

The Path to Risk Communication

By Rafael Roseira Barbosa – December 6, 2006

Risks identified within an organization, as well as the corresponding corrective actions, are demonstrated to both the strategic groups and operating teams by means of Risk Communication, one of the activities performed in the scope of Risk Management. This activity is crucial in producing the necessary basis on which to implement projects, protections, policies, configurations and every other form of control aiming to reduce risks.

In order to reach the results expected from any Information Security project, it is necessary to carefully plan the ways in which the critical areas of an organization will address the risks identified by the Risk Assessments. The organization's higher management, for example, plays an extensive role approving budgets and clearing resources. The IT area will be in charge of implementing security controls in the technological environment. The Human Resources department will also play an active part delivering awareness presentations and training programs.

Below we present some reports, charts and tables that can be generated by Risk Manager™ to ease the Risk Communication activity. By means of strategic, managerial, and operating reports, information security managers can have access to resources for prioritizing risks, as well as to information on which to base risk treatment activities.

The reports most commonly used: RAR and ROR

Among the several different reports generated by the Risk Manager tool, two of them can be highlighted, for they provide a simple and practical summary of risk assessments' results:

- **Risk Assessment Report - RAR:** Because it contains mainly risk indicators, priority tables and consolidated charts demonstrating the distribution of risks, this report is widely used by managers to guide the actions that should follow the assessments.
- **Operational Risks Report - ROR:** The purpose of this report is to guide the definition of priorities regarding controls to be applied according to the identified risk levels (PSR®). Since it contains detailed information as to how the controls should be implemented, this report is used as a plan for operating actions. The controls are presented according to risk level: the first controls in the reports are those which are most important and need highest priority for implementation.

All the reports made available by Risk Manager, including the RAR and the ROR, can be generated using filters. The Project filter can be used to view the results of a specific Assessment Project; the Scope filter displays the risks of one or more Perimeters analyzed in several Assessment Projects. The Business Component filter is particularly useful for communication of risks

associated with a given Business or System Process. The latter is extremely useful in obtaining support from the organization's higher management, since this filter allows risk to be communicated by linking the risks associated with the Company's assets to the organization's business.

Other filters can be used, making it possible, for example, to generate an ROR for a specific technology (for instance, in order to design an action plan for corporate databases), or to address only certain risk levels to be treated.

Tables: customized for any need

Although the RAR and the ROR are highly detailed, the need to produce more specialized reports may arise. Using the Tables available through the **Reports > Tables** menu, customized reports can be generated with information and guidance requested by the user.

The option to customize columns can be accessed through the icon **Customize Columns**. When this option is selected, the box **Field Selection** is displayed, and it is possible to build a table with the desired fields using the click and drag function. Another advantage of this table is that it the controls can be ordered according to any of the information displayed. Each of the tables available on the system is ordered by a specific column. When one of the other columns is moved to the top (the PSR column, for example) and positioned above the one heading the original order, a new order is created for the table. Other forms of customization and ordering can be obtained using the different Tables featured by the system, where information is available for composing columns that can be customized to build specific tables for different needs.

Risk Scorecard, Integrated View of Business Components and Geo-Referenced View of Risks

Risk Manager now offers three reports which are capable of expanding even more the range of resources used by CSOs in their Risk Communication activities.

- **Risk Scorecard:** Scorecards make it possible to produce an integrated, one-page display of the main risk indicators obtained by the Risk Assessments. Because it is a summarized report, it provides an excellent option to use when approaching the higher management. Risk indexes allow definition of strategic targets for the organization, in much the same way that the Top 10 tables show the main assets, business components, systems etc. that require more attention, precisely because they contribute more significantly to the corporate risks.

Use the menu **Administration > System Configuration > Scorecard** to configure the report containing the information the organization considers important to disclose.

- **Integrated View of Business Components:** This report was developed to make it easy to identify the relationship between the corporate assets and the business components they support. This relationship provides invaluable support in correctly defining the relevance of each asset and in prioritizing investments. The Integrated View of Business Components report makes

it possible to graphically view the risk indicators associated with each of the Business and System Processes. The risks associated with each of these elements are calculated based on the assessments conducted on the corresponding infrastructure.

Because it is a report containing a large number of visual attributes, it is widely employed in executive presentations to provide a clear view of the importance of each of the assets to the organization's business processes.

- **Geo-Referenced View of the Risks:** this feature makes it possible to view the risk indicators (Security Index, Risk Index, Compliance Index or Non-Compliance Index) regarding geographically dispersed organizational units. Using Google Earth (which can be installed at zero cost by any organization), the results of the analyses can be seen from a geographic standpoint, whether locally, state-wide, country-wide or internationally. In this way, the distribution of risks is displayed using a graphic and interactive approach, which eases even more the definition of priorities according to the distribution of risks in each of the units or regions where the organization operates.

The "Add Placemark" feature in Google Earth can be used to obtain the latitude and longitude values for each of the perimeters to be represented in a geo-referenced way. When the marker is positioned on the selected location, the properties window informs the corresponding latitude and longitude values, which can be copied and pasted on the properties of the perimeter in Risk Manager.