete and the mitigation efforts are captured via a self-assessment of the LSP's Supply Chain Security, the two data sets can be combined to prioritize LSP's for auditing. It is important to take both data sets into account to properly prioritize audits and follow-up actions. A facility in a high risk geography, for example, may be employing extremely robust security measures, and the resulting net prioritization may be lower than a facility in a medium-risk geography with lax security measures.

AUDIT AND ACTION

Audit Process

A Security Audit is an extensive and formal review of an organization's comprehensive security system against the contract and all other applicable corporate and regulatory policies and guidelines. With the prioritization phase completed, a comprehensive supply-chain security audit program can be designed and implemented. A manufacturer client may find that it has 100 outsourced LSP's globally and their resulting risk assessments and Supply Chain Security self-assessments have helped them develop a list of their LSP in an order by which they believe best represents the overall need to conduct their audits. They may find that they have the ability to conduct 24 audits per year with the resources they have. This allows them to address the top quartile of their audit pool the first year and each subsequent quartile the following year, resulting in a complete review of their outsourced LSP's every four years. If the organization decides that it needs to adjust resources applied to Supply Chain Security auditing, it can do so appropriately.

Action

The audit results are then used to determine the effectiveness of the security system. Changes to the system may be indicated. The LSP should be allowed a reasonable time frame to assess each finding and develop their corrective action plan. This timeline should be agreed upon by both parties, based on the criticality of the finding and the timeline necessary to correct it. Each finding should receive a disposition: Corrective action completed; Corrective action pending (with target date); No action to be taken. Based on the response, the LSP compliance score may be adjusted.

The manufacturer client should also establish a timeline for updates to the action plan until such time that all of the actions are deemed complete. Providing timely attention to ineffective security measures is critical. The follow-up of the finding and recommendations of an audit is a critical component to an effective Supply Chain Security Audit program. Some organizations find it effective to record follow-up items on a master schedule to allow for effective review of necessary follow-up items to completion.

Follow-up Audits and the Cyclical Process

The business value of the auditing and assessment process is determined by how effectively the identified gaps in performance are closed and the business risks mitigated. Auditing and assessing is a cyclical process. Each audit cycle begins with specifying the unit to be audited, identifying the relevant standards and regulations, making observation and collecting information, assessing the information, identifying the gaps, implementing a plan to close the gaps, and following up the corrective action implementation. The follow-up audit is the most underutilized step in the audit cycle.

Follow-up audits are conducted shortly after the corrective action plan established is scheduled for completion. It is used to document that the gap in standard was effectively closed, and should be used in cases where the normal audit cycle is not sufficient to ensure that the mitigation steps put in place are both effective and sustainable.

The information from these audits should be fed back into the analysis of risk and mitigation in the audit schedule. Risk information needs to be updated, usually annually will suffice, and the mitigation strategies can be updated as assessment, audit, and follow-up audits are conducted. What results is a process by which an organization can have a living audit plan for their third party warehousing and distribution facilities.

Companion Tools

In order to assist manufacturer clients with the application of the concepts in this white paper, two tools are included as companions. The first tool is supplied in the format of a template requirements document. This document is formatted so that it can quickly be edited and included as an addendum to a contract or can be used as a points-to-consider document in formulating a standard in supply chain security in the warehousing and distribution segment of the supply chain. The second tool supplied is the template audit tool. The audit tool was designed specifically for the warehousing and distribution segment and was built to closely match the requirements outlined in the first tool. This allows for an organization to utilize the requirements in their contracts and standards, and have an audit tool that closely matches their desired contract terms so they have a cohesive audit program.

CONCLUSION

The concept of auditing service providers is not a new one. While significant risks are seen in the security arena, the security industry lacks a universally agreed upon standard to audit to, and because of this, there are gaps in many security programs. These tools were constructed with these gaps in mind.



1 June 2012

Through collaboration, a comprehensive set of template standards was organized to help manufacturers fill this need. These documents will need to be updated continually though as new risks emerge. The application then of a continually updated company standard and audit program is intended to help pharmaceutical manufacturers address the risk in the area of Supply Chain Security.