

Security Assessment for Suppliers: SLA(Security Level Agreement)

by Rafael Roseira Barbosa - November 24, 2006

Organizations' are increasingly interested in keeping corporate governance functional and suitable, either for regulatory reasons - as is the case with Sarbanes-Oxley - or for the purpose of maintaining a good internal control structure. In this scenario, it is essential to have clear knowledge of related risks, and not only those associated with the company's internal environment. This results in the extension of security, risk management and compliance actions to companies providing services and supplies, so as to ensure quality and proper management of the risks associated with the company's supply chain.

This article discusses how to use Risk Manager to conduct security assessments in suppliers.

Conducting Security Assessments

Conducting a security assessment to measure and manage risks associated with the supply chain is not much different from conducting a security assessment within the company's internal environment. One of the few differences is that the checklists to be used in these assessments are customized. This customization seeks to make the assessment process as straightforward as possible, addressing only the main risk factors. The idea is to provide a faster assessment, focusing only on the most critical elements. This characteristic is important in assessments that involve third parties, and sometimes in "field" assessments.

The first step to be taken when analyzing suppliers is to create the functional structure that will hold the assets to be analyzed. In this phase, we can choose between two possible approaches:

- Creation of a new Organization (a root element in Risk Manager's perimeter tree): In this approach, the Risk Manager user will create a new organization to hold the assets that are to be evaluated. This is done by clicking on File ? Include Organization. Parameters and assets pertaining to environments in supplying companies should be registered to this new Organization.

It is not advisable to create a new organization for each supplying company, because this would make it impossible to generate reports comparing risks in different companies since you would not be able to relate data from different organizations.

This approach is best used when your purpose is to view risks regarding the supplying companies and not to compare these risks against the risks assessed within your organization.

- **Creation of parameters within your own Organization:** This approach should be adopted when your purpose is to compare risks pertaining to suppliers with your company's internal risks. It allows you to build an awareness of the risks existing throughout your products' or services' value chain.

There is not one single correct approach. The selection will depend on the types of results you intend to view at the end of the assessment: whether you wish to see suppliers' security levels in an isolated environment, or integrated and comparable with those from your own organization.

Business Components

When working with the second approach described above, the Business Components will have already been registered and suppliers' assets need only to be related (or linked) to the associated Business Components.

If you opt to work with the first approach - creation of a new organization - it is important to register this new organization's business components. One idea is to copy your main organization's current Business Component List. You can also think of new Business Components to represent a new relationship between assets and business, different from the one used in Risk Manager's main Organization.

Perimeters and Assets

The assets to be analyzed (which can be technology, people, process, and environment assets) should be organized into perimeters when they are registered to the Functional Structure. There is no need to create an extensive perimeter tree. Providing a detailed view of how the supplying company is organized can be a complicated job which does not produce practical results. It is best to focus on creating a perimeter tree and an asset list which are consistent with the level of detail expected from the security assessment. If the scope of the supplying company related with your organization is "X" (set of servers, workstations, employees, contracts, computer applications, information flow, offices, etc.), you will enter "X" on Risk Manager to be analyzed. Some features of the assets deserve special attention during registration:

- **Relevance of the asset:** shows how relevant the asset is to the service provided by the supplying company;
- **Asset owner:** a representative of the supplying company in charge of providing information and ensuring the confidentiality, integrity and availability of the information processed using the asset;
- **Relationships with Business Components:** relationships portraying how the assets support the Business Components.

Assessment Project

Once the Functional Structure has been created, containing the Perimeters related to the Suppliers to be analyzed and their respective assets, one or more Assessment Projects should be created before the risk assessments can be started.

The purpose of an Assessment Project is to bring together a group of assets, i.e. a scope, to achieve certain results. The scope can be defined, for example, by geographic area, supplier function, area within the organization which is responsible for managing a group of suppliers, etc.

Besides the Assessment Projects, there are two other focuses for viewing assessment results: Business Components and Perimeters. These items must be properly planned so that the assessments generate risk views which effectively meet the organization's needs.

Management of the Assessment Project

Each Assessment Project created will have its own asset and perimeter scope. For each asset, there are one or more checklists to be answered. Each one of these checklists should be forwarded to the asset owner who will be in charge of answering and returning it. The checklists will then be imported to Risk Manager™.

Analysts Responsible for analysis

Analyst users, responsible for checklist analysis, should be created for each Supplier representative.

New users can be created through the option **Administration** → **System Users**. In order to guarantee the confidentiality of data pertaining to the analyses, different logins should be created for each supplying company. When more than one employee in a supplying company is responsible for answering the checklists, a different login should be created for each one of those employees.

Each checklist should then be associated to the representative in charge of answering it. To do so, edit the "Responsible Analyst" field in the "Project Management" tab in the "Assessments" module, as shown below.

Checklist customization

For a more concise and faster analysis, the checklists can be customized by previously defining some controls as **Not Applicable**. The idea is to make sure that the security assessments cause the least possible inconvenience to the supplier organization and its associates. However, keep in mind that each control considered Not Applicable represents a control point which is known but will not be analyzed.

Generation of Offline Checklists

In order for the checklists to be answered, they should be sent to the representative(s) of the Supplier companies together with Risk Manager™ Offline, which can be generated by means of the option **File → Generate Risk Manager Offline**.

To generate several checklists at once, select them by Ctrl-clicking on the checklist and right-clicking the option "Create questionnaire with the latest version".

Use of Risk Manager™ PDA for "field" assessments

If the risk assessments are to be conducted by our own associates in the supplier company's physical environment, we recommend the use of Risk Manager™ PDA. This solution greatly eases assessments, reducing the required infrastructure to a minimum: only the PDA is needed.

Use of the Comments field and the Evidence tab

To enhance the quality of a security assessment, users should be instructed to use the **Comments** field in the checklists' controls. This provides the company with further information on the reasons that justify the answers provided. Likewise, the **Evidence** tab in each control allows you to attach digital files (photos, text, spreadsheets, etc.) that serve as evidence of the current status of a given control analyzed, whether it has been implemented, has not been implemented, or is not applicable.

Importing the completed checklists

After the supplier companies have completed the checklists, they should be instructed to send the ".cht" files back to the Leader of the Supplier Companies Assessment Project. Notice that every exported checklist has a .cht extension. The leader should then import the files to Risk Manager™.

In order for Risk Manager™ to process the results of the risks identified, each of the checklists imported should have its analysis concluded.

Consolidation of results and generation of records

Before generating the reports, it is important to check whether all the checklists used in the assessment have been thoroughly completed and properly imported. Operational reports, such as ROR, or managerial reports, such as RAR, can then be generated.

Generating Index Panels is recommended. They display risks strategically while concentrating the risks encountered and the actions to be taken in a one-page report.