What You Should Know about Your Identity & Access Management

Verifiable Implementation of Regulatory Requirements

In cooperation with

_betasystems

—

January 2019

Table of Contents

Garancy Access Intelligence Manager (AIM) Product Description

Garancy Access Intelligence Manager provides powerful analysis capabilities, such as:

- Monitoring a broad range of data sources
- Analysis of current access permissions
- Historical analysis of access permissions with the Garancy TimeTraveler module
- Forensic analyses
- Frequency and trend analyses
- Risk and role management analyses
- Meeting compliance requirements for access permissions
- Preventing identity abuse or threats from insiders

These functions give companies a deep insight into their authorization landscape and its underlying organizational layout.

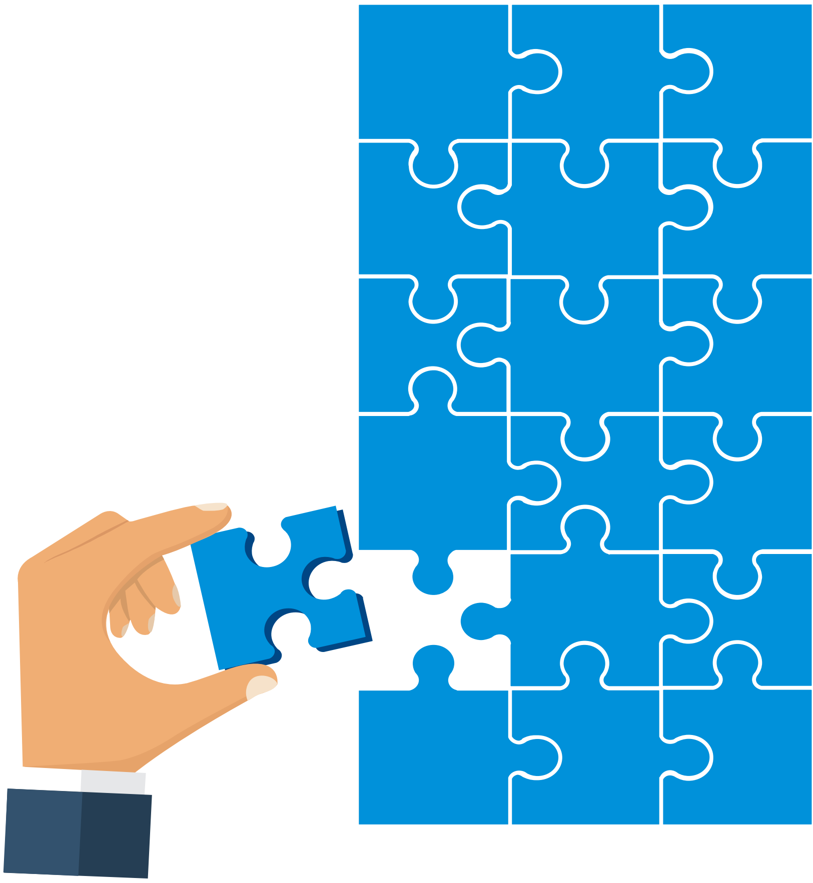
This information forms the foundation for effective governance measures across the company that allow you to instantly analyze and process data generated in the user provisioning systems.

It is increasingly the case that access authorizations are managed by the corporate specialist departments. For this reason, Garancy AIM provides the people in charge with all relevant user data in easy-to-use dashboards and offers analysis methods at the push of a button. This empowers you to demonstrate compliance with internal and external requirements, in particular in the event of an audit.

Based on a data warehouse system, Garancy AIM collects and stores authorization data and the relationships among individual data units. This specifically applies to changes in the status or interrelationships. The data is stored in a multi-dimensional format that facilitates advanced evaluations that are not possible in a normal reporting system (e.g. historical evaluations, end-to-end observations, risk analyses or compliance indicators). In contrast to snapshot-based mechanisms, a complete history is available thanks to a continuous track changes process. As a result, any time period or even daytime changes can be analyzed in a multitude of ways.

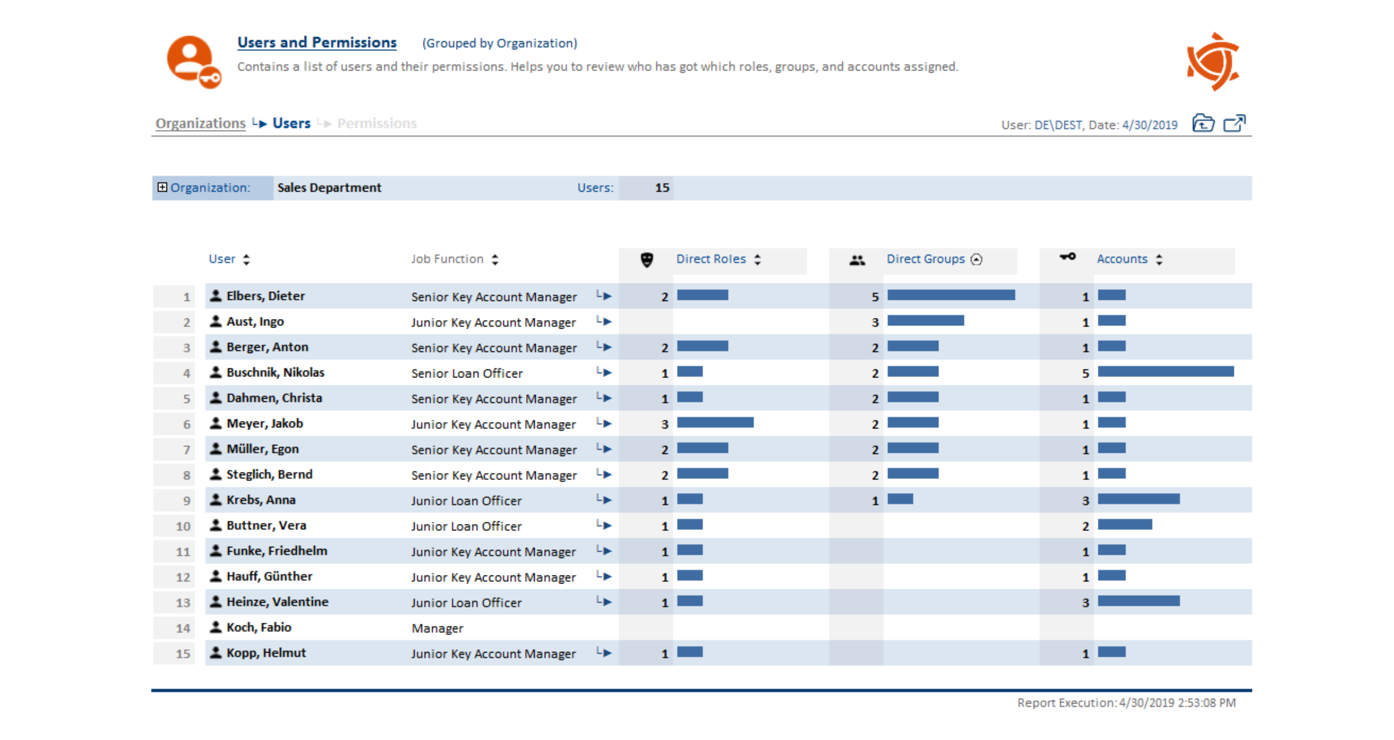
The solution brings transparency and security to business processes and allows them to be reviewed retroactively. It does so by analyzing all business-relevant data sources and providing information in the shape of interactive drill-down and drill-through reports.

The Garancy AIM analysis tool can be linked to the Garancy AIM suite or other IAM systems, providing a fast and efficient solution for advanced analysis options for processing specific IAM data.



Examples of Garancy AIM-Based Analyses

Analysis of current employee authorizations: This delivers a host of useful functions, such as comparing the employees of an organizational unit with regard to the number of assigned authorizations, e.g. as part of an outlier analysis.



Users and Permissions (Grouped by Organization)

Contains a list of users and their permissions. Helps you to review who has got which roles, groups, and accounts assigned.

Organizations ↳ Users ↳ Permissions

User: DE\DEST, Date: 4/30/2019

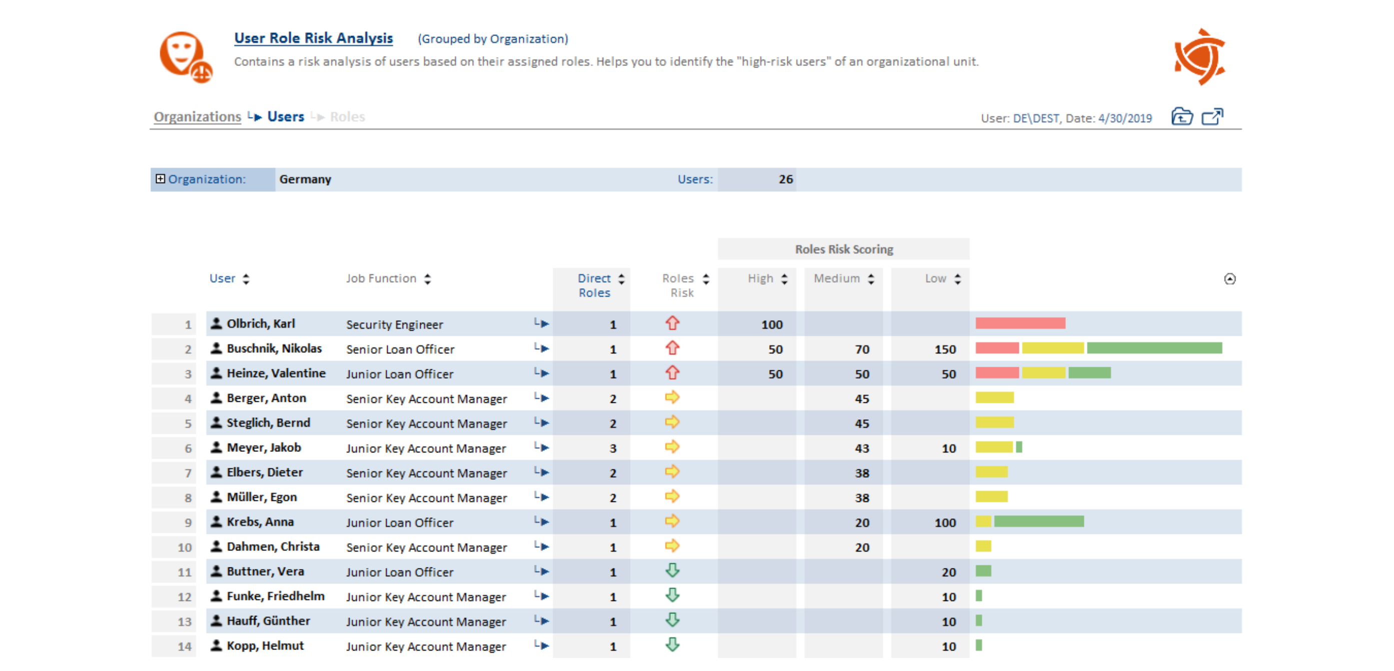
⊞ Organization: Sales Department Users: 15

