“MORE CONTROL - LESS RISK”

IDENTIFYING, ANALYZING AND CONTROLLING ACCESS RISK WITH THE GARANCY ACCESS INTELLIGENCE MANAGER

White Paper

VERSION 1.0
STEFANIE PFAU, THOMAS GROSSE OSTERHUES
CONTENTS

ACCESS RISK SUPPORT FOR ALL PHASES OF RISK MANAGEMENT ................................................................. 3

1. “Focus on What’s Important” – benefits for all target groups ........................................................................... 3
   1.1. Auditing/Controlling .......................................................................................................................................... 4
   1.2. IT-Administrator ................................................................................................................................................ 4
   1.3. Management ...................................................................................................................................................... 5
   1.4. Business users/department heads .................................................................................................................... 6

2. Risk management with Garancy Access Intelligence Manager ........................................................................ 7
   2.1. Risk identification with Garancy Access Intelligence Manager ........................................................................ 7
   2.2. Risk assessment with Garancy Access Intelligence Manager ............................................................................... 9
   2.3. Risk control with Garancy Access Intelligence Manager .................................................................................. 11
       2.3.1. Effective prevention and IT forensics – essential for IT audits .............................................................. 11
       2.3.2. High-Risk Users ......................................................................................................................................... 12
       2.3.3. Ad hoc analyses ......................................................................................................................................... 12
       2.3.4. Permission path analysis ......................................................................................................................... 13
       2.3.5. Temporary permissions .......................................................................................................................... 14
   2.4. Risk monitoring with Garancy Access Intelligence Manager ....................................................................... 14

3. “Focus on What's Important” – quickly, easily and clearly ................................................................................. 15
   3.1. Gradual introduction – from data import to risk ranking ................................................................................. 16
   3.2. Analysis of relevant regulations .................................................................................................................. 17

4. Recommendations for intelligence-based risk management ............................................................................ 18
Access Risk Support for All Phases of Risk Management

A risk management system that takes access control into account can help reduce IT risks significantly and thus mitigate the consequences of strategic and operational risk. All granted access permissions pose a potential risk for the company. And the number of accounts and access permissions in corporate data systems continues to skyrocket. This is the main reason why companies are now increasingly aiming their risk management efforts at managing access permissions, as deficiencies within the access control system can affect all other risks.

Legal requirements, such as stricter privacy policies, also play an important role, as the control and traceability of permission granting is a basic condition for compliance with various regulations. Therefore, internal access permissions should be set up so that employees can only access the specific systems needed for their jobs. Access must be limited to those functions that are absolutely necessary for completing assigned tasks.

Support in All Phases of Access Risk Management

Access Risk Management & Analytics with the Garancy Access Intelligence Manager offers the best possible support for all phases of access risk management, from identification, assessment and control to continuous tracking and monitoring of permission risks. Below, we show how the Garancy Access Intelligence Manager supports businesses and how the various target groups within the company can benefit from:

- ready-to-use analyses
- standard analyses for select use cases
- high interactivity through links between reports (drill-down, drill-through, etc.)
- use of identified deficiencies as a basis for ad hoc analyses for creating targeted and problem-based reports.

1. “Focus on What's Important” – Benefits for All Target Groups

Generally, a risk management system should ensure that its addressees, such as top management, officers, auditors, etc., are given only information that provides real added value. Here, it’s not so much the quantity but rather the quality of the information that’s important. Qualitative information is based on so-called key indicators, in which large amounts of data are aggregated to make a qualitative statement. This makes it possible to recognize important data immediately and keeps the focus on high-risk areas.

Beneficiaries of Access Risk Management

Lastly, the beneficiaries of Access Risk Management can be divided into four main target groups: auditing and controlling, IT or IT security, management, and users in the various departments. The following figure illustrates the benefits received by each of these four areas through the introduction of Access Risk Management & Analytics:
1.1. AUDITING/CONTROLLING

Corporate auditing has become an increasingly time consuming task. Almost all companies expend a significant amount of manual effort in meeting audit requirements. Here, Garancy Access Intelligence Manager offers many advantages. Spontaneous questions from the auditor regarding access management can now be answered with unprecedented flexibility.

