powered by network integration & solutions

RiS risk integrated service

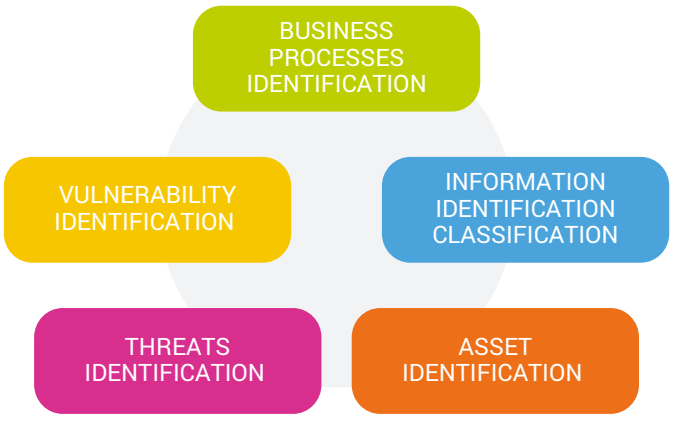
Nowadays defining a framework for the assessment, evaluation and management of risk according to standards and guidelines is the major challenge in IT governance and security compliance. Thus legal and regulation compliance lead to the definition and development of a Security Management System as part of business operations.
Owing to the complexity of planning and operating a Management System, a formal and comprehensive approach to IT Risk Management is the basis on which to build a successful organization.

RiS - RISK INTEGRATED SERVICE

is a web based solution, implementing the NIS methodology in accordance with ISO 31000, developed to help security consultants assess, evaluate and manage risks related to assets, threats and vulnerabilities.
Information gathered from operational sites belonging to the scope drives to the risk assessment application. Integration of information about business relevance, security criticality and real scope for the organization provide guidelines to define acceptable risks, risk scenarios (against threats and vulnerabilities) and produce quantitative results for reports.
The RiS application can thus result in management reviews and treatment plans definition including activities (controls) aimed at mitigating the risks identified.

Our Tool runs risk analysis with respect to either any standard specification family, such as ISO/IEC 27002, COBIT5, SOX, Cloud and so on, or customized ones (Business continuity in specific market sector) to evaluate a risk.

Information and asset classification reflect the importance given them by the management: consequently a direct dependence between risk analysis results and security targets set in policies can be measured. The correct identification of vulnerabilities and threats that can exploit them is the basis for the risk calculation.
Our risk assessment approach is applied to all assets involved in the enterprise, with particular reference to information, technological and infrastructural assets, as well as human resources related to service delivery.



RISK MANAGEMENT AS A SERVICE

The service web access allows to perform risk analysis without any infrastructure or software in house. A constant updating of asset classes, threats and vulnerabilities makes the analysis always up to date to the recent news in the security environments.

CMDB · ASSET INVENTORY · THREATS · VULNERABILITIES · REPORTS CHARTS · RISK ANALYSIS · WHAT-IF SCENARIO · TREATMENT

Organization security model

The tool provides a way to define a security business model that allows organizations to undertake intelligent decisions that minimize risk by:

- Reducing breaches and maximizing security
- Identifying and allocating security roles and responsibilities
- Consolidating and sharing security know-how
- Providing independent access to any actor taking part to the risk analysis process

Scope Definition

It helps to understand and define the scope of the analysis, identifying the perimeter within which the security issues must be evaluated, determining:

- The relevant processes, information and supporting assets for the organization
- Their inter-relationships and their critical value from different point of views (confidentiality, availability, integrity, monetary value, others…)

CMDB Integration

RiS can implement adapters to connect to external CMDB tools to have assets tied to configuration items attributes, as well as use the embedded CMDB feature.

Asset Definition

Threat Identification

Through a template of predefined threats, specific to the organization environment, makes easy to identify which are the most significant threats insisting on the perimeter of analysis

- Determining the threats to which those assets are exposed and their probability of occurrence
- Inheriting threats through the class of belonging of company assets

Risk Estimation

It provides a risk estimation to identify assets and processes that need to be investigated and treated

- Identifying asset and processes over Risk Appetite, seen as the level of risk that an organization is prepared to accept, before action is deemed necessary to reduce it
- Identifying risk situations global to a system or a company branch

Vulnerabilities Identification

Through a template of predefined vulnerabilities, specific to the organization environment, makes easy to identify which are the most significant vulnerabilities that can be exploited by the threats in the perimeter of analysis

- Determining the vulnerabilities level and how they can be exploited by the threats, through a Control Analysis with respect to the Regulatory Standard
- Making the vulnerabilities stand out from personalized and customized interviews

Risk Analysis

The tool has a wide range of analysis methods to identify the main risks and analyze the causes to undertake the best and most effective countermeasures

- Identifying, assessing and prioritizing risks (ISO 31000 definition)
- Analyzing the origin of the risk

Risk Management contribution

Besides the risk analysis, it is possible to get suggestions, hints, opportunities to identify the best actions to plan an effective Treatment Plan, minimizing cost impacts:

- Receiving recommendations on most effective controls to implement
- Providing What-If scenarios to address countermeasures and investments

What-if Scenario

What-if scenarios simulate the behaviour of the organizational environment after applying a treatment plan.