	User	Job Function		Direct Roles	Direct Groups	Accounts
1	Elbers, Dieter	Senior Key Account Manager	↳	2	5	1
2	Aust, Ingo	Junior Key Account Manager	↳		3	1
3	Berger, Anton	Senior Key Account Manager	↳	2	2	1
4	Buschnik, Nikolas	Senior Loan Officer	↳	1	2	5
5	Dahmen, Christa	Senior Key Account Manager	↳	1	2	1
6	Meyer, Jakob	Junior Key Account Manager	↳	3	2	1
7	Müller, Egon	Senior Key Account Manager	↳	2	2	1
8	Steglich, Bernd	Senior Key Account Manager	↳	2	2	1
9	Krebs, Anna	Junior Loan Officer	↳	1	1	3
10	Buttner, Vera	Junior Loan Officer	↳	1		2
11	Funke, Friedhelm	Junior Key Account Manager	↳	1		1
12	Hauff, Günther	Junior Key Account Manager	↳	1		1
13	Heinze, Valentine	Junior Loan Officer	↳	1		3
14	Koch, Fabio	Manager				
15	Kopp, Helmut	Junior Key Account Manager	↳	1		1

Report Execution: 4/30/2019 2:53:08 PM

Source: Beta Systems. Presentations are not based on actual data.

Risk analysis of the roles currently assigned within an organizational unit, sorted by the accumulated risk:



User Role Risk Analysis (Grouped by Organization)

Contains a risk analysis of users based on their assigned roles. Helps you to identify the "high-risk users" of an organizational unit.

Organizations ↳ Users ↳ Roles

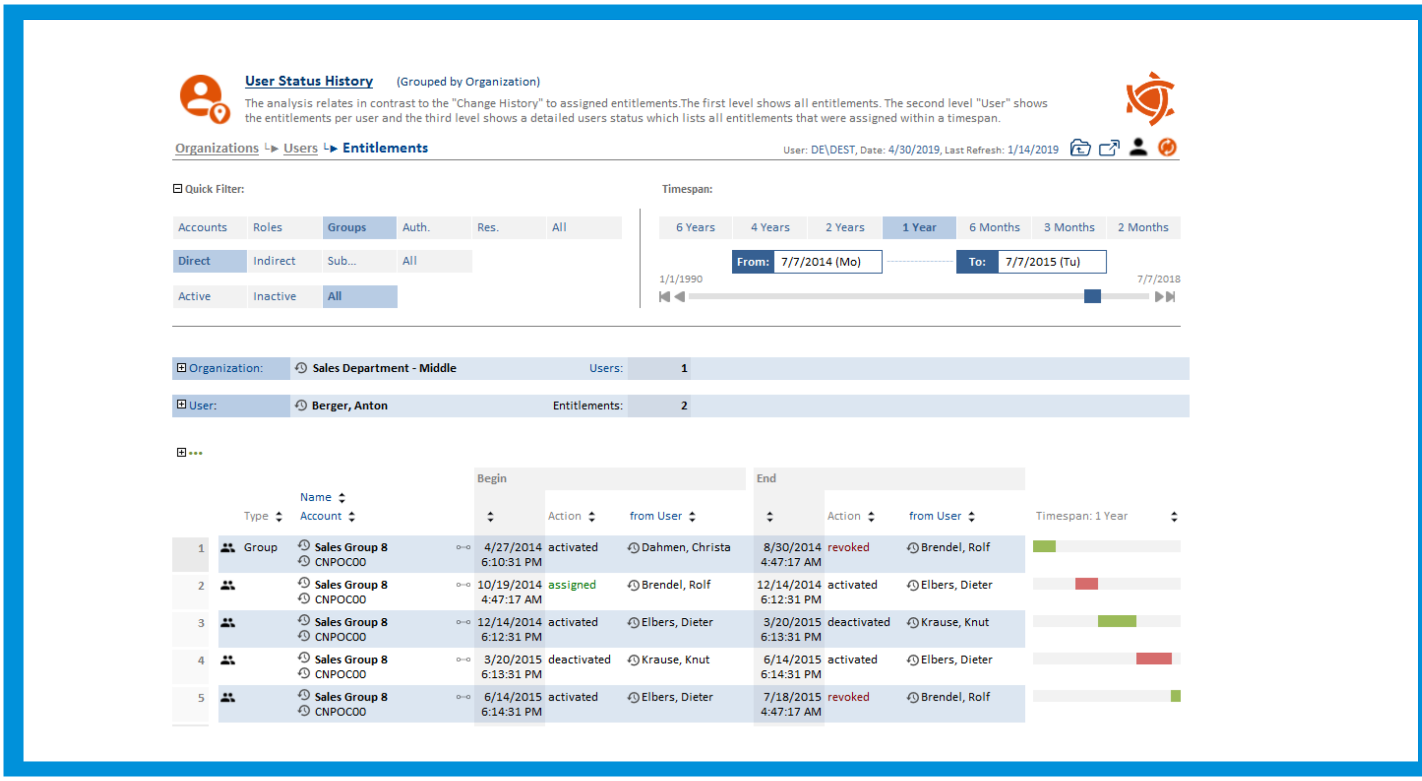
User: DE\DEST, Date: 4/30/2019

⊞ Organization: Germany Users: 26

	User	Job Function		Direct Roles	Roles Risk	Roles Risk Scoring High	 Medium	 Low
1	Olbrich, Karl	Security Engineer	↳	1	⇧	100		
2	Buschnik, Nikolas	Senior Loan Officer	↳	1	⇧	50	70	150
3	Heinze, Valentine	Junior Loan Officer	↳	1	⇧	50	50	50
4	Berger, Anton	Senior Key Account Manager	↳	2	⇨		45	
5	Steglich, Bernd	Senior Key Account Manager	↳	2	⇨		45	
6	Meyer, Jakob	Junior Key Account Manager	↳	3	⇨		43	10
7	Elbers, Dieter	Senior Key Account Manager	↳	2	⇨		38	
8	Müller, Egon	Senior Key Account Manager	↳	2	⇨		38	
9	Krebs, Anna	Junior Loan Officer	↳	1	⇨		20	100
10	Dahmen, Christa	Senior Key Account Manager	↳	1	⇨		20	
11	Buttner, Vera	Junior Loan Officer	↳	1	⇩			20
12	Funke, Friedhelm	Junior Key Account Manager	↳	1	⇩			10
13	Hauff, Günther	Junior Key Account Manager	↳	1	⇩			10
14	Kopp, Helmut	Junior Key Account Manager	↳	1	⇩			10

Source: Beta Systems. Presentations are not based on actual data.

Historic analysis of the groups assigned to a user in a certain period of time (Gantt diagram):



User Status History (Grouped by Organization)

The analysis relates in contrast to the "Change History" to assigned entitlements.The first level shows all entitlements. The second level "User" shows the entitlements per user and the third level shows a detailed users status which lists all entitlements that were assigned within a timespan.

Organizations ↳ Users ↳ **Entitlements**

User: DE\DEST, Date: 4/30/2019, Last Refresh: 1/14/2019

⊟ Quick Filter:

Accounts | Roles | **Groups** | Auth. | Res. | All

Direct | Indirect | Sub... | All

Active | Inactive | **All**

Timespan:

6 Years | 4 Years | 2 Years | **1 Year** | 6 Months | 3 Months | 2 Months

From: 7/7/2014 (Mo) — To: 7/7/2015 (Tu)