The secure and compliant implementation of new regulatory requirements also requires a structured approach for Identity Access Governance (IAG). Growing compliance pressure has resulted in administrative requirements – particularly with regard to the preparation of audit reports – that cannot be taken lightly, as they often constitute a significant portion of the workload in IT departments: Which users have access to which resources? How do I know exactly which cases are high-risk?

For example, information regarding the user’s permission profile within his or her business context, such as department or job function, can be included in the analyses. These can be exported in the form of a comprehensive and detailed report along with relevant recommendations from the auditor.

1.2. IT-ADMINISTRATOR

The IT administrator or IT security manager receives comprehensive analyses and information for assessing the risk and current status of access permissions. In addition, extensive drill-down and drill-through options are available which allow access permissions to be analyzed in almost any form.
The Garancy Access Intelligence Manager creates a link between the technical perspective and the business perspective. It compiles and organizes permission data by individual user and features an intuitive user interface developed especially for non-techies. This solution lets the departments not only create powerful risk analysis but also use them appropriately, thus alleviating the IT administration workload.

Risk management is particularly important with regard to structured and secure IT design initiatives. With risk management based on the Garancy Access Intelligence Manager, weaknesses in the organization can be directly identified and recommendations for reducing access risk formulated.

1.3. MANAGEMENT

Management benefits from the introduction of risk management systems in many ways. For example, transparency in permission granting is increased while changes remain traceable and accountable to ensure compliance with IT regulatory requirements. Through dashboards with weighted information and key risk indicators, management can quickly and easily obtain ideas for follow-up actions to minimize risk. Access risk is measured and expressed numerically for management review.

PROOF OF COMPLIANCE WITH REGULATORY REQUIREMENTS

Here, the importance of an effective internal control system (ICS) in preventing and detecting obvious compliance gaps is clear. The link between the compliance management system and the ICS centers on the following questions:

- Does the existing ICS have sufficient and appropriate controls to cover the identified and assessed compliance risks (control design)?
- Do existing controls prevent or detect enterprise-wide compliance effectively (control effectiveness)?

The compliance management system thus allows the continuous assessment and monitoring of ICS components used to monitor compliance. This includes the implementation of controls in business processes, such as through incorporation into work policies and procedures, process documentation and prescribed approval processes.

The key is to ensure that the controls are visible within the systems themselves. This is where Garancy comes into play with the Compliance Indicator. It shows key indicators such as users without permissions or orphaned accounts, which are essential to compliance (see Figure 2). The analysis helps companies detect anomalies quickly so they can be investigated further. The analysis is available in four different categories: users, accounts, roles and groups. It shows the most important indicators selected at a glance.
The risk analysis presents data at different levels of aggregation and detail and can thus be used by everyone from top management all the way down to the department heads. Department heads can detect differences in permissions inside a peer group at a single glance. This allows comprehensive monitoring of risks and forms the basis for the implementation of risk reduction measures.

Business users, i.e., users within the respective departments, also benefit from the simplicity and clarity of the system. The Garancy Access Intelligence Manager solution is intuitive and self-explanatory, letting users feel at home right away in their customary environment. They can use ready-made analyses that meet their individual needs, such as peer group comparisons.

These analyses can be sent regularly and automatically as a push service. The structure of the analyses creates a priority lists for further risk handling, such as for high-risk users. This allows for more effective recertification based on risk ranking, for example.
2. RISK MANAGEMENT WITH GARANCY ACCESS INTELLIGENCE MANAGER

**Definition:** Risk management is defined as the systematic handling of risks. It consists of several phases: risk identification, assessment, control and monitoring.

**Cause-based strategies**
The aim of these strategies is to reduce the extent of potential losses and/or the probability of their occurrence. Cause-based strategies include risk avoidance and risk reduction.

