



# **ORC** ..... Operational Risk Center

Standard software  
for managing operational risks



### **The Relevance of Operational Risks**

Operational risks, i.e. the risk of losses arising from business operations (e.g. system downtime, fraud etc.) as well as external sources (e.g. terrorist attacks, natural disasters, hackers etc.) are becoming more and more important for financial institutions and other businesses. Cases of devastating damages like Barings Bank, Allied Irish Bank, or Enron were, for the most part, made possible by operational risks. The increasing complexity of operational procedures, higher dependency on IT-systems, global company networks, and the increasing number and complexity of products and services incorporate an enormous risk potential.

Supervising authorities have become aware of this development at an international level and have acted accordingly. With its law for control and transparency in businesses (KonTraG), the German government requires corporations to install and maintain an adequate risk management system. With the "International Convergence of Capital Measurement and Capital Standards" paper (aka Basel II), the Bank for International Settlement (BIS) has outlined the importance of operational risks, enforcing the international awareness. Basel II requires not only market and credit risks, but also operational risks to be controlled and sufficiently covered by a bank's net assets. In Germany, these guidelines have already been transformed into national law by the minimum requirements for risk management (MaRisk) and solvency regulation (SolV). Furthermore managing operational risks has also demonstrated a remarkable impact on the bank's rating. International rating agencies like Moody's etc. ask rating candidates more and more about the management of op-

erational risks. The proof of a well established framework for managing operational risks is becoming a considerable requirement for a good rating.

### **Benefits of an Operational Risk Management System**

- Compliance with supervisory guidelines (Basel II etc.)
- More efficient allocation of the company's net assets and capital charge reduction
- Improved rating assignment by external agencies
- Improved risk awareness in all organizational units
- Pro-active handling of operational risks – avoid damages before they occur
- Basis for company control on risk-return aspects
- Process optimization by systematic identification of vulnerabilities resulting in an increased efficiency or cost savings
- Transparent dependencies between IT-systems and business processes

### **Operational Risk Center – The standard solution for controlling and managing operational risks**

ORC is a joint project from interexa AG and VÖB-Service GmbH, an affiliated company of the German Federal Association of Public Sector Banks (VÖB), and was designed as a standard solution based on the demands of numerous members of the VÖB. Within a short time, ORC has become the market leader in Germany and is currently in full use by more than thirty institutes inside and outside Germany. The modular architecture of ORC supports the entire controlling and management process: from risk

# Standard software for managing operational risks

identification and measurement via the analysis up to the reporting, including the initiation and control of preventive measures. The software also offers interfaces for importing legacy data and data export to external systems. User administration, workflow definition and the customizing of data structures, user interfaces, reports and processing rules are, to the greatest extent, administrable without programming knowledge. This allows the client to configure the system according to its operational risk management framework definition.

## Modules

### ORC-RE (Risk event data)

Risk measurement begins with a structured collection of risk events, an important element of the overall regulatory requirements. With the ORC-RE (Risk Events) module, the software offers an effective instrument for the structured collection of loss event data, allowing for user-defined data fields and data capturing rules. Since loss events can occur in any organizational unit, the decentralized data acquisition is an important feature of the ORC system.

Internally collected data is often not sufficient to realistically quantify operational risks. Especially “low frequency, high severity” events are often not appropriately accounted for, as they occur seldom or not at all in the span of time monitored. This problem is solved by adding external data to the database. External loss event information in form of public data or coming from data consortiums (e.g. DakOR) can be incorporated with little effort thanks to the customizable data structure of the loss event database and an effective matching function. If requested, ORC-RE can be delivered preconfigured based on the standards defined by the German Federal Association of Public Sector Banks.

### ORC-RC/RP (Self Assessment)

While the loss event database addresses the past only, capturing data based on actual risk sources and managing losses that have already occurred, self assessments allow for the identification of potential risk sources and possible future losses. Here both quantitative aspects of risk estimation (potential loss amount and probability of the event) as well as a qualitative risk appraisal (judgment on

The screenshot displays the 'Interexpa Risk Inventory - Answer' software interface. The main window is titled 'Risk Inventory - Answer' and features a navigation bar with tabs for 'Losses', 'Risk Inventory', 'Self Assessments', 'Risk Indicators', 'Reporting', and 'Quantification'. Below the navigation bar, there is a 'Query is based upon current date: 05/01/2007 02:18:11 PM' and a 'Main Page' button. The interface is divided into several sections:

- Update record (RP-Assessment):** This section on the left contains a form for updating records. It includes fields for 'Topic' (Information Technology), 'Contact', 'Event', 'Reason', 'Risk Category' (Business disruption and system failures), 'Relevance' (Not relevant), 'Business Unit' (Sales & Marketing (SB)), 'Process' (Online Order Processing), 'Appraisal' (Any down time is an essential risk to business continuity due to the high level of dependency on IT systems), 'Typical Severity' (10,000.00), and 'Typical Frequency' (2).
- Risk Inventory - Answer:** This central section displays a list of risk categories and their associated risks. It includes sections for 'Internal Infrastructure', 'Internal Practices', 'Employees', and 'External Influences'. Each section lists specific risks and their potential impacts.
- Regular Losses:** This section on the right contains a table for 'Regular Losses' and a 'Legend' section. The table has columns for 'T number', 'T Amount', and 'T Potential'. The 'Legend' section defines the risk categories and their corresponding colors.

the quality of business processes and controls in place) can be covered.

