Product Introduction

CARISMA

Corporate Risk Management System

Version 1.0

2008

TABLE OF CONTENTS

1. General introduction to CARISMA program family

CARISMA is a **C**orpor**A**te **RIS**k **MA**nagement System. The system supports risk management both in the field of *information technology systems* and *business systems* starting with exploring operational risks throughout the definition of qualitative and quantitative risk values, preparation of corporate risk map, preparation, storage and handling of linked protection measures, action plans and regulations, and also the management and complete monitoring of prospective risk events.

The functionality of CARISMA is based on the measures of Security Management Methodology (SMM®) that, in the field of IT processes, stands the recommendation and standards of Cobit3 (ISACA), BS 7799 (ISO 17799), TCSEC and the Common Evaluation Methodology which is the part of CC (ISO 15408) standard, and in the field of business processes it meets the MABISZ (Association of Hungarian Insurance Companies) standards. SMM® is the result of the development of the last seven years, it has been applied successfully for different security, qualification and system organization tasks at more than 150 national and international security system organization projects.

The system is able to provide the risk management of companies or organization units of concerns and the creation and support of handling of linked regulatory documents, so the first step is the definition of the organizational and dependency relations of the company or concerns. Then, after identifying the risk areas of each organization unit (company), the corporate risks are defined by organization units and business processes with the help of the knowledge base containing the typical national risk sources.