1/1/1990 — 7/7/2018

⊞ Organization: Sales Department - Middle — Users: 1

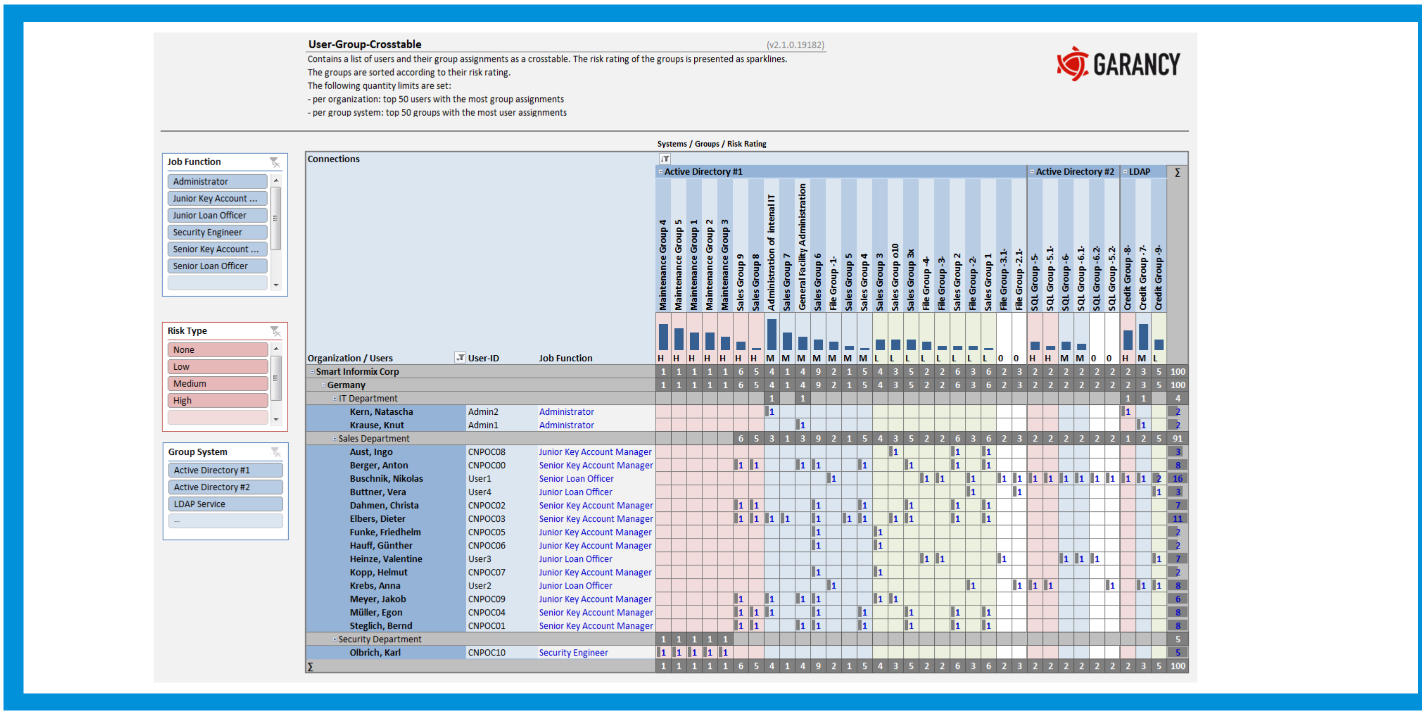
⊞ User: Berger, Anton — Entitlements: 2

⊞ •••

			Begin			End			
	Type	Name Account		Action	from User		Action	from User	Timespan: 1 Year
1	Group	Sales Group 8 CNPOC00	4/27/2014 6:10:31 PM	activated	Dahmen, Christa	8/30/2014 4:47:17 AM	revoked	Brendel, Rolf	🟩
2		Sales Group 8 CNPOC00	10/19/2014 4:47:17 AM	assigned	Brendel, Rolf	12/14/2014 6:12:31 PM	activated	Elbers, Dieter	🟥
3		Sales Group 8 CNPOC00	12/14/2014 6:12:31 PM	activated	Elbers, Dieter	3/20/2015 6:13:31 PM	deactivated	Krause, Knut	🟩
4		Sales Group 8 CNPOC00	3/20/2015 6:13:31 PM	deactivated	Krause, Knut	6/14/2015 6:14:31 PM	activated	Elbers, Dieter	🟥
5		Sales Group 8 CNPOC00	6/14/2015 6:14:31 PM	activated	Elbers, Dieter	7/18/2015 4:47:17 AM	revoked	Brendel, Rolf	🟩

Source: Beta Systems. Presentations are not based on actual data.

Example of an ad-hoc analysis of users and their assigned groups in the form of an Excel cross table.



User-Group-Crosstable (v2.1.0.19182)

Contains a list of users and their group assignments as a crosstable. The risk rating of the groups is presented as sparklines.
The groups are sorted according to their risk rating.
The following quantity limits are set:
- per organization: top 50 users with the most group assignments
- per group system: top 50 groups with the most user assignments

GARANCY

Job Function
- Administrator
- Junior Key Account ...
- Junior Loan Officer
- Security Engineer
- Senior Key Account ...
- Senior Loan Officer

Risk Type
- None
- Low
- Medium
- High

Group System
- Active Directory #1
- Active Directory #2
- LDAP Service
- --

Connections

Systems / Groups / Risk Rating

			Active Directory #1																								Active Directory #2						LDAP			Σ
			Maintenance Group 4	Maintenance Group 5	Maintenance Group 1	Maintenance Group 2	Maintenance Group 3	Sales Group 9	Sales Group 8	Administration of intenal IT	Sales Group 7	General Facility Administration	Sales Group 6	File Group -1-	Sales Group 5	Sales Group 4	Sales Group 3	Sales Group o10	Sales Group 3x	File Group -4-	File Group -3-	Sales Group 2	File Group -2-	Sales Group 1	File Group -3.1-	File Group -2.1-	SQL Group -5-	SQL Group -5.1-	SQL Group -6-	SQL Group -6.1-	SQL Group -6.2-	SQL Group -5.2-	Credit Group -8-	Credit Group -7-	Credit Group -9-	
Organization / Users	User-ID	Job Function	H	H	H	H	H	H	H	M	M	M	M	M	M	M	L	L	L	L	L	L	L	L	0	0	H	H	M	M	0	0	H	M	L	
⊟ Smart Informix Corp			1	1	1	1	1	6	5	4	1	4	9	2	1	5	4	3	5	2	2	6	3	6	2	3	2	2	2	2	2	2	2	3	5	100
⊟ Germany			1	1	1	1	1	6	5	4	1	4	9	2	1	5	4	3	5	2	2	6	3	6	2	3	2	2	2	2	2	2	2	3	5	100
⊞ IT Department										1		1																					1	1		4
Kern, Natascha	Admin2	Administrator								1																							1			2
Krause, Knut	Admin1	Administrator										1																						1		2
⊞ Sales Department								6	5	3	1	3	9	2	1	5	4	3	5	2	2	6	3	6	2	3	2	2	2	2	2	2	1	2	5	91
Aust, Ingo	CNPOC08	Junior Key Account Manager																1				1		1												3
Berger, Anton	CNPOC00	Senior Key Account Manager						1	1			1	1			1			1			1		1												8
Buschnik, Nikolas	User1	Senior Loan Officer												1						1	1		1		1	1	1	1	1	1	1	1	1	1	2	16
Buttner, Vera	User4	Junior Loan Officer																					1			1									1	3
Dahmen, Christa	CNPOC02	Senior Key Account Manager						1	1				1			1			1			1		1												7
Elbers, Dieter	CNPOC03	Senior Key Account Manager						1	1	1	1		1		1	1		1	1			1		1												11
Funke, Friedhelm	CNPOC05	Junior Key Account Manager											1				1																			2
Hauff, Günther	CNPOC06	Junior Key Account Manager											1				1																			2
Heinze, Valentine	User3	Junior Loan Officer																		1	1				1				1	1	1				1	7
Kopp, Helmut	CNPOC07	Junior Key Account Manager											1				1																			2
Krebs, Anna	User2	Junior Loan Officer												1									1			1	1	1				1		1	1	8
Meyer, Jakob	CNPOC09	Junior Key Account Manager						1		1		1	1				1	1																		6
Müller, Egon	CNPOC04	Senior Key Account Manager						1	1	1			1			1			1			1		1												8
Steglich, Bernd	CNPOC01	Senior Key Account Manager						1	1			1	1			1			1			1		1												8
⊞ Security Department			1	1	1	1	1																													5
Olbrich, Karl	CNPOC10	Security Engineer	1	1	1	1	1																													5
Σ			1	1	1	1	1	6	5	4	1	4	9	2	1	5	4	3	5	2	2	6	3	6	2	3	2	2	2	2	2	2	2	3	5	100

Source: Beta Systems. Presentations are not based on actual data.

General Legal Framework

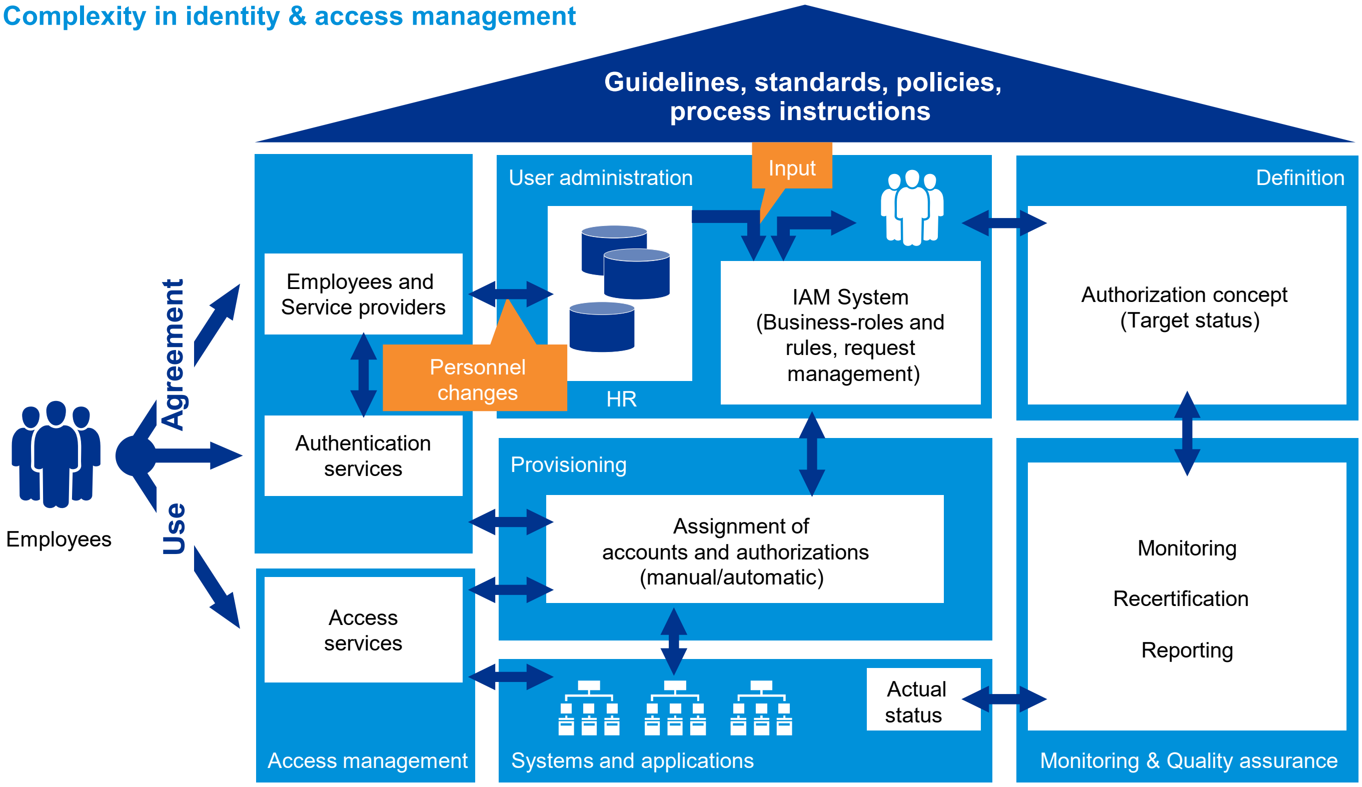
Many companies, in particular those of the financial sector, are subject to strict regulatory requirements. Key provisions are MaRisk (Circular 09/2017 (BA) issued 27 Oct. 2017) and BAIT (Circular 10/2017 (BA) issued 03 Nov. 2017). Other sectors, too, have to meet specific legislation (e.g. BDSG - German Data Protection Act - or GDPR) or are subject to various standards (e.g. ISO/IEC 27001 or COBIT) that aim to protect internal IT. As of 2015, this has also included companies with critical infrastructures to which the BSI IT baseline protection ordinance applies. The topic of identity and access management is a key aspect in all the regulations listed above. MaRisk AT 4.3.1 para. 1, for example, provides a precise definition of segregation of duties, while BAIT 24 deals with authorization concepts.