**Effect-based strategies**
These are aimed at reducing the estimated damage resulting from permission abuse. They include risk transfer and risk provision strategies.

The Garancy Access Intelligence Manager employs primarily cause-based strategies (preventive approach). It allows risk to be reduced in a number of different ways. To better depict the extent of the risks and their progression over time, a number of highly informative indicators can be used. By using standard as well as ad-hoc analyses, risks can be portrayed precisely according to the client’s needs.

2.1. RISK IDENTIFICATION WITH GARANCY ACCESS INTELLIGENCE MANAGER

Before risks can be avoided, reduced or managed, they must first be identified. While this may seem trivial, it is a complex task in terms of permission management. Detecting and assessing risks among the enormous amounts of data that continuously accrue in the access management environment is a lot like finding the proverbial needle in the haystack. With a growing number of users, roles and IT systems – all of which must be granted permissions – the sheer number of risk opportunities rises exponentially.

A company with 5,000 employees and only 50 IT systems with ten permission groups each, for example, has over 2.5 million permission-granting possibilities, each of which may represent a high or low risk for the company. In light of this, the task of identifying all the existing risks from these permissions, assessing their effects and defining appropriate measures seems hopeless.

In fact, even a reasonable amount of effort is usually not enough to detect and assess all the possible risks associated with access management. Therefore, a better strategy is to identify the most risky permissions first, assess them and then combat them with adequate measures.

To determine which permissions pose which risks, the Garancy Access Intelligence Manager features high-performance tools that allow companies to use standard analyses to obtain, for example, information on the effects of certain risk assessments on individual permissions and users in a short period of time.
**USER RISK ANALYSIS**

The User Risk Analysis provides data on risks by user based on their assigned groups. It shows the number of users in a department grouped by risk type (none, low, medium, high) along with the associated direct and indirect roles or the number of direct user groups and subgroups as well as the number of accounts and IT applications used by each user (see Figure 3). High-risk departments are directly and immediately identified. The User Risk Analysis allows companies to identify high-risk users and roles within an organizational unit quickly and determine the source of these risks.

![User Risk Analysis](image)

*Figure 3: Sample User Risk Analysis*
2.2. RISK ASSESSMENT WITH GARANCY ACCESS INTELLIGENCE MANAGER

The major challenge of risk analysis is that, even though the company’s systems are provided by the IT team, they are largely operated and used by other departments. Naturally, an access permission risk analysis must also take into account large volume of data – currently a major topic in the industry. In our view, however, the biggest task is in assessing and depicting whether and why an employee holds access permissions and what type of risk arises from these permissions. This assessment should not be performed by the IT team alone.

Identity Risk Management metrics must fulfill a number of important tasks. First, they must make the distribution of access permissions clear and provide information on the quality of the identities, the roles they play within the organization and how they are managed. Secondly, they must provide information on the decision-making process for access permission granting based on an origin analysis. Problem areas should be easily detectable through dashboards.

Now, if our goal is to make risk management into a measurable, objective parameter, we are faced with the challenge of deriving a single piece of information (such as “how high is the risk for a particular user, role or group?”) from a large number influencing factors.

These include:

- **Risk assessments**: at the role, group, resource and permission level
- **Risk observation**: at the user, organization or job function level

**RISK TYPE AND RISK RATING**

Garancy uses a class-based approach, under which roles, groups, resources and permissions are evaluated by risk type (low, medium, high risk) and risk rating. The risk rating is a numerical classification of individual permission objects, in which risk is generally assessed on the basis of threat potential, the probability of the damage event and the expected impact. All other risk parameters are automatically calculated.