The other usage of the knowledge base is the corporate protection measures created for reducing risk and the qualification of their impacts based on the industry averages. The system defines the qualitative and quantitative risk values based on the corporate risks and the qualification of risk measures. This way the operation model of the complete company is mapped on a risk map that could be pictured both with quantitative and qualitative methods.

Based on the security maps the protection strategies, the disaster plans, the actions reducing or preventing risks could be defined. Thereby a common security system evolves regarding the risk management processes, tools and regulations of the company.

The system generates projects from the operating regulations and disaster plans reducing operating risk and from the protection actions of business continuity plans. The report-generating module displays these projects for the decision makers in an order prioritized according to a ROSI (Return on Security Investment) model and pictured graphically.

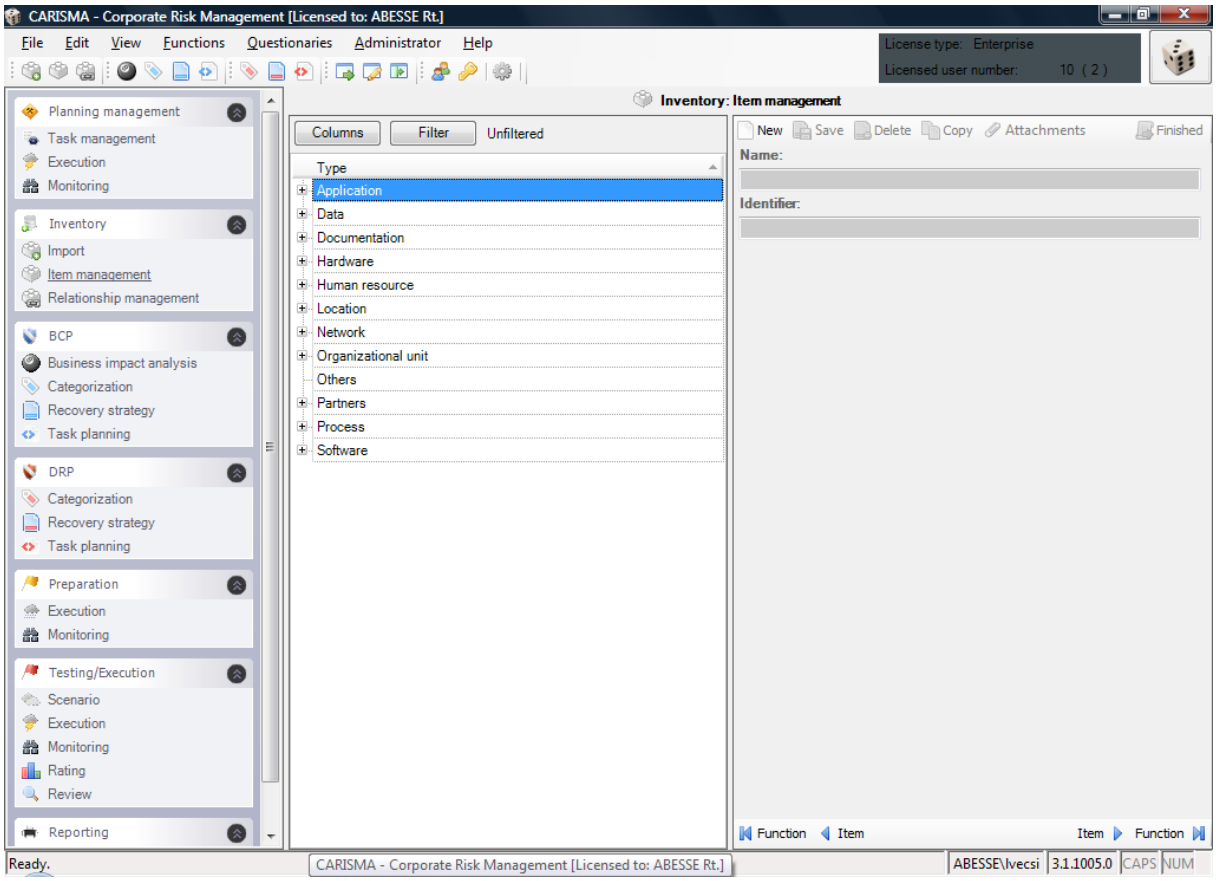
Connected to external systems the company could follow the changes of their risk values on-line and they can make decisions about taking them on, and about the consequences of its reduction. At present the connection is solved and tested with the most common system management softwares as HP Openview, IBM Tivoli, CA Unicenter, Microsoft System Center family etc, and with process management tools as ARIS (cARISma consolidated risk and regulatory management framework designed by ABESSE and IDS Scheer Hungary) and ViFlow.