ORC supports both forms of expert polling with the modules RC (Risk Check Points) and RP (Risk Profile). Questionnaires asking for expert opinions can be defined, administered and distributed using ORC-RC. Here the user can define question and answer types and distribute the resulting surveys residing inside the system. With the module ORC-RP financial institutions do also have the possibility to capture self assessments resulting from interviews or workshops, thus not requiring a decentralized capturing of the result data, while still having the same powerful functions available as in the modules RE and RC.

*If desired, standard questionnaires from our reference customers can also be provided, building a potential starting point for establishing an operational risk management framework.*

#### **ORC-RI (Risk Indicators)**

An effective risk management should allow for the anticipation of changes to the company's risk profile at an early stage, at best before losses occur. An appropriate early warning system is provided by the integration of risk indicators into the business processes. This way, pro-active action can be taken and their efficiency can be measured based on the changes to the respective indicator levels.

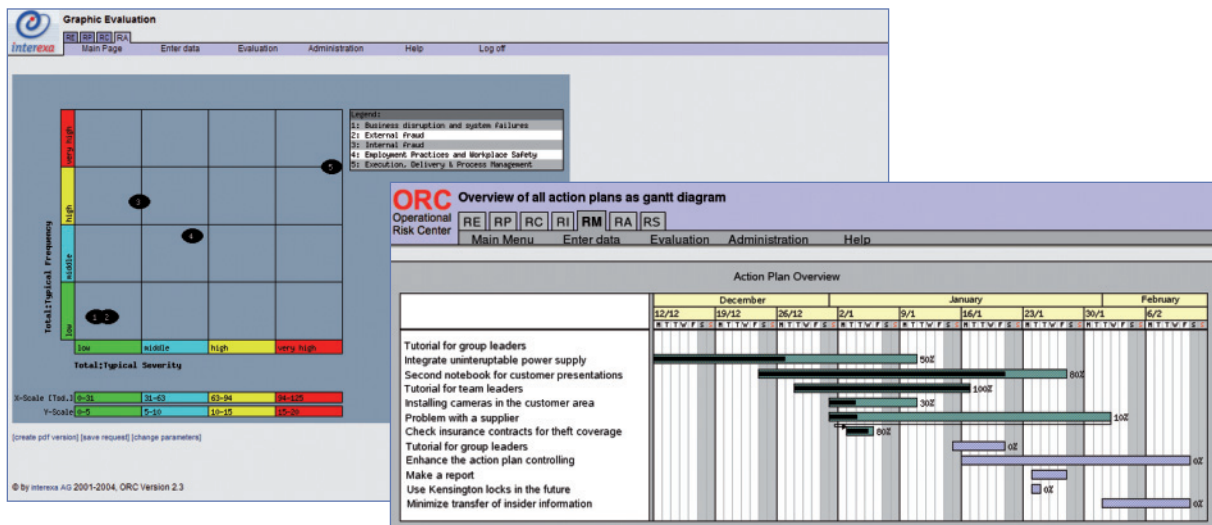
ORC provides this function in the ORC-RI (Risk Indicators) module. Here user-defined indicators and data acquisition workflows can be configured. Furthermore escalation procedures for threshold violations can be specified. Customizable reports brief managers of the bank's current risk on a periodic basis or when exposed to an imminent threat.

#### **ORC-RM (Risk Measures)**

If risk information is delivered in real time upon any event, pro-active measures can be taken before losses occur, potentially fully avoiding them or at least reducing their impact. Once a loss occurred, an analysis of its causes should be performed in order to derive improvement measures avoiding future damages of the same kind. In this context fast communication concerning the measures to be taken as well as monitoring their efficiency is very important. An effective risk management system should support this aspect of operational risk management. Operational Risk Center does so in each of its modules. The user can establish measures to be taken concerning each loss event, self assessment or risk indicator. The communication and monitoring workflow can also be defined. Finally the ORC-RM module offers a complete overview of all measures initiated inside the ORC system and allows for the creation of action plan templates that can be used in any context.