The feature suggests to management the best domains in which to invest after providing a comparison between the actual risk profile and the hypothetical one associated to the what-if scenario.

Continuous monitoring and review

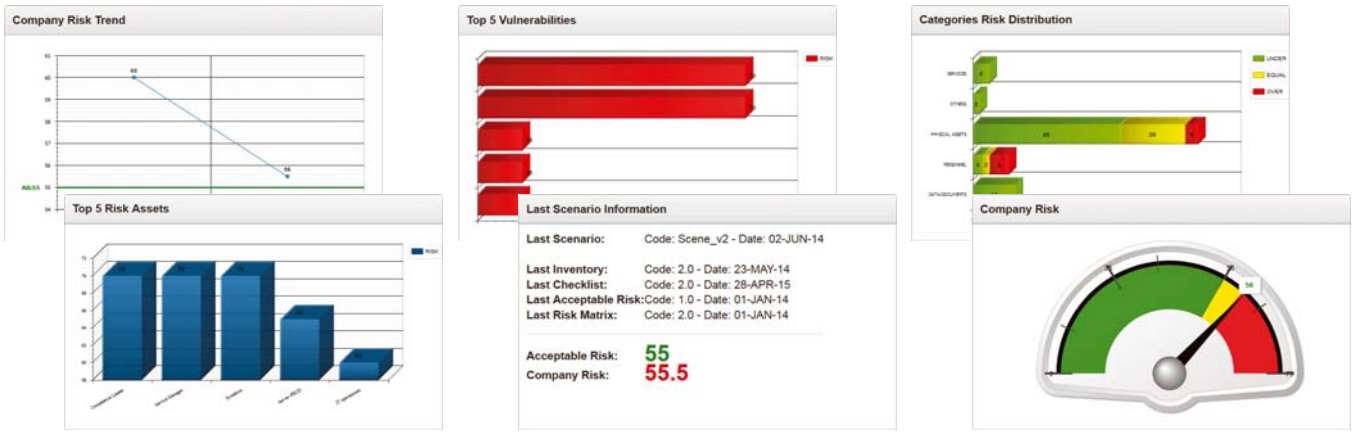
In accordance with the process-based model, the tool allows a continuous improvement process of the Information Security Management System

- Comparing assets and processes in different scenarios
- Making repeatable and comparable analysis in the course of time

Results documentation

A wide range of results lets the organization to understand the actual situation providing many keys to read and analyze the risk profile

- Reports and Charts
- Documentation available in CSV and PDF format
- Documentation archive to track project activities



Integrated and holistic approach to Risk analysis

Risk analysis can be performed with respect to different standards and regulations:

- ISO 27001:2005 - Information Security Management System
- ISO 27001:2013 - Information Security Management System (ISO27005 compliant)
- ISO 20000:2011 - IT Service Management
- ISO 22301:2012 - Business Continuity
- Cloud Security - Consumer Side

INNOVATION
FUTURE FEATURES

COST/BENEFIT ANALYSIS

Cost benefits analysis allows to evaluate the cost of a remediation vs the cost of a potential loss of an asset: this is an extraordinary support to drive investments and management decisions in the company's strategies.

IMPROVEMENT OF DATA SOURCE RELIABILITY

Gathering and correlating data generated by multiple systems/devices (ex. Vulnerability assessment tools, penetration testing tools, network analysis tool, threat detenction tool, etc.), the risk evaluation process can be improved in terms of data source reliability: in fact, integrating data obtained from checklists/interviews with data generated by IT systems it is possible to have a picture closer to reality.

SECURITY RISK MODELING

The state-of-art provides new models that can be studied and adopted to introduce new functionalities into traditional risk assessment algorithms (for example identification of causal relationships among risk factors, complexity of vulnerability propagation, etc.). Examples are soft computing methods and attack trees, used to model the threats against a system and graphical represent how attacks might succeed and which attacks are most likely to succeed.

REAL-TIME RISK ANALYSIS

Given the dynamic nature of both IT and the threat landscape, it becomes more and more important to be able to assess and mitigate the risks in real-time. The tool may be improved by making it dynamic, continuously adapted to new ways of managing risk to keep up with the ever evolving threat and vulnerability landscape. It will be able to correlate ever changing information (asset changes, vulnerability assessments, new threats, etc.) and immediately report on new types or levels of risks. This ensures that the way in which you prioritize remediation decisions is reflective of real threats, timely and effective.

SECTOR-SPECIFIC ANALYSIS

Methodologies for risk assessment and information security standards differ between industries and market sectors (ex. banking, healthcare, energy, transportation, etc.).
The risk assessment tool may be improved to meet sector-specific requirements of different industries, in compliance with their own standards.

RIS risk integrated service powered by NIS network integration & solutions

GENOA MILAN TURIN ROME LONDON

Main Office: Via al Porto Antico 7 - 16128 GENOA - Phone +39 010 5954946 - Fax +39 010 8680159 More info: ris@nispro.it