Using the program family provides support for the users in not only making static documents, but in possessing an organic, continuously refreshable document system. The functions of the program package offer possibility to adapt the created documents to the company's continuously changing organization structure and to its altering business procedures.

The CARISMA program family helps

- the identification of qualitative an quantitative risks of corporate business procedures,
- the preparation of corporate risk map,
- the security qualification of processes, resources and with its knowledge base, comparison by industry,
- the development of security measures and the continuous monitoring of their impacts (regulations, disaster plan, business continuity plan, action plans),
- in presenting the overall picture of risk management methods and tools,

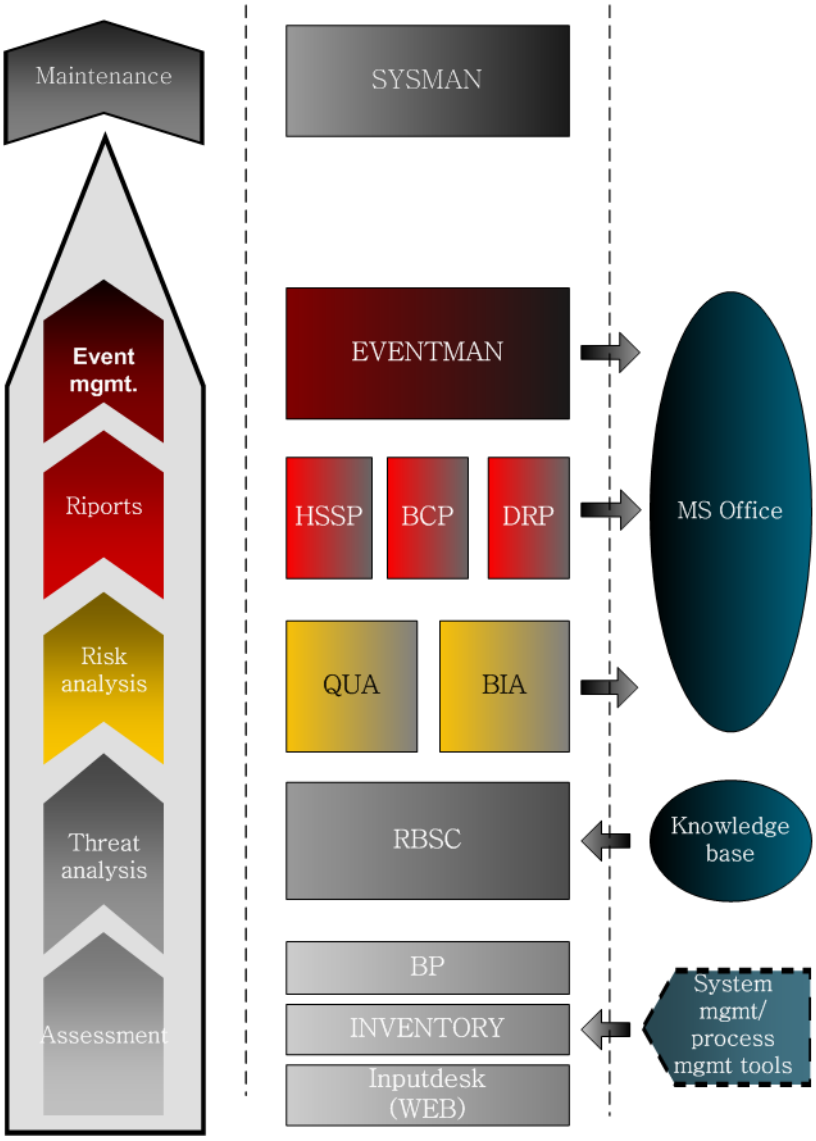
- the management of occurring events, disasters.



2. The structure of CARISMA

The structure of CARISMA is illustrated in the figure below.

The left side of the figure illustrates the complete process and each phase of corporate risk management. The column in the middle contains the functional structures of CARISMA supporting each step of the process, and the integrated data connections and the output data formats can be found in the right side column.



The structure of CARISMA system

The explanation of CARISMA functions and data connections:

- **INPUT-DESK** – Questionnaire generating and data summarizing function;
- **BP** (*Business Process*) – Business Process assessing and registering function;
- **INVENTORY** – Corporate resources registering function;
- **RBSC** (*Risk Base Score Card*) – Risk sources and controls estimating and evaluating function;
- **QUA** (*Qualitative, Quantitative*) –Function calculating risk value of risk sources;
- **BIA** (*Business Impact Analysis*) – Function analyzing business impact;
- **HSSP** (*Homogenous Security System Planning*) – Function preparing security map and classifying security systems;
- **BCP** (*Business Continuity Planning*) – function preparing and maintaining business continuity plans;
- **DRP** (*Disaster Recovery Planning*) – function preparing and maintaining the disaster recovery plan of resources;
- **SYSMAN** – System data base, user and network management function, journalizing, license handling;
- **Knowledge base** – the experience of more than 150 Hungarian projects of Insurance Technology (applying international methodologies), the knowledge base includes the typical Hungarian risk sources and the linked controls;
- **System mgmt/process mgmt tools** – system management softwares like HP Open View, Microsoft SCOM etc. that provides the continuous monitoring and administrating of the IT infrastructure and following their changes. Process management tools like ARIS, ViFlow, Mega etc.

2.1. The functionality of CARISMA

There is a tight connection on professional and methodology level between the certain elements of the functionality, but aligning with user needs, the possibility is given for providing unique and narrowed service levels also. This way the CARISMA RISKMAN, CARISMA BCP, CARISMA DRP modules could be bought separately, which supports the preparation and monitoring of documents and providing the functions only defined particularly by the customer.

