

Practical Cases in Risk Management

Twenty uses for Risk Manager

by Rafael Roseira Barbosa - June, 2006

Risk Manager offers a set of resources that can be used to meet different needs associated with compliance, information security management, assessment of legal risks, and audits. In order to instruct users on how to get the most of Risk Manager, we have prepared this "Twenty Uses for Risk Manager" guide.

COMPLIANCE

1- Roadmap for Gap Analysis, Compliance and ISO 27001 Certification

With the help of checklists ISO 17799:2005 and ISO 27001:2006, organizations can conduct assessments based on the new ISO 27001 standard. The application also provides a single repository for storing control evidence, and capabilities for following up on the certification process and demonstrating compliance with requirements during the audit.

2- Assessment Automation

Using Risk Manager's Checklist Editing module, it is possible to automate several assessment-related activities, such as inclusion of specific checklists to Risk Manager, remote analyses using questionnaires, and automatic, hassle-free generation of reports.

3- Compliance with SOX

Checklists ISO 17799:2005, Data and System Backup, System Continuity Management, Operational Applications and strategic view regarding compliance with Cobit 4.0 processes can be used to support compliance with SOX.

4- Self-Assessment concerning Internal Security Area Practices (ISO 17799)

Regular self-assessments can be conducted using the ISO 17799:2005 checklist to measure the organization's level of conformity with the standard. By implementing the controls mentioned in this checklist, the existing gap regarding proper management of information security is greatly reduced.

INFORMATION SECURITY PROJECTS

5- Asset Mapping

Risk Manager can be used as a database for asset-related information, such as the assets' owners, their particular relevance to the organization's business, their relationship with business components, how often they are analyzed, and, for assets of the *people* type, the corresponding email addresses.

6- Risk Assessment in Information Security

Using Risk Manager's knowledge base, it is possible to conduct risk assessments for an extensive

number of assets, including continuous management of risks by means of a permanent analysis and control implementation process.

7- Support to PCN Projects

Risk Manager allows users to identify assets and business processes that are critical to the organization, thus making it easy to define both the scope and the continuity strategy for the several different plans within the PCN methodology.

8- Basis for Awareness Campaigns

It is possible to conduct assessments of risks associated with people in such a way that a large number of collaborators is reached. These assessments create risk indexes and help define aspects to be addressed during awareness campaigns. The Web Interview feature allows users to collect evidence using questionnaires, therefore reducing the operating costs involved.

9- Assessment of Risks Related to Suppliers: SLA (Security Level Agreement)

Use of tools such as Web Questionnaire and Risk Manager Offline enables analyses of technologies, people, processes, and environments within supplier and service providing companies. Reports can be easily generated, as well as other indexes regarding all of the suppliers analyzed, grouped by supplier based on specific criteria.

10- Creation of Indexes - Security Scorecards

It is possible to automatically generate customized scorecards and display indexes to demonstrate the results of the analyses conducted. Metrics and criteria can be defined and used to monitor the evolution of risks and guide the implementation of controls.

11- Creation of Security Baselines

The extensive knowledge base offered by Risk Manager allows users to create security standards for a number of corporate assets, such as workstations, hardening of servers, employee training and contract templates.

12- Application Assessment

The Developed Application Systems and the Maintenance checklists are based on the international standard, ISO 15408, providing organizations with the worldwide best practice standards in systems development.

13- Risk Assessments in Datacenters

The Datacenter checklist addresses concerns regarding temperature control, electric network, access controls, and incident control, as well as other topics. It is also possible to attach photographs to provide evidence of the assessments conducted.

14- Transfer of Technical Knowledge

After checklists have been disseminated through the organization, analysts in different areas will have an extensive knowledge base containing detailed and up-to-date information on information security.

ASSESSMENT OF LEGAL RISKS

15 - Revision of Contracts and Agreements with Service Providers

The Contracts with Service Providers and Third Parties checklist, which contains a set of controls

involving best practices and detailed clauses involving different aspects of information security, is remarkably helpful to lawyers and specialists in the Contracts area with regard to information security.

16- Legal Support to Electronic Monitoring

The Electronic Monitoring and Privacy checklist provides controls on actions to be implemented in the corporate environment so that monitoring procedures are conducted according to the applicable legislation.

17- Administrators' Legal Risks

Legal checklists are available specifically to prevent problems regarding civil liabilities of administrators, including the Board of Directors and the Chief Security Officer.

AUDITING

18- Repository of Evidence for Audits

In the course of an assessment, evidence can be added to each of the controls investigated. Evidence produced by means of interviews, questionnaires, automatic collection or importing of digital files such as documents, images or photographs, is stored in a single repository.

19- Security and Information Flow

Using the Information Flow checklist, risk assessments associated with the classification of information can be conducted in the scope of a workflow. Issues such as labeling, responsibility, and disposal of information are addressed in this checklist.

PARTNERSHIPS

20- Security Provider

Módulo's Security Provider Program forms partnerships and enables organizations to add information security to their portfolios. Partnership agreements make it possible for Risk Manager to be used in services rendered in the fields of risk management and information security.