To ensure that these requirements are met, companies are audited by external or internal auditors. In this context, it is advantageous to be able to present targeted audit analyses in order to ensure fast data delivery within the framework of an audit. This also allows the company to be able to demonstrate it has observed compliance requirements and to document deviations where necessary.

Technical support can help you meet these requirements and thus the objectives of identify & access management (compliance, security and efficiency). It is not enough to purchase a tool that handles the automated implementation of various identity & access management processes; the corresponding processes and specifications (specialist/ technical) must also be defined and implemented.

KPMG AG Wirtschaftsprüfungsgesellschaft (KPMG) is the number one choice for companies looking for an identity and access management (IAM) service provider. KPMG has extensive project management experience as well as broad technical and architectural expertise with a strong focus on identity & access management. This provides the trust and reliability needed to operationalize and implement the relevant identity & access management tasks. The complexity of the subject area is illustrated in the following diagram:

Complexity in identity & access management



Guidelines, standards, policies, process instructions
Employees
Agreement
Use
Employees and Service providers
Personnel changes
Authentication services
Access services
Access management
User administration
Input
HR
IAM System (Business-roles and rules, request management)
Definition
Authorization concept (Target status)
Provisioning
Assignment of accounts and authorizations (manual/automatic)
Actual status
Systems and applications
Monitoring
Recertification
Reporting
Monitoring & Quality assurance

Source: KPMG, Germany, 2019

The following findings arise again and again during external or internal audits. This underscores how urgently companies need to ramp up their identity & access management:

- Lack of transparency regarding authorizations assigned or required (e.g. no reporting options or poor quality of authorization descriptions)
- Lack of transparency regarding 'legalizations‘ (requests/approvals are not comprehensible)
- Excessive authorizations (e.g. ‘trainee effect’ or in relation to privileged accounts)
- Violations of SoD requirements of a supervisory nature (in particular MaRisk for financial institutions) or of an internal nature (e.g. in purchasing procedures)
- Authorization problems with individual systems, especially SAP, Active Directory, file system, SharePoints but also applications and others.
- Inefficient and unclear request procedures (e.g. inconsistent or without a clear structure, reference user-based)
- Considerable time and effort required for process of manual authorization allocation/deletion
- No periodic quality assurance (‘recertification’)
- Lack of acceptance of responsibility
- Downtimes of and delays in IT systems
- Handling www authorizations (e.g. regarding information owners, entry in CMDB)
- Overburdened service desk due to increasingly diverse application landscapes and repetitive routine requests
- Overview of external employees/service providers and their access to company data is not available/incomplete
- Authorizations not organized according to business functions; no role model available

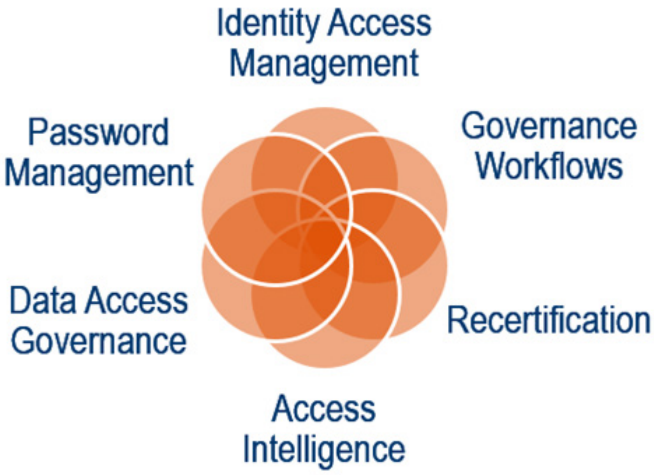
In order to demonstrate how the Garancy AIM analysis tool (technical solution) and the technical competence of KPMG can deliver efficient solutions when faced with such issues, several findings are presented and analyzed below as illustrative examples.

It is strongly advised that you have an IAM (identity and access management) system in place to get the most out of Garancy AIM. This can be achieved by connecting the existing AIM system to the Garancy AIM analysis tool. IAM systems are explained briefly based on the example of the Garancy IAM Suite product developed by Beta Systems.

The Garancy Identity Access Management Suite from Beta Systems provides you with a set of tools for controlling and monitoring access to data and applications according to the individual organizational requirements and specialist role of each user.

The modules of the Beta Systems IAM Suite support all tasks relevant to identity access governance and are available as cloud-based or on-premise solutions run in your own data center:

Garancy IAM Suite from Beta Systems



Source: Beta Systems

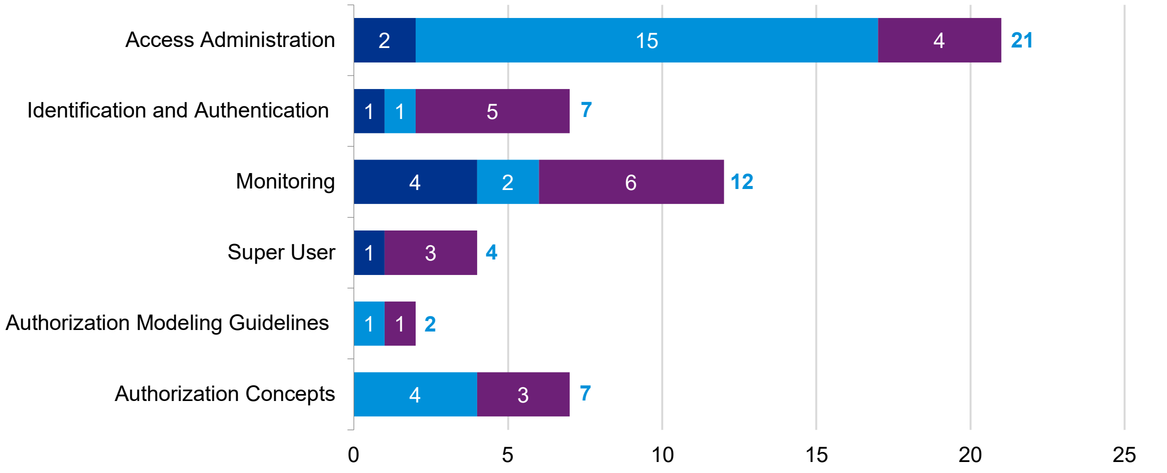
Investigated Authorization Management Findings

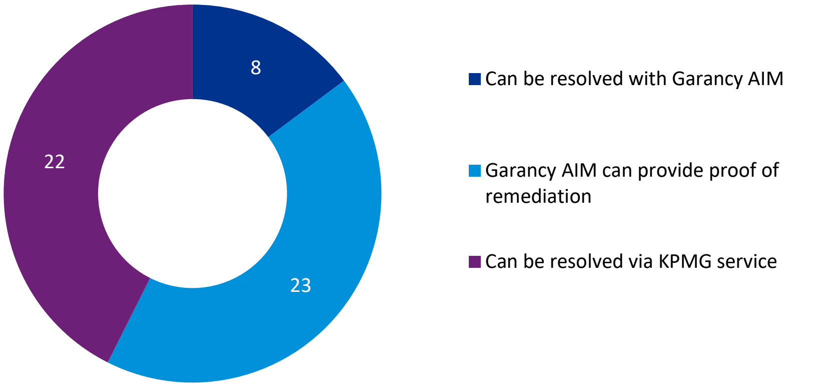
The Beta Systems cooperation partner KPMG examined the findings in the area of identity & access management that it had determined and processed itself. In the following section, ‘finding’ is to be understood as a deviation from binding internal or external requirements.

It turned out that 15% of the findings can be resolved directly using the analysis and reporting capabilities of Garancy AIM. In addition, Garancy AIM provides assistance in resolving more than half of the findings, for example by creating evidence. Overall, Garancy AIM can provide solutions and support for more than half of all findings. Garancy AIM is also suitable for internal monitoring and the preparation of audits. Moreover, Garancy AIM simplifies the task of implementing core concepts for the documentation of authorization structures and the solution provides proof of their implementation. Identified findings not related to Garancy AIM and where Garancy AIM is not used can be supported using KPMG services.

The 53 findings identified were classified into six categories in order to cluster them thematically. The categories are based on a KPMG audit guide. This document describes examples of general IT controls and IDW PS 330 application controls, audit procedures for structural and functional audits, frequent IT findings, possible effects of these findings on application controls and possible supplementary audit procedures. They represent typical IT controls that may, however, vary for of individual clients depending on the complexity and risk assessment. Individual findings can be assigned to several categories. In this case, the most applicable category was chosen.

Findings per category





Source: Beta Systems

Description of the Categories Used

1. Access Administration

The Access Administration category covers the basic tasks of identity & access management. These tasks include the recertification of access authorizations and the implementation of the principles of 'minimum authorization assignment' and functional separation. This includes temporal aspects relating to the process duration as well as formal tasks regarding documentation and the approval of authorization processes. Such processes usually deal with the assignment, change or withdrawal of authorizations.

Findings result frequently from the lack of a request procedure, insufficient refresh cycles for permissions or when one or more of the above principles have been disregarded.

The resulting risks pose a direct threat to the integrity and confidentiality of the company's intellectual property. This could allow an unauthorized person, for example, to misappropriate (intentionally or unintentionally) or intentionally manipulate company data to the detriment of the company.