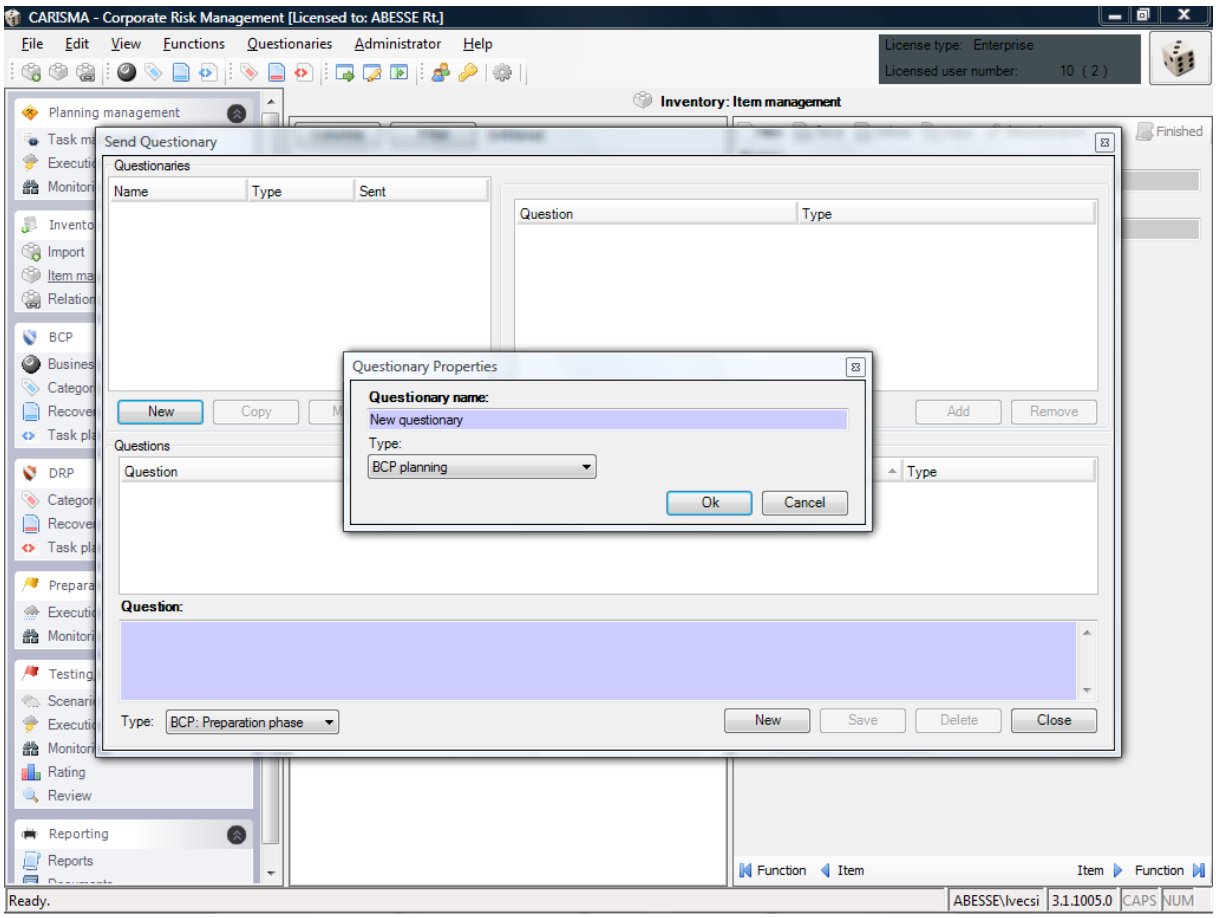
However, proceeding from the narrowed service, the function level connection permits that a company thinking in complex risk management could expand the services of CARISMA modules efficiently to every part of risk management.

2.1.1. INPUT-DESK (Questionnaire generation and data summary)

INPUT-DESK is a web based assessment generator and data summarizing function. The basic need of the status measuring is that only actual data should be entered into our system. Furthermore, the data could come in interview minutes, in filled in questionnaires, and as complements of external tools (software) and databases. INPUT-DESK provides support for each case:

- Based in the interviews a minute could be prepared that could be sent to the interviewed person and after the approval it could be saved permanently into the database,
- For measuring the status and for collecting new data or checking existing ones questionnaires could be created with INPUT-DESK function. These could be available and filled in by the responsible experts via the company's intranet,
- Pulling data from existing databases,
- the HP Openview application sends the description and data of the tools and resources connected to the network in data file format.