**RISK CLASSES**

Based on the risk type and risk rating, the analyses form risk classes with three levels per risk type. Class configuration can be customized. The following class definitions are standard (see Figure 4):

<table>
<thead>
<tr>
<th>Risk Type</th>
<th>Begin</th>
<th>End</th>
<th>Risk Class</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low</td>
<td>0</td>
<td>30</td>
<td>L+</td>
</tr>
<tr>
<td>Low</td>
<td>31</td>
<td>60</td>
<td>L++</td>
</tr>
<tr>
<td>Low</td>
<td>61</td>
<td>x</td>
<td>L+++</td>
</tr>
<tr>
<td>Medium</td>
<td>0</td>
<td>30</td>
<td>M+</td>
</tr>
<tr>
<td>Medium</td>
<td>31</td>
<td>60</td>
<td>M++</td>
</tr>
<tr>
<td>Medium</td>
<td>61</td>
<td>x</td>
<td>M+++</td>
</tr>
<tr>
<td>High</td>
<td>0</td>
<td>30</td>
<td>H+</td>
</tr>
<tr>
<td>High</td>
<td>31</td>
<td>60</td>
<td>H++</td>
</tr>
<tr>
<td>High</td>
<td>61</td>
<td>x</td>
<td>H+++</td>
</tr>
</tbody>
</table>

*Figure 4: Standard Class Definitions*

Risk ratings are always aggregated or totaled within a risk type. Thresholds are defined to determine which totals are classified as high, medium or low. The system clearly shows the totals within each type or class. In contrast to a purely numerical value, this approach makes the risk carried by each employee easy to identify.
RISK SCORING

Risk scoring involves “adding up” all the attributed risks (see Figure 5). This can be based on various mathematical approaches (sums, algorithms, etc.).

![Figure 5: Risk Score](image)

The advantage of this approach for assessing risk is that it aggregates individual risks for each permission by individual user. Here, the Garancy Access Intelligence Manager provides support by aggregating individual risks by entitlement type (role, group, resource, permission). Rather than simply adding up the risks, Garancy uses a class-based method in which aggregation takes place solely within a class.

In the detailed view, the Garancy Access Intelligence Manager shows the permissions granted to the user as well as individual risk classes and risk assessments (see Figure 6):

![Figure 6: Risk classes and risk assessment](image)

The risk grade shows the risk potential of the individual user. This is automatically calculated on the basis of the given information.

The underlying risk assessment model gives companies a detailed overview of the total risk of a particular user, the composition of said risk and the origin of the risk.

RISK LIMITS

To prevent or monitor risk potential, risk limits must be configured. These limits are based on an individual object (such as role) and may be set up per user or per organizational unit. When permissions exceeding these limits are requested via the workflow, the involvement of the risk manager is triggered. The risk manager then decides whether to approve or deny the request. In doing so, he or she relies on the analyses provided by Access Intelligence.
2.3. RISK CONTROL WITH GARANCY ACCESS INTELLIGENCE MANAGER

What effects does risk control have on access management? Why should qualified and quantified risk assessments not be used for previously unconsciously risk-controlled decisions? How does risk scoring affect risk reduction strategies? What does it mean for organizational processes and what can be done to further reduce the probability of the risk, i.e., the damage incident? Through clearly arranged dashboards and compressed data, the Garancy Access Intelligence Manager shows you in a highly condensed and easy-to-understand fashion how to reduce access management risk.

Key risk indicators are used to control risks. They are based both on standard analyses and reports such as the User Risk Analysis and Compliance Indicator Report as well as on ad hoc analyses.

Risk analyses can be used for other important functions, such as:

- improving processes
- checking the efficiency of the organization
- introducing preventive controls
- dashboard-based risk score cards for top management and the departments
- risk reporting for the Identity Access Management system (in preparation for overall risk management)
- prioritizing IAG tasks (e.g., recertification for high-risk users first)
- defining approval processes and approval levels based on risk scores
- KRIs (key risk indicators) for monitoring the current risk situation
- controlling the quality of current permission structures from a risk perspective

2.3.1. EFFECTIVE PREVENTION AND IT FORENSICS – ESSENTIAL FOR IT AUDITS

An Access Intelligence based risk management system is much more than just a reporting system – it allows effective prevention and IT forensics through intelligent analyses. In IT forensics, suspicious or peculiar permissions are detected and thoroughly analyzed and their digital traces evaluated.