2. Identification and Authentication

Identification and authentication refers to the allocation of uniquely assignable identities, the development, establishment and implementation of guidelines for passwords, as well as technical user account monitoring.

Typical findings include incomplete insights into external employees, the inadequate allocation of responsibilities for technical user accounts or insufficient requirements/enforcement of password policies.

The failure to meet or observe the relevant requirements jeopardizes all three basic IT protection objectives: integrity, availability and confidentiality. This, in turn, means that the security of corporate data and intellectual property can no longer be guaranteed. The risk thus arises that all or a part of the data could be manipulated, destroyed or disclosed.

3. Monitoring

The monitoring category refers to the monitoring of activities relating to assigned authorizations. This also involves the evaluation of whether duties have been segregated across the system. Violations regularly result from requirements not being observed as regards documentation of a procedure, the monitoring of critical authorizations or the creation of historical reports.

Monitoring and verification of the implementation of IT security guidelines directly serves the implementation of the defined protection goals. Without monitoring, there is a risk that abuse is not identified and that necessary guidelines are softened or circumvented.

4. Super User

When establishing a super user, monitoring of related activities and a thoroughly documented approval process for the revocation of security settings is of the essence. In addition, super user privileges or access to multi-user accounts with super user privileges must be restricted to a small group of people.

These controls and restrictions are designed to protect the company from unsupervised individuals with far-reaching powers. There is a potential risk of a highly authorized individual acting without supervision and manipulating, misappropriating or destroying business-critical information and data without this being identified.

5. Authorization Modeling Guidelines

When designing the identity & access management scheme, a company may have to comply with government and industry-specific requirements as well as internal regulations. This area also includes the development of business roles in which particular attention must be paid to SoD (segregation of duties) compliance.

These specifications serve to ensure that inappropriate access rights cannot be assigned neither intentionally nor unintentionally.

6. Authorization Concepts

The authorization concepts must document who has what kind of access to which data and IT systems.

This documentation is used to record and check identity & access management. It serves the purpose of identifying and eliminating incorrectly assigned authorizations and assigned authorizations that deviate from the defined target status.

Assessment of the Individual Findings by Category in Relation to the Audit

The findings can either be supported or directly resolved with Garancy AIM, or they can be resolved by means of specialist processes and implementations – with or without proof of resolution through Garancy AIM.

The following tables show the remediable findings including an assessment, the resulting risks or a possible solution. Each category includes a final evaluation and conclusion.

The risk description is based on the three fundamental IT security objectives of integrity, availability and confidentiality. Any finding violates at least one of these three protection objectives. No significance or weighting of the overall risk can be derived from assigning a finding to one or more of the protection objectives.

1. Access Administration

1.1 Changing/Leaving Employees – Insufficient Checks

Classification

Problem

No timely reviews are performed to manually revoke or adjust the access rights of employees who have left the company or changed their function within the group. According to MaRisk AT 4.3.1 para. 2, authorizations and competences must be allocated in accordance with the thrift principle (need-to-know principle) and adapted promptly if necessary. According to ISO 27001 A.9.2.5, user authorizations need to be checked regularly.

Risk

Without regular authorization checks, especially for employees who change their function or leave the company, there is a risk that unauthorized users may gain access and may not be detected. Both the confidentiality and integrity of corporate data can no longer be guaranteed.

Solution

For example, you can evaluate how user authorizations have changed due to changes in their job function. One method would be to analyze each user based on a time stream (similar to a Gantt diagram). Users concerned can be identified using the attribute history.

✓

Can be resolved with Garancy AIM

1.2 Transparency: Inadequate Overview of Current User Authorizations

Classification

Problem

Excessive time and effort is required to determine which authorizations an employee has and who approved them. According to BAIT 28, the creation, modification, deactivation and deletion of authorizations and their recertification must be documented in a transparent and analyzable manner.

Risk

The lack of responsibility for and transparency of authorizations carries the risk that the principle of need-to-know authorization assignment will no longer be implemented. The resulting excess authorization increases the risk of a breach of confidentiality and threatens the integrity of company data.

Solution

Part of the finding can be corrected directly with Garancy AIM. The solution allows you to evaluate which authorizations an employee has (with a timeline function that makes changes visible) or which employees have been assigned a particular authorization. According to the current roadmap, future versions will also provide a function for evaluating who has granted the approvals in each case.

✓

Can be resolved with Garancy AIM

1.3 Employee Transfer – Missing Definition Regarding Authorization Revocation

Classification

Problem	There is no definition of how long previously assigned access rights may be kept after a change in function. According to MaRisk AT 7.2 para. 2, the assignment of authorizations must ensure that each employee only has the rights needed for their job. According to ISO 27001 A.9.2.3, the reservation of privileged authorizations should be controlled and restricted.
Risk	In order to uphold the principle of minimum authorization allocation, reasonable time limits for the withdrawal of access rights are necessary. Depending on the type of change of position, even temporary retention of the existing authorizations may result in a violation of the segregation of duties principle. Violation of the principle increases the risk that the confidentiality or integrity of company data may be violated, or that breaches of SoD criteria may result in financial or regulatory damage or damage to reputation.
Solution	You can check how user authorizations have changed due to changes in their job function. One method would be to analyze each user based on a time stream (Gantt diagram).

Garancy AIM can provide proof of remediation

1.4 Employees Leaving – No Account Blocking

Classification

Problem	User accounts of employees who have left the company are not (consistently) deleted or blocked. According to MaRisk AT 4.3.1 para. 2 and AT 7.2 para. 2, each employee may only have the rights needed to perform their job. Authorizations and other competencies granted are to be reviewed within a reasonable period of time both regularly and on a need basis. According to BAIT 26, it must be ensured that the procedures for setting up, changing, deactivating or deleting authorizations comply with the provisions of the authorization concept. According to ISO 27001 A.9.2.6, access rights should be removed or modified upon termination or change of employment, contract or agreement.
Risk	Inactive user accounts unnecessarily obstruct and complicate identity & access management. Unauthorized and active user accounts that still have access to corporate data jeopardize the confidentiality and integrity of that data and carry the risk of these transactions not being attributable to any originator.
Solution	Proof can be generated that indicates blockings and deletions of the user accounts of former employees. If required, it can also be used to evaluate the average or maximum time that elapsed until the respective action was taken.

Garancy AIM can provide proof of remediation

1.5 Authorization Concept – Not in Place for Group-Wide Access Rights

Classification

Problem	There is no group-wide access rights concept, which means that the principle of minimum authorization assignment cannot be guaranteed. According to MaRisk AT 4.3.1 para. 2, processes and their associated tasks, competencies, responsibilities, controls and communication channels must be clearly defined. Authorizations and competencies are to be allocated and adapted according to the need-to-know principle. According to BAIT 24, the scope and terms of use of authorizations are to be specified by means of authorization concepts. Authorization concepts must ensure that authorizations are assigned in accordance with the need-to-know principle.
Risk	If there is no central and group-wide access rights management in place, there is no guarantee that access to the corresponding company data is limited to authorized persons. This results in an increased risk of data leakage or data corruption.
Solution	If, for example, authorization names correspond to internally defined nomenclatures and descriptive attributes such as category and type exist, the proof can be generated that a comprehensive access rights concept has been implemented throughout. This also allows for checking/identifying patterns in the authorization structures, including the documentation of any deviations.

Garancy AIM can provide proof of remediation

1.6 Recertification – Missing Role Model

Classification

Problem	Qualified recertification is not possible because there is no effective role model for authorizations, i.e. there are many individual authorizations. According to MaRisk AT 4.3.1 para. 2 and AT 7.2 para. 2, each employee may only have the rights needed to perform their job, and these rights are to be assigned according to the need-to-know principle. It is possible to bundle authorizations in a role model.
Risk	The recertification of authorizations is intended to ensure that only active and authorized access is possible. This serves to protect corporate data. A role model offers options for bundling and can therefore form the basis for making even extensive data manageable for recertification.
Solution	A record can be generated that documents which authorizations are assigned to employees directly or via roles. In this context, Garancy AIM can also be used for role mining, which helps to correct the finding.

Garancy AIM can provide proof of remediation

1.7 Segregation of Duties – Not Available for Roles

Classification

Problem

No adequate segregation of duties has been implemented for the roles required for the further development and operation of an application (e.g. administrators have authorizations that exceed the required functions, such as entry/modification and release of payments). According to MaRisk AT 4.3.1 paragraph 1 and BTO paragraph 9, it must be ensured that conflicting activities are carried out by different employees. Appropriate procedures and protective measures must be in place to ensure that segregation of duties is maintained for any IT-based process.

According to BAIT 24, the segregation of duties must be ensured when assigning authorizations to users.

Risk

The segregation of duties serves to protect the company against manipulation. The aim is to prevent individuals from making and implementing far-reaching decisions. If ongoing development and operation is not properly separated, for example, a security gap could be deliberately built in that would allow malicious postings in favor of the attacker.

Solution

If the relevant information is loaded into the system via the CSV interface, proof can be generated of all rules and possible violations existing in the system.

Garancy AIM facilitates the initial introduction of rules for the segregation of duties in the form of an ad-hoc analysis.

Garancy AIM can provide proof of remediation

1.8 Substitute Function – Unchecked Authorization Approval

Classification

Problem

An employee acting as a substitute can approve his or her own requested authorizations since no additional check takes place for the approval of requested roles. According to MaRisk AT 4.3.1 para. 1, conflicting activities must be performed by different employees.

Risk

Such a process violates the necessary segregation of duties. Without this separation, individuals can make far-reaching decisions that could, among other things, result in the manipulation or misappropriation of corporate data.

Solution

The finding can be remediated by changing the process. Proof that the above incident has not occurred can be evaluated in a future version of Garancy AIM using the TimeTraveler function.

Garancy AIM can provide proof of remediation

1.9 Authorization Assignment – No Escalation Levels

Problem	No escalation levels have been defined for the request procedure. As a result, prompt processing of requests cannot be guaranteed. According to BAIT 50, escalation mechanisms must be established for processes.
Risk	A request system that delivers results within an appropriate timeframe is necessary in order to prevent impairment of day-to-day business. Such impairment can also lead to the proper process being undermined or circumvented, which runs counter to ensuring effective identity & access management.
Solution	If this finding applies, Garancy AIM will be able to provide proof of the correction of this finding in a future release. This will allow companies to check how quickly processes are completed, for example by displaying the times when and by whom approvals were granted. This functionality is part of the current roadmap.