The colleague responsible for operating CARISMA could measure the accuracy and usability of the data, and after checking them he could add them to the system. With this step the collected information turns into real input data.



2.1.2. BP (Business Process assessing and registering function)

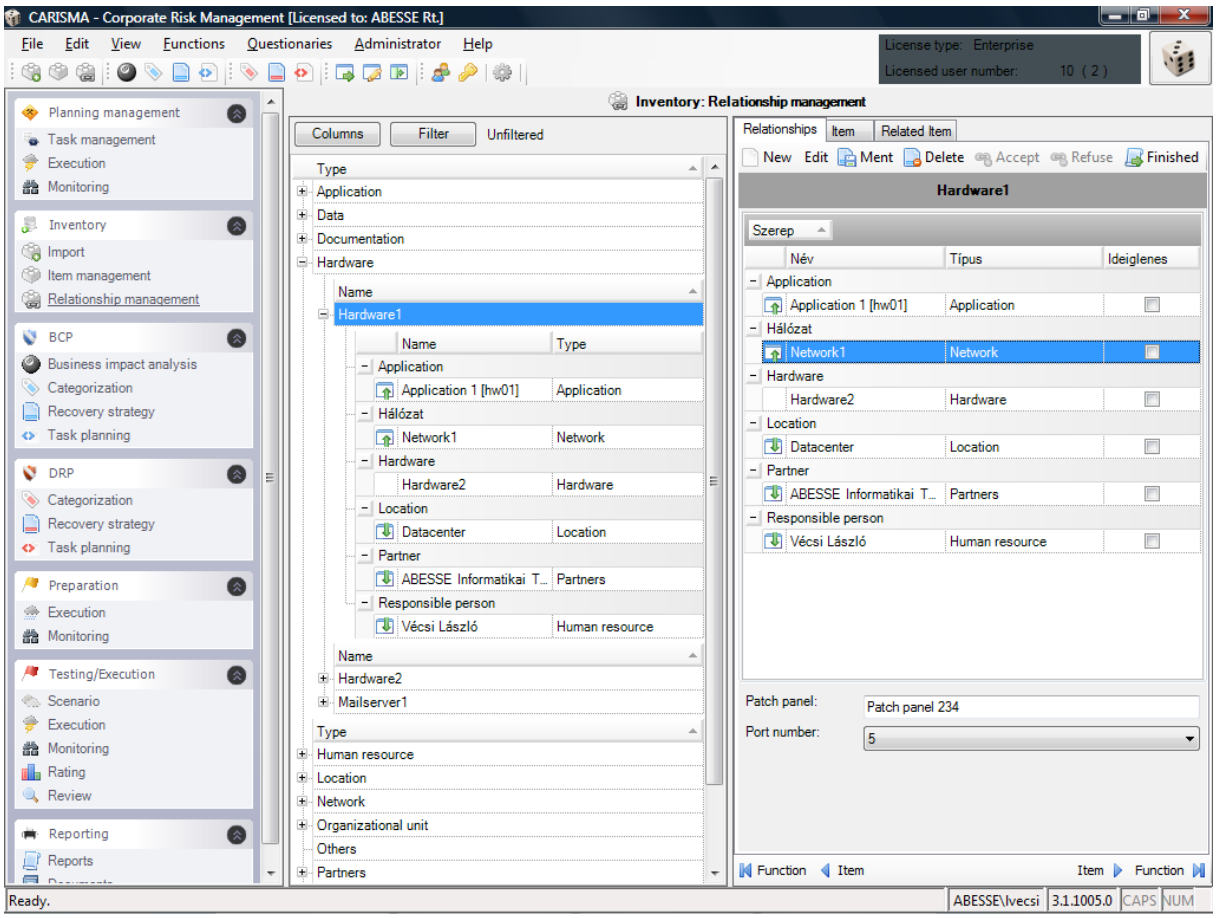
BP function is for estimating and registering corporate business processes. It provides the possibility for defining the relationship between the adopted processes and their resources, for adopting process-process and process-resource dependence (resources are matched to processes from the INVENTORY function).