Effective prevention and IT forensic tasks include:

- **Risk classification of users** based on granted permissions; in accordance with client requirements or data needs; based on roles, groups, permissions or resources
- **Comparison of actual versus target values**: Does a user’s risk classification match his or her risk level?
- **(Top ten) list of high-risk users**: grouped by different criteria (organization, job function, source system, etc.)
- **Object filtering**: Focus on critical users or critical permission objects
- **Identification of orphan accounts**, i.e., accounts not associated with a user but which remain active and may be used illegally. These are to be deleted per ISO 27002.
- **Generation of key risk indicators and trend analyses**: View risk progression over time
The following examples clearly show the preventive and forensic benefits of a BI technology based risk management system.

### 2.3.2. HIGH-RISK USERS

Due to the time and effort required, it is rarely possible to identify and assess all the risks related to access management. Therefore, an effective strategy is to identify the most risky permissions first, assess them and then combat them with adequate measures. Every company should be capable of answering the following questions with regard to high risk users, privileged users or administrators:

- Does the company have users who have access to sensitive data in their daily business?
- Does the company have adequate tools to reduce access permissions to a minimum?
- Can the company reduce risk even further by modifying access permissions, such as through role concepts?
- Can the activities of privileged users be recorded?

Given the rising numbers of users and IT systems and increasing compliance requirements, companies need systems that can help bring transparency to the highly complex IT landscape. For users with special permissions this means:

- Periodic review of these permissions in terms of who they are granted to and which higher-level groups or roles use them
- What activities do these authorized users perform?

By identifying privileged users or high-risk permissions or authorizations, the company can focus on these groups. This results in a fast and focused analysis from which appropriate measures can be derived.

### 2.3.3. AD HOC ANALYSES

Whether a granted permission is risky and, if so, how high the risk is, depends on many non-standardizable factors:

- **Toxic permission combinations** can be defined using SoD rules. The question here is how much a user’s potential risk grows when allowable permissions are combined. Whether or not granting several individually harmless permissions increases a user’s risk can only be judged with knowledge of the systems and organizational units involved.

- **Role models** in the access management system, which are based on the job description for each employee, generally serve as an efficient and transparent link between business and IT perspectives. Here, too, however, determining which risks arise when a company grants multiple roles to a single user is highly individualized.

- In many cases, **standard permission models** can be developed for individual organizational units. Users from the same department often receive identical or similar permissions. Comparing risk across organizational units (e.g., different subsidiaries) requires detailed knowledge of the tasks/processes, similarities and differences between these units – a task that is difficult to solve using standard reports.
For special cases such as these, Garancy Access Intelligence Manager offers ad hoc analyses. An Access Intelligence based risk management system serves as a tool in which companies and organizations can process all of their access management data by using the world’s most powerful and advanced ad hoc reporting system: Microsoft Excel. Microsoft Excel is literally the most flexible form of end-user data processing and visualization. It is known to millions of users who appreciate its functions and operations.

**SEMANTIC INTERFACE**

The semantic interface is based on the data model of the Garancy Access Intelligence Manager, making it easy to understand from a business perspective. It can be used to conduct analyses in Excel. Unlike database/data warehouse-oriented systems, Garancy Access Intelligence Manager provides a fully comprehensive semantic interface in which Access Intelligence objects (user, system, group, role, etc.) can be used for ad hoc reports with their attributes (name, type, category and many more) and existing links. This interface serves as the basis (in Excel) for the drag and drop approach. Users need no technical knowledge of table structures or internal database links to generate custom information and reports on their access management universe.

With the Garancy Access Intelligence Manager, users can formulate questions at the high abstraction level of the business intelligence (BI) cube using pivot tables and charts in Excel. By linking any series of data model objects to one another, Garancy Access Intelligence delivers the desired information. From detailed lists of individual permission areas to aggregation of key indicators, the functionality of Microsoft Excel is unlimited.