Classification

Garancy AIM can provide proof of remediation

1.10 Authorization Assignment – Missing Second Approval

Problem	Users are created or modified without the approval of a second, correspondingly authorized person. According to BAIT 26, approval and control processes for the setup, modification, deactivation or deletion of user authorizations must ensure that the requirements of the authorization concept are complied with.
Risk	Due to the lack of control and documentation in the allocation of authorizations, there are no safeguards against or, in cases of doubt, no evidence for the manipulation or misappropriation of corporate data.
Solution	If this finding applies, Garancy AIM will be able to provide proof of the correction of this finding in a future release. This will allow for evaluations that prove/refute whether a second approver who differs from the initial approver took part in the process. This functionality is part of the current roadmap.

Classification

Garancy AIM can provide proof of remediation

1.11 Employee Transfer – Missing Approval for Old Authorizations

Problem

When employees are transferred within the company, they may temporarily retain all or some of their previous authorizations in addition to the new authorizations, provided their new supervisor approves of this. No approval of the former supervisor is obtained. According to MaRisk AT 4.3.1 para. 1, AT 4.3.1 para. 2 and BTO para. 9, authorizations and competencies are to be allocated according to the need-to-know principle and, where necessary, adapted promptly. Conflicts of interest must be avoided when changing function. Segregation of duties must be ensured through appropriate procedures and protective measures.

Risk

Without the involvement of all relevant supervisors, it cannot be ensured that only required authorizations are assigned. Excess authorization increases the risk of the confidentiality or integrity of corporate data being violated.

Solution

If this finding applies, Garancy AIM will be able to provide proof of correction in a future release. As soon as the core issue of the finding has been fixed by changing the workflow engine, Garancy AIM can be used to check how quickly processes are completed, for example by displaying the times when approval was granted by previous and current supervisors. This functionality is part of the current roadmap.

Classification

Garancy AIM can provide proof of remediation (in a future release)

1.12 Employee Transfer – Lack of a Cool-Down Phase

Problem

When an employee is transferred within the company, required cool-down phases for authorizations are not enforced (for example, if an employee changes from the front office area to the back office area, a certain time must elapse between the withdrawal of the front office authorizations and the assignment of the back office authorizations). According to MaRisk AT 4.3.1 para. 2 and BTO para. 9, appropriate transition periods must be provided for when employees move from sales/front office areas to downstream areas and control functions. Conflicts of interest must be avoided when changing function. Segregation of duties must be ensured through appropriate procedures and protective measures.

Risk

The lack of a cool-down phase can lead to excess authorization or the violation of segregation of duties. In both cases, there is an increased risk that company data may be manipulated or not treated confidentially.

Solution

If this finding applies, Garancy AIM can provide proof of remediation using the TimeTraveler feature. This allows users to prove that old authorizations are prematurely revoked for employees who require a cool-down phase, while the process temporarily prevents the assignment of new authorizations. In addition, the current roadmap includes functions for evaluating individual process steps.

Classification

Garancy AIM can provide proof of remediation (in a future release)

1.13 Authorization Assignment – Existing Excess Authorizations

Problem	Excess authorizations exist because authorizations are not assigned according to the need-to-know principle or recertification is not performed (properly). According to MaRisk AT 4.3.1 para. 2, authorizations and competencies must be allocated in accordance with the need-to-know principle and must be adapted promptly where necessary. According to BAIT 24, the need-to-know principle must be applied when allocating authorizations.
Risk	Excess authorization increases the risk that company data is manipulated or not treated confidentially.
Solution	If this finding applies, Garancy AIM can be used in part to provide evidence of the correction of the finding. First, an outlier analysis can be used to check whether employees have excess authorizations in a department/cost center/organizational unit, for example. Second, in a future Garancy AIM release, information from recertification will also be available, allowing companies to provide proof of recertification.

Classification

Garancy AIM can provide proof of remediation (in a future release)

1.14 Authorization Assignment – Lacking Overview of Approved Access Rights

Problem	There is no reliable central database for approved access rights. According to BAIT 28, the creation, modification, deactivation and deletion of authorizations and the recertification process must be documented in a transparent and analyzable manner.
Risk	Insufficient documentation in access rights management can lead to excess authorizations or compromise the segregation of duties. In certain cases, it may also be difficult or impossible to provide proof of a specific access event.
Solution	If this finding applies, Garancy AIM can provide evidence of remediation. Companies can check who has approved the respective rights via the authorization request workflow component. This functionality is included in the current roadmap and will be available in a future release. Depending on the configuration of the workflow, it is currently possible to check whether approval has been granted, but not when or by whom.

Classification

Garancy AIM can provide proof of remediation (in a future release)

1.15 Authorization Assignment – Lack of Dual-Control Principle

Classification

Problem	The approval procedure for handling authorization requests is implemented such that a multi-stage approval may be performed by one and the same person, thus undermining the dual-control principle. According to BAIT 26, the requirements of the authorization concept must be ensured through approval and control processes in the procedure for creating, changing, deactivating or deleting authorizations.	
Risk	If this finding applies, segregation of duties is not ensured. The segregation of duties principle serves the purpose of ensuring that no far-reaching decisions can be made by individuals, thus protecting the company from misuse and/or manipulation.	
Solution	The finding can be remediated by changing the process. In a future version of Garancy AIM, proof of whether the processes have been adapted can be generated using the TimeTraveler function. As a basis for this, authorizations must be able to be evaluated.	**Garancy AIM can provide proof of remediation (in a future release)**

1.16 Segregation of Duties – Infrastructure Components Are Not Included

Classification

Problem	The infrastructure components of an application (operating system, database, application) can be managed by the same person. According to BAIT 24, personal conflicts of interest must be avoided when assigning authorizations to users.	
Risk	There is a risk of manipulation of data or the application’s configuration; as a result, the integrity, authenticity and confidentiality of the data cannot be assured.	
Solution	To correct this, the authorizations must be allocated to both a component and an application by means of an attribute, and it must be possible to determine whether these are administrator permissions by means of an attribute. If this finding applies, Garancy AIM can be used to provide proof of whether there are users who have administrative access to several components of an application.	**Garancy AIM can provide proof of remediation (in a future release)**

1.17 Segregation of Duties – Rule Violations in Business Roles

Problem	It is possible to request business roles that lead to segregation of duties violations without triggering a separate workflow for explicit risk acceptance. According to BAIT 24, the segregation of duties must be ensured when assigning authorizations to users.
Risk	Safeguarding the segregation of duties serves the purpose of protecting the company from misuse or manipulation.
Solution	The finding can be remediated by changing the process. Proof that the above incident has not occurred can be generated in a future version of Garancy AIM by checking the individuals involved in the process. If a segregation of duties violation has occurred, an additional approver must be recognizable in the workflow.

Classification

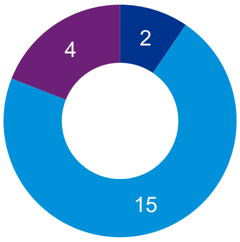
Garancy AIM can provide proof of remediation (in a future release)

Conclusion

Garancy AIM can help a company overcome the challenges posed by requirements such as segregation of duties, recertification and need-to-know-based authorization assignment. These principles are designed to directly protect the company's intellectual property from misappropriation or manipulation.

In addition to the direct monitoring of authorizations, historical reports can also be created that allow further refinement of authorization management and evaluation of the results of processes completed in the past. Moreover, companies can determine characteristic values (e.g. average processing time) for processes that interface with identity & access management in a user-friendly way. These values can be used to provide evidence that a finding under investigation has been resolved or that it still needs to be resolved.

It is not possible to make direct changes to the authorization assignment, change or revocation process. However, the effects of such changes can be demonstrated. KPMG offers to analyze problematic processes with the respective company and develop both technical and non-technical solutions.



🟦 Can be resolved with Garancy AIM 🟦 Garancy AIM can provide proof of remediation 🟪 Can be resolved via KPMG service

2. Identification and Authentication

2.1 External Employees – Incomplete Overview

Problem Overview of external employees and their access to corporate data is incomplete. According to BAIT 28, the creation, modification, deactivation and deletion of authorizations and the recertification process must be documented in a transparent and analyzable manner.

Risk The integrity and confidentiality of corporate data and intellectual property cannot be ensured without full insight into the access rights of external employees.

Solution In the IAM system, external employees can be identified as such (for example, using the nomenclature of their user ID or manually maintained attributes). Once this has been done, Garancy AIM can be used to directly correct the finding. Now it is possible to generate a report that lists the authorizations of external employees.

Classification

✓ **Can be resolved with Garancy AIM**

2.2 Technical Users – No Assignment

Problem Not all technical users are assigned to a responsible employee. According to BAIT 25, non-personalized authorizations must be clearly attributable to an acting person at all times. In justified exceptional cases, deviations must be documented and the resulting risks need to be approved and documented.

Risk Technical users should be clearly attributable to a responsible person to prevent abuse or misuse of the access granted. Such misuse endangers the availability, integrity and confidentiality of accessible corporate data.

Solution If this finding applies, Garancy AIM can provide evidence of implementation of a remedy, depending on the nature of this correction. If technical users can be recognized uniquely in the IAM (for example by using a defined nomenclature, certain HR attributes, or manually assigned attributes), Garancy AIM can be used to generate an evaluation of whether the assignment attribute is filled continuously and consistently points to active users.

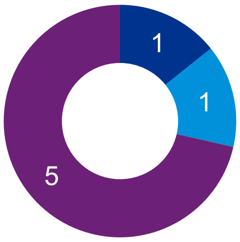
Classification

Garancy AIM can provide proof of remediation

Conclusion

Garancy AIM supports the maintenance and monitoring of authorizations of all kinds, making it possible to retrieve the authorizations of internal and external employees at any time. Even attributes of technical users, such as their assignment, can be viewed and checked for gaps. Gaps in attribute assignments or inappropriate permissions compromise integrity and confidentiality and set the stage for corporate data and intellectual property to be manipulated.

