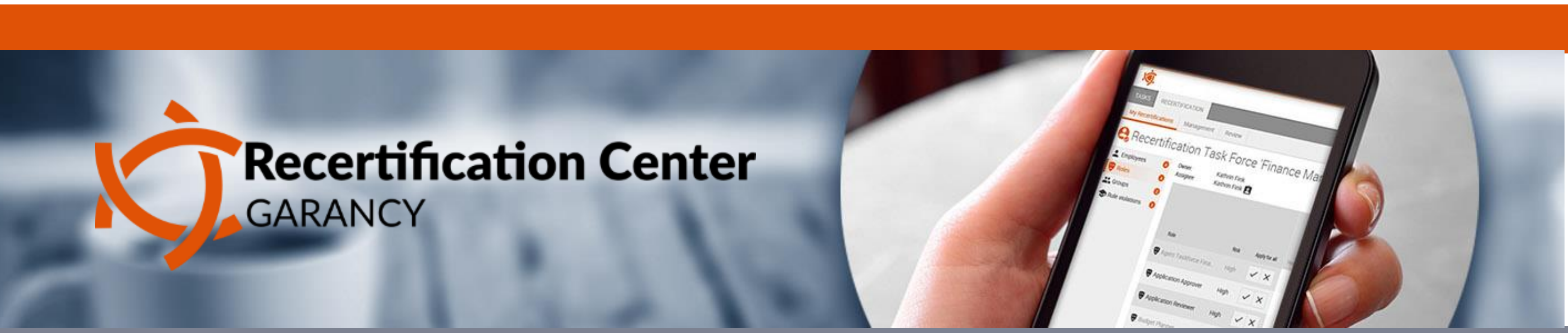
Datasheet

Recertification Center
GARANCY



Certified Access Rights – Reliably up to date

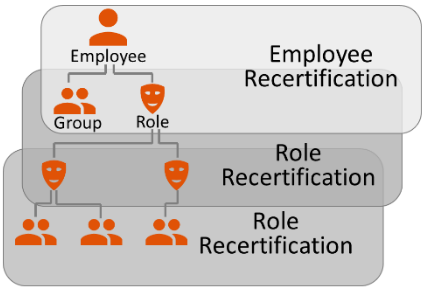
A significant share of regulations and legal standards require a recurring review of all access rights for all users. Such recertification ensures, that managers periodically confirm their team members job-related need for the granted IT access rights.

This ensures, that all users are just equipped with access rights that are needed to perform their tasks. The compliance with this need-to-know principle raises the information security as well as data privacy significantly.

Advantages:

- Compliance with many regulations
- Elaborated data privacy and data protection
- Increased efficiency and lower costs for the access right management

The Garancy Recertification Center allows company-wide recertification campaigns. In such campaigns, selected users are presented with their access rights to their managers for inspection and confirmation. If a manager rejects a previously granted access right, this entitlement will be automatically revoked.



This employee recertification covers users and all access groups and roles they are directly assigned to, since such assignments can be assessed by business managers.

In order to recertify the entire entitlement spectrum from the person down to the lowest level access right, Recertification Center also provides separate recertification campaigns for role structures. In these Role Recertification campaigns, managers are asked to validate and to potentially correct the attributes and the content of their role structures.

Features and Functions

Employee Recertification

- ✓ Configuration of recertification campaigns by affected organization unit, job functions or certain managers
- ✓ Recertification conducted by line managers, business managers or the owners of roles and groups
- ✓ Optional Bulk Recertification
- ✓ Limitation of campaigns to certain access rights basec on e.g. risk scores
- ✓ Optional transfer of employees from a campaign to a different manager in case of wrong assignments
- ✓ Display of users to be recertified in a per-user listing or as a user-comparing cross table

Role Recertification

- ✓ Recertification of role structure and role attributes
- ✓ Recertification conducted by the owner of the affected role and by the owner of the entitlements, contained in the affected role.
- ✓ Graphical display of role hierarchies