### 2.3.4. PERMISSION PATH ANALYSIS

In addition to the typical question of “who has what type of access to which resources,” the widely ramified permission structures give rise to another important question: “Through which classifications (roles, groups, permission objects, etc.) were the permissions granted to the user?” To answer these questions, Beta Systems has developed a method that breaks down the entire permission structure into individual paths that form the basis for powerful analysis capabilities. The second question above thus becomes much more transparent: **Over which permission paths does the user have access to the resources?** With this path-oriented approach, a variety of innovative analyses are possible, which Beta Systems summarizes under the term “permission path analysis.”

The permission path concept makes it possible to perform analyses that add a high degree of value to the security of a company, such as redundancy analyses and path length analyses.

**REDUNDANCY ANALYSIS**

The redundancy analysis examines permission structures for path redundancy. Redundant paths are duplicate permissions that can arise from the assignment of different security objects and from the relationship between these objects. This is typically caused by overlapping role or group models. The assessment of whether redundancies have a positive or negative effect on the use and maintenance of the permission structure is highly client-specific and depends on the objective of the respective models.

**PATH LENGTH ANALYSIS**

On the other hand, path length analysis examines individual permissions based on their path length. The greater the number of permission objects the user must run through, the longer the permission path. However, the more permission objects that are involved, the less user permissions can be controlled. The reason for this is that, with every new object, permission granting is delegated to a higher level. Since additional permissions can be added on each new level, there is also the danger of a “dilution.”
2.3.5. TEMPORARY PERMISSIONS

A typical use scenario in which the issue of transparency and monitoring is extremely important is the classic case of temporary maintenance and support permissions, which are often granted for a single weekend and automatically revoked thereafter (see Figure 7).

![Role Details](image)

Figure 7: Role Details

Often, permissions cannot be automatically revoked because IT systems are not available, for example, at a specific time. Depending on how often permissions are automatically revoked, employees may end up keeping their permissions longer than originally planned. During this time, there is increased risk potential.

2.4. RISK MONITORING WITH GARANCY ACCESS INTELLIGENCE MANAGER

Changes in threats, in the organization itself and technological advances require the ongoing re-assessment and monitoring of risks to continuously and consistently secure the IT infrastructure and critical data. For this purpose, the Garancy Access Intelligence Manager provides continuous monitoring to complement existing standard analyses with client-specific or situational ad hoc analyses.

Errors and irregularities in permissions are identified immediately. The immediate traceability of permissions and permission granting is particularly important.

With Access Intelligence solutions, the intelligent analysis and monitoring of permissions is raised to a new level of quality, allowing risks to be displayed transparently by employee, role and group at any time.

This is made possible through the use of analytical functions that employ business intelligence/data warehouse technologies. Since risk monitoring occurs on different levels, many questions need to be answered, as shown in diagram below:
Through comprehensive risk monitoring, the Garancy Access Intelligence Manager can uncover weaknesses in the IAM system, such as cases where users had more access privileges than necessary or privileged users (i.e., user groups with privileged accounts, such as those with elevated permissions, or shared accounts) were able to perform activities that they should never have had the ability to perform.

**SOD MONITORING**

As a consequence of the Minimum Requirements for Risk Management (known as MaRisk), explicit rules for the segregation of duties with technical systems are required; these must also be technically implemented and adherence/compliance demonstrated. With the Garancy Access Intelligence Manager, SoD violations can be uncovered.

### 3. “FOCUS ON WHAT’S IMPORTANT” – QUICKLY, EASILY AND CLEARLY

No risk management system can promise to detect absolutely every access risk. However, our BI technology-based Access Intelligence solutions ensure that all the important factors for compliance are identified and documented. Access Intelligence shows you specifically where problems might arise and provides detailed starting points for reducing risks.