The actions performed on accounts cannot be monitored. KPMG develops suitable processes in close collaboration with their customers and, where necessary, provides aid in selecting suitable tools.



■ Can be resolved with Garancy AIM ■ Garancy AIM can provide proof of remediation ■ Can be resolved via KPMG service

3. Monitoring

3.1 Authorization Evaluation – No Insight into Connected Systems

Problem	It is not possible to provide the IAM tool with an overview of the systems already connected. According to MaRisk AT 12 4.1, a complete and up-to-date overview of the methods and procedures used for risk quantification must exist. Since the connection to an IAM tool has an impact on risk assessment, insights into the connected systems must exist.	**Classification**
Risk	If there is no complete and up-to-date assessment of the risks, it is not possible to adopt a reasonable risk-based approach to identity & access management. Optimal and budget-efficient protection of the business processes and the necessary IT systems can thus not be guaranteed.	
Solution	Garancy AIM can be used to generate an evaluation of which systems are connected to the IAM tool.	✓ **Can be resolved with Garancy AIM**

3.2 Authorization Evaluation – No Historical Reports

Problem	It is not possible to generate historical reports or reports for a specific time frame. According to BAIT 28, the creation, modification, deactivation and deletion of authorizations and the recertification process must be documented in a transparent and analyzable manner.	**Classification**
Risk	In addition to monitoring the development of identity & access management, these reports also serve as proof of compliance with regulatory requirements. Failure to meet these requirements can have significant economic consequences. In addition, it makes it difficult or impossible to provide internal evidence or traceability after an incident.	
Solution	Garancy AIM can be used to create historical reports and reports for specific time frames. Garancy AIM's TimeTraveler feature offers different perspectives on the authorization structure and a status history ('which authorizations did an employee have in a given period?') or a change history ('which authorizations have changed in a given period?').	✓ **Can be resolved with Garancy AIM**

3.3 Missing Authorization Check in Target Systems/Applications

Problem	The recertification of applications is not based on the individual access rights actually approved and implemented (target/actual comparison). According to BAIT 29, companies need to provide verifiable proof that the authorizations are only used as intended. In this context, BAIT 26 also applies as a requirement. This provision implicitly stipulates a requirement that the request situation/target status must correspond to the actual status.	**Classification**
Risk	Inadequate recertification or recertification based on incorrect data increases the risk of unauthorized access. Depending on the application, corporate data or intellectual property might be disclosed, manipulated or made inaccessible.	✓
Solution	The composition of authorizations down to the transaction level can be loaded into Garancy AIM in CSV format. This means that Garancy AIM reports can be generated down to the transaction level and thus serve as the basis for such a recertification.	**Can be resolved with Garancy AIM**

3.4 Individual Authorizations – No Verification

Problem	The review of the composition of authorization groups comprising individual rights is inadequate. BAIT 23 requires that authorizations be designed in accordance with the organizational and technical requirements of the institute. This means that there should be a review process, for example based on recertification, which regularly or on a case-by-case basis reviews the composition of the authorization groups to determine whether all individual rights contained are still required to fulfill the relevant specialist tasks.	**Classification**
Risk	Inadequate verification and securing of the authorization bundles increases the risk of excess authorization. Such excess access jeopardizes the confidentiality and integrity of shared systems, applications and data.	✓
Solution	The composition of authorizations down to the transaction level can be loaded into Garancy AIM in CSV format. This means that Garancy AIM reports can be generated and evaluated down to the transaction level. As part of role recertification, Garancy AIM provides information about the individual rights in the form of a hierarchy representation of each role to be recertified.	**Can be resolved with Garancy AIM**

3.5 Segregation of Duties – No Workflow for Rule Violations

Classification

Problem There is no documented procedure for dealing with and resolving segregation of duties violations identified by the IAM system. According to BAIT 28, the creation, modification, deactivation and recertification process must be documented in a transparent and analyzable manner. Recertification also indirectly includes the approval or resolution of segregation of duties violations. In order to avoid segregation of duties violations, AT 4.3.1 para. 1 also stipulates that appropriate transition periods (‘cooling-off’) are to be provided for when employees transfer from the sales / front office area to downstream areas and control functions that do not violate the prohibition of self-inspection and self-checking.

Risk Inadequate implementation of segregation of duties, including with regard to the handling of violations, carries the risk that individuals might acquire far-reaching powers that permit the misappropriation or manipulation of business-critical data and applications.

Solution The finding can be remediated by changing the process. Garancy AIM can provide evidence of how long it takes on average or in specific cases to correct segregation of duties violations using the TimeTraveler feature. This also indicates how the fix was implemented (for example, authorization withdrawal, special authorization, reclassification).

Garancy AIM can provide proof of remediation

3.6 Recertification – Undefined Time Intervals

Classification

Problem Recertification intervals are not defined for all applications. According to MaRisk AT 4.3.1 para. 2, IT authorizations, signatory powers and other competencies granted must be recertified regularly and as required within reasonable periods of time. The deadlines are based on the significance of the processes and, in the case of IT authorizations, the protection requirements of the information being processed.

Risk Regular recertification of all applications according to their level of criticality is necessary to prevent excess authorizations. Recertification thus serves the direct purpose of protecting corporate data with regard to confidentiality and integrity.

Solution If this finding applies, future releases of Garancy AIM will partially help with this issue by providing proof of which applications/users have been recertified in which time period. This helps to identify which applications have not yet been recertified or areas for which no set time intervals have been defined.

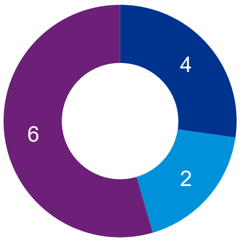
Garancy AIM can provide proof of remediation

Conclusion

Garancy AIM provides deep insights into the composition of various authorizations. This makes it possible to monitor all basic principles of authorization assignment with regard to whether authorizations are actually needed to fulfill certain functions and whether the principle of segregation of duties is being complied with. This monitoring can also include past events by means of historical reports. Key figures such as the average process duration or process flow can also be evaluated and optimized accordingly.

Insufficient control can lead to violations of the defined rules, requirements and principles that serve to protect the company from manipulation, embezzlement or sabotage.

Necessary process adaptations, especially in the context of recertification, cannot be implemented or proven with Garancy AIM. This might require adjustments to the workflow tool used, which means that proof must also be provided at this point. KPMG can support companies in adapting their processes.



🟦 Can be resolved with Garancy AIM   🟦 Garancy AIM can provide proof of remediation   🟪 Can be resolved via KPMG service

4. Super User

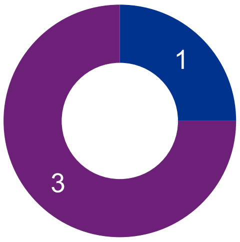
4.1 Authorization Evaluation – Undetectable Critical Authorizations

		Classification
Problem	Critical authorizations are not visible. According to BAIT 24, authorization concepts are required to define the scope and conditions of use of IT system authorizations in a way that is consistent with the determined need for protection and such that this can be completely and comprehensibly derived for all authorizations provided by an IT system.	
Risk	Users with critical authorizations can gain far-reaching authority within an organization if they are not adequately controlled. This poses the risk that individuals may manipulate, misappropriate and/or destroy business-critical data or intellectual property.	
Solution	Garancy AIM can directly correct this finding once a risk assessment has been performed in the IDM for each role, group and resource. The Garancy IAM Suite offers an end-to-end risk model for this purpose.	✓ Can be resolved with Garancy AIM

Conclusion

Garancy AIM allows you to monitor authorizations flagged as critical, such as those of a super user. This control is necessary to prevent individuals from gaining the power to interfere with business-critical processes by manipulating, disseminating or destroying data. In addition, critical authorizations should always be highlighted in an evaluation report.

Necessary process or governance adaptations cannot be implemented or proven with Garancy AIM. KPMG can support companies in adapting their processes or governance structure.



■ Can be resolved with Garancy AIM ■ Garancy AIM can provide proof of remediation ■ Can be resolved via KPMG service

5. Specifications for Authorization Modeling

5.1 Segregation of Duties – Possible to Create Business Roles that Violate Rules

Problem	Segregation of duties is not applied when creating authorization roles (i.e. it is possible to create business roles that contain conflicting groups from an SoD perspective). According to BAIT 24, companies must ensure that authorization concepts assign authorizations to users according to the need-to-know principle in order to uphold segregation of duties and avoid conflicts of interest of personnel.
Risk	If segregation of duties is not observed, this increases the risk that users may have been granted authorizations that give them critical power over corporate processes. For example, this could allow individuals to manipulate, delete or disseminate corporate data.
Solution	If this finding applies, Garancy AIM will be able to provide proof of the correction of this finding in a future release. For this purpose, the set of rules must be made available to Garancy AIM in a format that can be evaluated by Garancy AIM. The evaluation can become a complex affair if there are multiple ways in which SoD conflicts can occur (e.g. in each case resulting from the interplay of application designations, departments, MaRisk identifiers and locations).

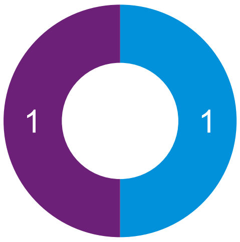
Classification

Garancy AIM can provide proof of remediation (in a future release)

Conclusion

Garancy AIM allows you to evaluate issues relating to segregation of duties. However, the prerequisite for this is that the corresponding authorizations have been marked according to a predefined SoD matrix, for example using respective labels, such that Garancy AIM can process these. When it comes to authorization roles, companies must define models in advance to ensure that authorizations are properly stored in the IDM system and can be evaluated in Garancy AIM. KPMG has already supported many customers and projects in the development of an integrated identity & access management concept. Moreover, as a cooperation partner of Beta Systems, KPMG can help with the necessary preliminary work if the initial situation matches the provider's skill set.

Necessary process or governance adaptations cannot be implemented or proven with Garancy AIM. KPMG can support companies in adapting their processes or governance structure.