2.1.3. Inventory (asset registering function)

INVENTORY function is basically a tool registration. With the help of INVENTORY it is possible to register the hardware, software and application units installed at the company and handle the their changes.

With the help of its interfaces INVENTORY is able to obtain data from other, already existing systems, databases via the INPUT-DESK function: As a result of this, the consistency between the database of CARISMA and the company's other tool databases could be sustained continuously.

CARISMA has a data exchange function integrated with HP Openview software, so the INVENTORY function is adaptable for following the changes in the customer's tools in the network even on-line.



2.1.4. RBSC (Risk Base Score Card – evaluating risk sources and controls)

The risk sources are matched to the resources picked during status analysis by the RBSC (*Risk Base Scorecard*) function. As a self-control or professional supporting the list of typical risk sources are available in the continuously updated KNOWLEDGE-BASE.

An other main task of the function is that we compare the controls applied in connection with the risk sources with the controls located in the KNOWLEDGE-BASE in a way that we weight and qualify them at the same time.

RBSC potentiates overall qualification of risk sources and controls. The KNOWLEDGE-BASE supports the comparison of the survey results to standard databases and the benchmarking with companies in similar profile.

2.1.5. QUA (Qualitative, Quantitative – Risk value calculation of risk sources)

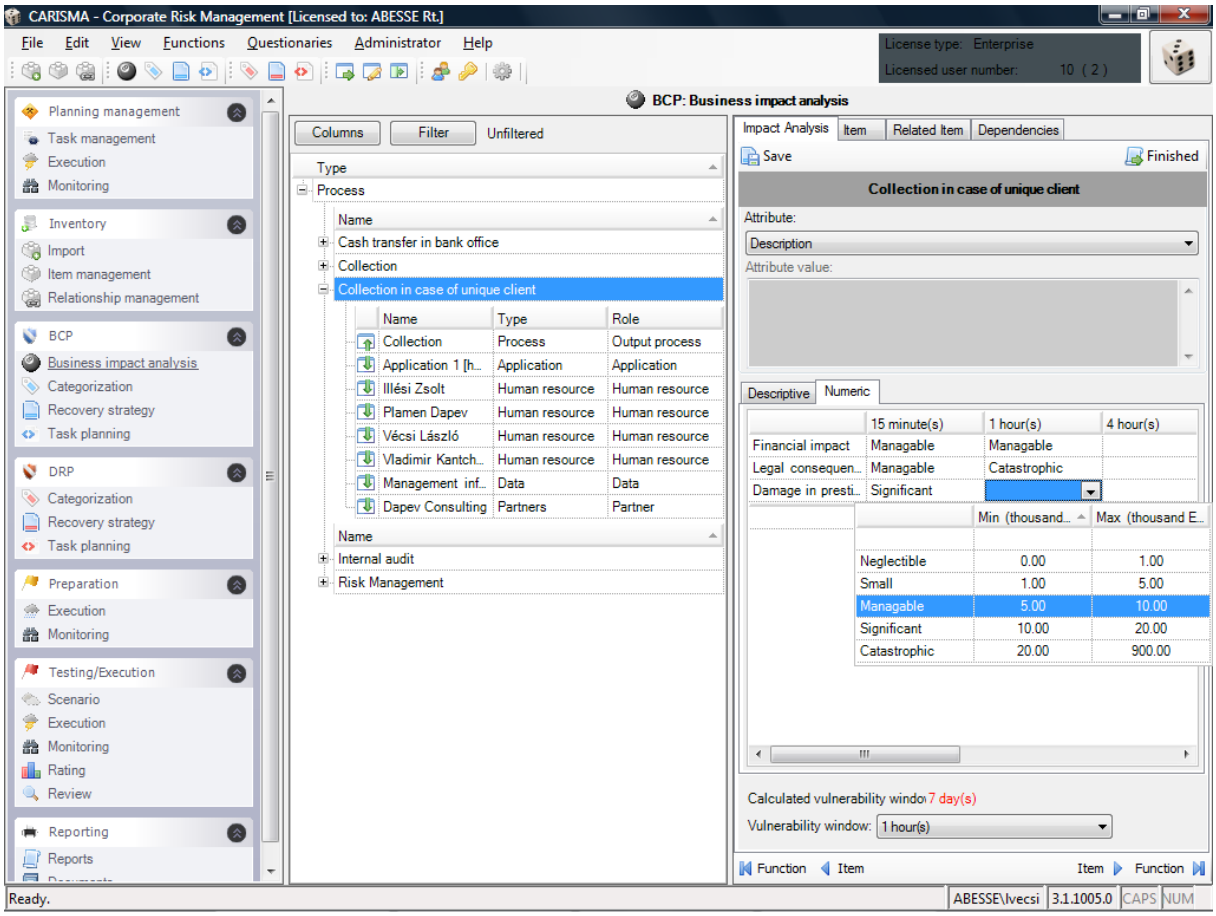
One of the risk analysis method offered by the system is the QUA function that calculates the risk value of the risk sources defined in the RBSC function.