Recertification History

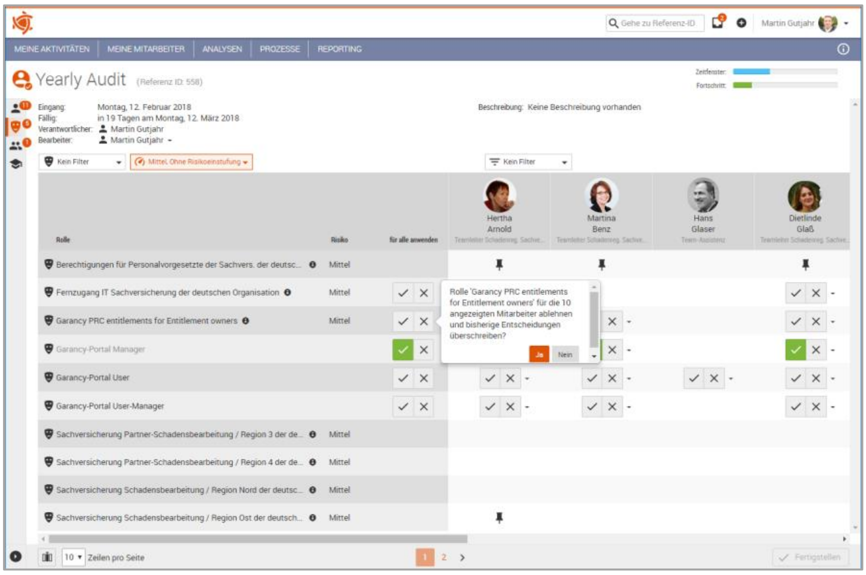
- ✓ Per Recertification Campaign
- ✓ Per Employee
- ✓ Per Role

General Features

- ✓ Easy-to-use configuration of revolving campaigns
- ✓ Start of ad-hoc campaigns
- ✓ Campaign design with various options concerning process details and scope of the recertification
- ✓ Export and Import of recertification designs
- ✓ Overview on ongoing recertification campaigns with details concerning the campaigns progress
- ✓ Assume tasks by appointed substitutes
- ✓ Delegation of campaigns to other managers
- ✓ Automated deprovisioning of rejected access rights
- ✓ Audit reports for the results of each campaign
- ✓ Delegation report for each campaign
- ✓ 100% integration with Garancy IDM
- ✓ Quick start by fast and comprehensible configuration
- ✓ Easy adaptation to Corporate Design guidelines
- ✓ Auditability of campaigns by preserving historic data
- ✓ E-Mail notification for all people involved in the process
- ✓ Web application / HTML5
- ✓ Support of SSO based on KERBEROS
- ✓ Multi-language support

Product Details

Your perfect support for compliance audits with Recertification Center
Recertification Center allows the configuration of ad-hoc as well as revolving recertification campaigns. Supporting Employee- and Role Recertifications, the legally often required 'consistency' of a recertification, from the person down to his individual access groups, is ensured. The split into different recertification layers provides an optimized scope for every recertifying manager. From the business oriented assessment of a person and his directly assigned roles to the more technical aspects of the role components - every recertifier is only engaged in those parts of the entitlement tree, he is familiar with.



Yearly Audit (Referenz ID: 558)

Eingang: Montag, 12. Februar 2018
Fällig: in 19 Tagen am Montag, 12. März 2018
Verantwortlicher: Martin Gutjahr
Bearbeiter: Martin Gutjahr