🟦 Can be resolved with Garancy AIM 🟦 Garancy AIM can provide proof of remediation 🟪 Can be resolved via KPMG service

6. Authorization Concepts

6.1 Authorization Concept – Missing, Incomplete or Obsolete

Classification

Problem

The following items required for the further development and operation of applications are either missing, incomplete or not up to date:

- Technical specifications
- Documentation of the target state (specialist and technical design)
- Authorization concept
- Suitable testing concepts
- Definition of test objects
- Test case portfolio
- Operating manual

According to BAIT 24, authorizations are assigned to users based on the need-to-know principle, segregation of duties is maintained and conflicts of interest with staff are avoided.

Risk

Without documentation of the target state and the processes associated with the application, there is a risk that that the segregation of duties principle might be violated, the proper administration channels disregarded and authorizations assigned to users that do not match their actual needs. This increases the risk that users are granted authorizations that give them critical power over corporate processes. For example, this could allow individuals to manipulate, delete or disseminate corporate data. The failure to carry out tests or to carry them out inadequately can lead to operation downtimes due to unidentified errors. Worse, there is the risk that the integrity and confidentiality of data may be jeopardized by malicious functionalities put in place by developers or third parties.

Solution

If this finding applies, part of the proof that the finding has been corrected can be provided using Garancy AIM. If the documentation of the authorizations is implemented directly via the IAM system or in the target systems, an evaluation can be generated that provides a KPI of which attributes that require documentation have actually been documented and to what extent.

Garancy AIM can provide proof of remediation

6.2 Authorization Concept – NoTemplates

Problem	There is no template for authorization concepts. Authorization concepts may therefore differ greatly, depending on the motivation and knowledge of the creator. In order to be able to understand and implement the principle of authorization control and the associated rule processes in the respective systems and applications, it is necessary to create an authorization concept for the corresponding IT system. A template is essential to ensure that all relevant information for authorization control is available consistently in a viable format. This measure prevents a heterogeneous landscape from emerging.
Risk	If authorization concepts are documented inadequately – either in quality or scope – a well-founded strategy for assigning authorizations is not possible. This increases the risk that excessive authorizations might be granted.
Solution	If this finding applies, Garancy AIM can provide partial evidence of remediation. For example, it can be demonstrated that all authorizations in the IAM are documented consistently and that, for instance, authorization nomenclatures are being adhered to.

Classification

Garancy AIM can provide proof of remediation

6.3 Authorization Concept – No Nomenclature

Problem	There is no central specification of a content-based nomenclature that applies to the various business roles. To ensure that needs-based authorizations as required by BAIT are observed – including regular checks (as required in BAIT 23 in conjunction with BAIT 26 and 27) – it must be clearly recognizable to all relevant persons which functionalities are associated with the authorizations (for example the business roles). One of several measures that ensure compliance with this provision is to introduce a self-explanatory nomenclature.
Risk	A poorly worded or inadequate description of authorizations does not provide the foundation for making well-founded decisions during the request process or during each recertification cycle. This increases the risk that incorrect or excessive authorizations are requested, maintained or deleted.
Solution	An overview can be generated that indicates whether and which nomenclatures/categories correspond to the business roles.

Classification

Garancy AIM can provide proof of remediation

6.4 Authorizations – Inadequate Descriptions

Problem

Descriptions of authorizations are not precise enough to enable a qualified assessment in the context of request or recertification processes. MaRisk and BAIT stipulate that recertification must take place. In order to be able to qualify the authorizations to be evaluated, a clear description of the authorizations is needed. This description must be comprehensible to all actors involved in the recertification. The same applies to the assessment of authorizations in the request process.

Risk

Gaps in the request or recertification process can lead to excessive authorizations or may prompt staff to bypass the process because it is not suitable for everyday use. Both cases significantly increase the risk that corporate data or intellectual property may be misappropriated, manipulated or published by unauthorized individuals.

Solution

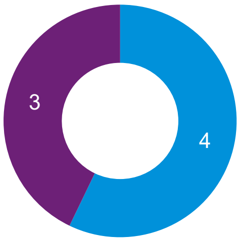
If this finding applies, Garancy AIM can provide partial evidence of remediation of this finding. It allows users to create an overview that lists, for example, the groups for which no description exists or whose description does not meet certain criteria (for example, date of creation/last update). Complete proof of implementation beyond these minimum objectives is only possible through the systematic manual review of the descriptions. To prepare for this, it would make sense to list and compare all descriptions according to type, category or other attributes.

Classification

Garancy AIM can provide proof of remediation

Conclusion

When it comes to content-based analysis of authorization concepts, Garancy AIM can, in many cases, provide evidence as to whether and in what quality the contents of authorization concepts are available, especially as regards the description of authorizations. Prior to this, however, a comprehensive identity & access management governance scheme must be established, documented, subjected to undergo quality assurance checks and used in live operation. KPMG is highly experienced in this field and can thus provide expert support.



■ Can be resolved with Garancy AIM 🟦 Garancy AIM can provide proof of remediation 🟪 Can be resolved via KPMG service

Findings that Can Be Remedied by Means of a KPMG Service

Findings not related to Garancy AIM can be corrected with the aid of a KPMG service. This challenge is tackled by taking a holistic approach to identity & access management in order to align the specialist and organizational/technical aspects with one another. For example:

- Specialist side: Identification of specialist requirements, support in mapping SoD requirements and business roles

- Technical side: Integration of IAM systems into an existing IT landscape and subsequent transfer to operations; orchestration of authentication, request workflows, rule engine, rights administration, provisioning, recertification

- Organizational side: Definition and introduction of governance, processes and responsibilities; communication and control of the various contacts; implementation of interface functions; 'translation' of specialist requirements into concepts and technology

KPMG can provide the following support using the example of Finding 1.21 (see next page):

It is often found that the technical system-related responsibilities for applications are not clearly documented and not observed in daily business operation. For example, necessary information does not exist for authorization assignment, recertification or role design. There is thus the risk that required authorization monitoring does not take place in the respective system, which may lead to excess authorizations. As a result, companies are not adequately protected against misuse and/or manipulation.

In general, the definition and description of responsibilities relating to identity & access management (AM) tasks and activities must be considered a prerequisite for setting up effective authorization management. This holds true regardless of the technical maturity level of the corporate IAM solution. The basic toolkit comprises an AM guideline, the definition of standard 'Responsibilities in AM' as well as the 'AM process manual'. This also includes the definition and documentation of system responsibilities, as this information is imperative to ensure that the respective recertifications are performed without any gaps.

As regards Finding 2.3 (see next page), KPMG's solution may look as follows:

It is fairly common for companies to assign highly privileged user accounts to entire teams. As a result, it is not possible to attribute an action to a specific employee. This carries the risk of the highly privileged user being misused or abused. Such misuse endangers the availability, integrity and confidentiality of accessible corporate data. If there is no feasible technical solution, a process instruction should be drawn up which prohibits the use of highly privileged users by multiple individuals. The respective assignment and use by an employee can be recorded and controlled by means of documentation. In addition, a guideline should include the requirement that each highly privileged user be assigned unique responsibilities.

If you are interested in further solution concepts or would like a workshop on the subject, please do not hesitate to contact us.

Findings		
1.18	There is no process for blocking all authorizations of an employee who is absent (from performing duties) for a longer period of time.	1 Access Administration
1.19	There are no uniform request procedures.	
1.20	Requested access rights are entered into the IT systems without systematic verification.	
1.21	Technical system-related responsibilities for applications are not clearly documented and not observed in daily business.	
2.3	Highly privileged user accounts can be used by entire teams. As a result, is not possible to attribute an action to a specific employee.	2 Identification and Authentication
2.4	It cannot be conclusively determined how many people know the password for technical user accounts in the company.	
2.5	The requirements specified in the password policy are inadequate.	
2.6	A regular password change is not enforced.	
2.7	There is no individual assignment of the initial password (e.g. current month, current season, company).	
3.7	The activities of the technical user accounts set up in the IT system with extensive authorizations are not regularly monitored.	3 Monitoring
3.8	Technical user accounts are not included in the recertification process.	
3.9	Recertification does not extend to access rights granted temporarily or in test environments.	
3.10	The composition of the business roles, their assignment rules and the user accounts authorized without adhering to assignment rules are not recertified at regular intervals.	
3.11	Not all actors of the authorization request procedure are involved in the recertification process.	
3.12	It cannot be guaranteed that the actual state in the system corresponds to the target state defined in the IAM tool. There are no regular consistency maintenance checks and no guidelines on how to deal with deviations.	
4.2	Passwords of highly privileged user accounts can be changed by individual employees without the knowledge of other employees or without applying the dual-control principle.	4 Super User
4.3	There is no mechanism to ensure that the use of a privileged generic user account will be terminated after a reasonable period of time, such as four hours.	
4.4	The requirement to use personalized administrator user accounts where possible is not observed.	

Findings		
5.2	There are no overarching guidelines for role modeling or guidelines/processes on how authorization groups are created and they undergo quality assurance checks.	**5 Authorization Modeling Guidelines**
6.5	There is no complete, central overview of all used applications. Therefore, it cannot be guaranteed that all applications are adequately controlled via access rights management.	**6 Authorization Concepts and their Contents**
6.6	The processes for identity & access management (in particular for requesting and approving authorizations) are not described in any company-wide guideline or process manual.	
6.7	The authorization concepts do not regularly undergo quality assurance checks.	

Your Contacts

KPMG AG
Wirtschaftsprüfungsgesellschaft
The SQUAIRE/Am Flughafen
60549 Frankfurt, Germany

Beta Systems IAM Software AG
Alt-Moabit 90 d
10559 Berlin, Germany

Hans-Peter Fischer
Partner,
Consulting – Cyber Security
T +49 69 9587-2404
hpfischer@kpmg.com

Detlef Sturm
Senior Business Consultant
T +49 30 726118-557
detlef.sturm@betasystems.com

Saskia Behrend
Senior Manager,
Consulting – Cyber Security
T +49 69 9587-4802
sbehrend@kpmg.com

www.kpmg.de

www.kpmg.de/socialmedia

The information contained herein is of a general nature and does not address the specific situation of any individual or legal entity. Although we endeavor to provide reliable and up-to-date information, we cannot guarantee that this information is as accurate as it was at the time it was received or that it will continue to be so in the future. You should not act on this information without appropriate professional consulting and a thorough analysis of the situation in question.