#### **ORC-RS (Risk Quantification)**

The ORC-RS (Risk Simulation) module allows for the calculation of the capital charge using a Monte Carlo Simulation based on actual losses coming from the loss event database and optionally the loss estimates coming from the self assessments. To simulate the severity and frequency of the loss distribution, a variety of distribution functions are available, e.g. Poisson, Binomial, Negative Binomial, Lognormal, Gamma, Weibull, etc. Using a freely definable confidence level, the simulation engine calculates the expected and the unexpected loss as well as the OpVaR (Operational Value-at-Risk). The results can be incorporated into user-defined reports which can be distributed or made accessible to other ORC users.



## ORC-RA (Risk Analysis/Reporting)

Providing the management with the latest and most up-to-date information on the company's risk profile as well as any exceptional losses is a crucial part of a pro-active operational risk management framework. Especially if a company is managed in a risk/return-oriented manner, a realistic assessment of the current risk profile is necessary for the precise appraisal of the input factors. In this context, the ORC-RA (Risk Analysis) module offers a powerful and flexible reporting framework. Here the business departments can freely define and administer standard reports for all management levels, with the data represented in table or graphical form. The creation of reports can be automated using event or time-driven triggers and a notification about new reports can be sent via e-mail. Furthermore users can create their own report definitions and save them for future use. Ad-hoc reports can also be created by users with the appropriate permissions.

## Data Consortium

A realistic estimate of the operational risk profile requires financial institutions

to collect data on loss events occurred in the past. Unfortunately, a prediction of future development based on historical data is difficult, as normally the information available is from the recent years only, i.e. it does not show sufficient historical depth, and extreme events (e.g. natural disasters etc.) are underrepresented (if at all). This problem can be solved by "enriching" internal data with external or consortium information.

External or consortium data also allows for establishing industry benchmarking and deriving best practices. Operational risk management systems must therefore be able to load this kind of data or at best interface to the referring data services directly, and manage the data potentially coming from several external sources as an integrated part of the overall database. Using the ORC technology, the DakOR data consortium for the collection and exchange of operational risk loss data was established in 2006. The VÖB-Service GmbH operates the consortium open to all interested institutions as a trustee. Currently the following financial institutions are registered members of the DakOR data consortium: BayernLB, DZ BANK, Helaba, HSH Nordbank, LBBW, LBB, NORD/LB, Deutsche Postbank



#### Our clients

Aareal Bank  
Bankhaus Wölbern  
Landesbank Berlin  
Bausparkasse Schwäbisch Hall  
BayernLB  
Bremer Landesbank  
CMSS  
dwp bank  
Deutsche Postbank  
DG HYP  
DVB Bank  
DZ BANK  
DZ Bank International  
HSH Nordbank  
Investitionsbank Berlin  
IZB Informatik-Zentrum  
KfW Bankengruppe  
Landesbank Baden-Württemberg  
Landesbank Hessen-Thüringen  
NRW.Bank  
Landesbank Rheinland-Pfalz  
Landwirtschaftliche Rentenbank  
Landesbank Sachsen  
LfA Förderbank Bayern  
Norddeutsche Landesbank  
Norddeutsche Landesbank Luxembourg  
Raiffeisenlandesbank Oberösterreich  
Reisebank  
Sächsische Aufbaubank  
Union Asset Management  
VR Leasing  
Westdeutsche ImmobilienBank  
WestLB

and Sachsen LB. Further information on the DakOR data consortium can be found under <http://www.dakor.org>.

#### Advantages – Why ORC?

- Solutions designed by banks for banks.
- Flexibility – can be adapted to company-specific requirements as well as to industry best practices for operational risk management
- Comfortable user administration
- Flexible, user-defined workflow
- Powerful reporting features
- Multi-client support allows for enterprise-wide use
- Considerable expertise in implementation of operational risk systems through numerous related projects and partnerships with well-known consulting firms.
- Long-term investment security through additional maintenance and development guarantees issued by the VÖB-Service GmbH

#### Technology

Operational Risk Center (ORC) is fully web-based and platform independent. ORC supports all common browsers (e.g.

Microsoft Internet Explorer, Mozilla Firefox etc.), operating systems (e.g. Microsoft Windows, Linux, Unix, Solaris, AIX etc.) and database systems (e.g. Oracle, DB2, Microsoft SQL-Server, MySQL, PostgreSQL, Sybase etc.). The software was developed based on the best practices of several customers. This includes a state-of-the-art three-tier architecture and an object-oriented design. The result is a high performance system that can be used on a desktop as well as in distributed workplace environments.

#### ASP-Operation

For banks having outsourced their IT departments, ORC can be operated as an ASP solution.

#### Demo Version

A demo version of the Operational Risk Center accessible via the internet can be provided on demand.

#### Training

ORC training for administrators as well as for users are regularly held at VÖB-Service, but can also be run in-house.



**interexa**

Contact details:  
Andrés Alvarez  
+ 49 (0) 6131/14 40 728  
E-Mail: [orc@interexa.de](mailto:orc@interexa.de)



Contact details:  
Frank Reiff  
+49 (0) 228/8 19 21 60