For this purpose, the Garancy Access Intelligence Manager provides best-of-breed analysis techniques, comparison options and dashboards for visualization purposes (see Figure 10).
3.1. GRADUAL INTRODUCTION – FROM DATA IMPORT TO RISK RANKING

A clearly formulated and easy-to-understand model for introducing a risk management system for access control is fundamental. The introduction must take place step by step, with the technology itself implemented only at the very end. It is especially important to decide who will assess the risks.

Initially, only the most important potential risks are assessed. In this area, the experienced consultants of Beta Systems Software can provide in-depth proposals and recommendations for action. To keep costs within budget, we recommend focusing on only the most important areas, such as high-risk applications and systems. Non-relevant issues or very minor risks are not pursued at this point. This will allow the quick introduction and implementation of the risk management system.

The Garancy Access Intelligence Manager features a data import interface for importing data from different systems. These are typically IAG systems, but other source systems are also possible.

The risk assessment process can be gradually expanded at a later stage. For example, risk limits can be entered or business-oriented workflows incorporated to trigger a number of automated actions.

Figure 10: Sample management dashboards
3.2. ANALYSIS OF RELEVANT REGULATIONS

The regulations cited most often by German financial companies as being most relevant to risk management are the Banking Act (KWG) and MaRisk.

KWG AND MARISK

KWG section 25a provides for the introduction of a risk management system to ensure organizational compliance with legal requirements. It states:

“An institution must have a proper business organization that ensures compliance with legal requirements applicable to the institution and the needs of the business. The persons referred to in section 1, paragraph 2, sentence 1 are responsible for the proper business organization of the institution. A proper business organization includes, but is not limited to, adequate and effective risk management to allow the institution to continually ensure its risk-bearing capacity;”

MaRisk includes provisions relevant to IT with regard to risk management or internal control procedures (AT4), requirements for internal audits (AT 4.4) and technical/organizational equipment (AT 7). With regard to segregation of duties, MaRisk requires the following:

- AT 4.3.1: When designing organizational structures and procedures, care should be taken to ensure that incompatible activities are performed by different staff members.
- BT O 1.1.: The basic principle for the design of these processes in the lending business is a clear organizational separation between the front and back office, up to and including the top management of the company. For small institutions, exceptions to the rules regarding segregation of duties are possible under certain conditions.

What does this mean for IT? In IT, segregation of duties is used within the context of user permission management. Different technical functions are assigned to different roles. This helps prevent criminal actions by employees. If, for example, an employee is able to update supplier data or create new suppliers in the IT system and simultaneously initiate payments, he or she would have the opportunity to embezzle funds (such as by creating fictitious vendors and generating payments to them).

MaRisk very clearly calls for the establishment of an organizational and technical permission management system. In addition to segregation of duties, MaRisk also calls for the following under AT 7.2:

The IT systems (hardware and software components) and related IT processes must ensure the integrity, availability, authenticity and confidentiality of the data. For these purposes, the design of IT systems and related IT processes should generally be based on established standards; in particular, processes for the appropriate granting of permissions by IT are to be implemented to ensure that each employee has only the permissions needed for the job; permissions may be grouped in a role model. The suitability of IT systems and associated processes should be regularly checked by technical and operational staff.
4. RECOMMENDATIONS FOR INTELLIGENCE-BASED RISK MANAGEMENT

What factors in particular should companies keep in mind when planning, introducing and implementing an access risk management system?

- Take advantage of the possibilities offered by modern risk management solutions in conjunction with Access Intelligence.

- “Think big, start small!” The Business Intelligence approach offers tremendous potential for far-reaching analyses. Utilize an expandable system early on.

- Manage risk using a phase model.

- Make it as easy as possible for your colleagues to quickly and reliably generate useful risk management information within their departments or for top management.

- Don’t get bogged down with simple quantitative risk assessments: use qualitative, content-based ratings instead.

- Identify high-risk users: You don’t need an answer to every single question – just focus on what’s important.

- Use permission path analyses to determine who granted the permission and when, and whether he/she was authorized to do so.

- Take advantage of ad hoc analyses: Insist on the ability to create your own analyses in a simple, customized fashion according to your needs.