The calculation is based on the control qualification made by RBSC function, the size of the expected damage, and the supervening probability of risk sources. The QUA function calculates the risk value from these items. The program is prepared for both qualitative and quantitative calculation. QUA defines the supervening probability of risk sources endangering data according to the Common Evaluation Methodology, which is the part of the CC (ISO 15408) standard.

2.1.6. BIA (Business Impact Analysis – function analyzing the impacts of processes to business)

An other risk analysis method of CARISMA is the so-called BIA function (*Business Impact Analysis*), that does the impact analysis of business processes for the business continuity planning and for the disaster recovery planning.

Business impact analysis is the inspection of how the attributes added to each process (priority, description, impact elements) and the processes build on each other. The function supports the printing of the status analysis and the risk analysis reports.

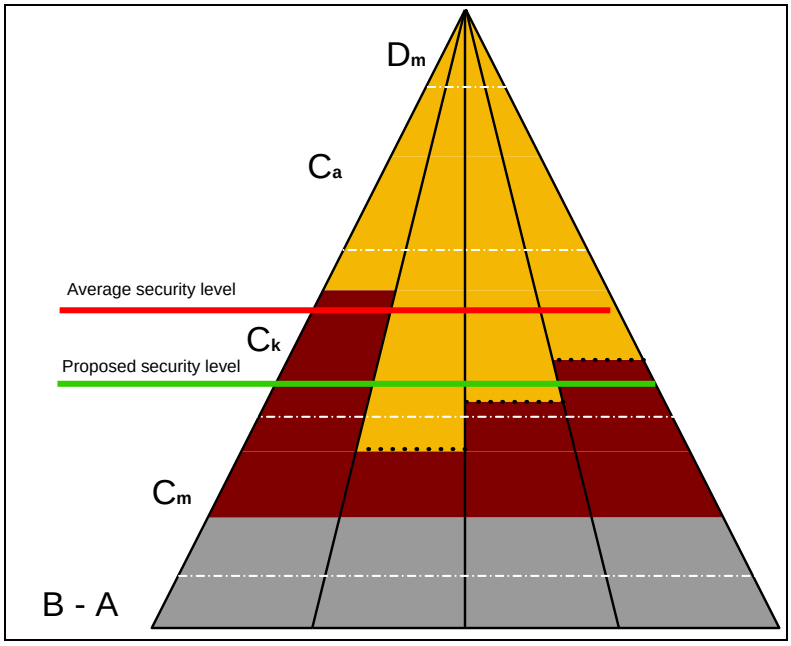


2.1.7. HSSP (Homogenous Security System Planning)

The HSSP function *(Homogenous Security System Planning)* draws the security map of the company in each field of security system organizing – organizing, physical, logical, network, life cycle security - based on the risk values of risk sources. According to the set parameters it does the classification to security classes by fields.

The suggested security class defines the security measures that are necessary to reach the next protection level, i.e. that the company should carry out.

The next picture shows the correlations handled by HSSP:



Correlations handles by HSSP

HSSP supports making those type of decisions, that are about the investments that a company should make in each field to reach the required security level. The program does the definition of the order and priority of the investments based on the impact correlation number, the so called ROSI model (*Return on Security Investment*).

2.1.8. BCP (Business Continuity Planning)

Based on the collected data (business processes, resources, risk sources, controls, etc.) with the BCP function the measures and action plans could be worked out to the critical business processes. The function provides support for the preparation and refreshment of the business continuity plan documents. It automatically generates the actual version of the plan, provides help in the realization of consistent planning and in working out efficient measures.

2.1.9. DRP (Disaster Recovery Planning)

Similarly to BCP, DRP does the preparation, actualizing and continuous maintenance of IT disaster recovery plan. DRP focuses on the IT support systems and resources (of course in a consistent way with BCP and BIA). It supports also building background IT strategies. In the function arbitrary objects could be picked (graphics, pictures, descriptions) that completes the process and tool descriptions with special data (topography, network connection system, cluster builds, etc). DRP function has a disaster recovery plan printing function that is built on the complete, actual database.

2.1.10. EVENTMAN (Testing reports, monitoring execution, handling events)

2.1.10.1. Testing

The process of testing is supported by the patterns and extracts built in the software. During testing we actually model the "event" (disaster) itself. With the software events could be modeled in different size, coverage, and impact. After setting the parameters of the event (type, effect, importance, etc.) the software leads the testers through the each step of the action plans of the answer, reset and recovery phases.

At testing we could organize the steps of the action plans by resource, responsible or process. This way a responsible person doing a task could be tested just like all the responsible people of a complete process. The results of the test are connected to each other in a matrix like the resource

and process structures. During testing the time frame of reset and recovery could be monitored continuously and could be compared to the vulnerability window of the processes in threat (maximum acceptable drop out time). With forms defined in advance a test diary could be generated form the complete process of testing.

2.1.10.2. Training

Similarly to testing, training is worked out with the concentrated and structured collection of adequate information (stored in a decentralized way). The tasks and responsibilities of users and people in charge could be collected and reproduced in a form of training material.

2.1.10.3. Tracking changes in reports

In case if the modification results in a change that could not be handled automatically (e.g. as an effect of a modified risk value, a process becomes critical and an action plan has to be worked out for it), the software leads along the user systematically in the fields and tables to be filled in.

2.1.10.4. Handling events

We consider as an event every occurrence that is different from normal business procedure. Event handling itself is similar to testing (as during testing we try to model the event as life-like as possible). Structuring the action plans arbitrarily helps preventing damage and the reset and recovery as fast as possible. Of course the more up-to-date the data in the system is, the more we can reduce the reset and recovery timeframe and the secondary damage consequence itself. (The secondary damage consequence includes the indirect, propagating impacts of the disaster. These effects grow exponentially as time passes.) The software supports forming disaster teams (according to tasks and sphere of operation).

2.1.11. SYSMAN (System database, user and network management function)

The authorization system of CARISMA permits the forming of user groups with freely chosen parameters and the adding individual users. This way the security of sensitive data in connection with the operation and IT of the company can be assured. The administrative functions provides the possibility to choose parameters for certain entering formats, drawing, workflow and printing outputs.

Besides user administration the diary settings are done assured by the SYSMAN function, and we can save statuses here as well (in order to be able to track history).

3. References

CARISMA Corporate Risk Management System has been implemented at the following companies:

- Aegon Hungary Insurance Ltd.
- Pannon Hungarian Telecom Ltd.
- Giro Bank Card Ltd.
- Malév Hungarian Airlines Ltd.
- T-Online Ltd. (member of T-Com group)
- Budapest Waterworks Ltd.
- Budapest Airport Ltd.
- Unicredit Mortgage Bank Ltd.
- MOL Hungarian Oil and Gas Plc.
- ERSTE Bank Hungary Plc.
- OTP Bank Plc.
- OTP Savings Ltd.
- FHB Mortgage and Commercial Bank Plc.
- CIB Bank Ltd.
- CIB Leasing Ltd.
- Hungarian Development Bank Plc.
- Summit Car Finance Ltd.
- Prime Ministers Office
- Netlock Ltd.