Beschreibung: Keine Beschreibung vorhanden

Rolle	Risiko	für alle anwenden	Hertha Arnold Teamleiter Schadenreg. Sachve...	Martina Benz Teamleiter Schadenreg. Sachve...	Hans Glaser Team-Assistenz	Dietlinde Glaß Teamleiter Schadenreg. Sachve...
Berechtigungen für Personalvorgesetzte der Sachvers. der deutsc...	Mittel		📌	📌		📌
Fernzugang IT Sachversicherung der deutschen Organisation	Mittel	✓ ✕				✓ ✕ -
Garancy PRC entitlements for Entitlement owners	Mittel	✓ ✕		✕ -		✓ ✕ -
Garancy-Portal Manager		✓ ✕		✕ -		✓ ✕ -
Garancy-Portal User		✓ ✕	✓ ✕ -	✓ ✕ -	✓ ✕ -	✓ ✕ -
Garancy-Portal User-Manager		✓ ✕	✓ ✕ -	✓ ✕ -		✓ ✕ -
Sachversicherung Partner-Schadensbearbeitung / Region 3 der de...	Mittel					
Sachversicherung Partner-Schadensbearbeitung / Region 4 der de...	Mittel					
Sachversicherung Schadensbearbeitung / Region Nord der deutsc...	Mittel					
Sachversicherung Schadensbearbeitung / Region Ost der deutsch...	Mittel		📌			

Rolle 'Garancy PRC entitlements for Entitlement owners' für die 10 angezeigten Mitarbeiter ablehnen und bisherige Entscheidungen überschreiben?

Ja Nein

Employee-Recertification reviews directly assigned entitlements of a recertified person. The questions, which access rights and which employees are subject to a recertification are configured in every recertification campaign individually. This concept allows the creation of most specific campaigns, like periodic reviews of elevated risk holders besides global campaigns like the corporate recertification of all users and access rights on an annual basis.

Role-Recertification reviews the content of a role. This recertification covers the contained entitlements (role in role / group in role) as well as all attributes of a role like its risk rate, or its responsible managers.

Both recertification types contain the option to consider and display existing SoD conflicts and to confirm such violations in the recertification or solve the conflict by the rejection of some access rights.

In order to reduce the manager's efforts for the recertification to a minimum, a bulk-recertification can be configured, that allows the one-click confirmation of all access rights that have been recertified in the last campaign already.

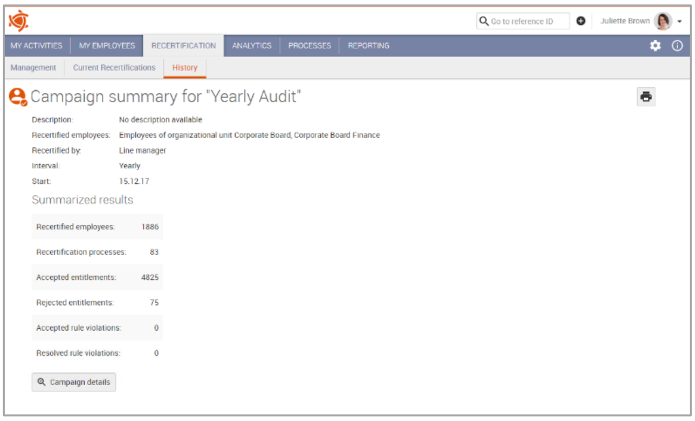
Additional Modules
Garancy Portal acts as the gateway to further modules, which enriches the feature set of Recertification Center

- ***User Center (USC)***
  Standard workflows to support the User-Life-Cycles.- On-/Offboarding, Transfer, Requests
- ***Access Intelligence Manager (AIM)***
  Business Intelligence-based, interactive Analytics of enterprise-wide access data

Recertification Views
Besides the tabular view on a person and his entitlements, the assessment of employee access rights is facilitated by the use of cross-tables. The direct comparison of entitlements of different users displays their deviations and conformities and helps the recertifying manager concerning the assessment of need-to-know aspects.

Results of a Recertification
After finalizing a recertification campaign, the rejected access rights are automatically deprovisioned without the need for any further manual interaction.

All results are summarized by campaign, allowing auditors to see at a glance how many employees have been recertified and how many entitlements were rejected or confirmed.
This campaign summary provides a perfect entry point for further analytics of recertification campaigns. E.g. recertification tasks could be challenged, that combine a high confirmation rate with a minimum handling time.



Campaign summary for "Yearly Audit"

Description: No description available
Recertified employees: Employees of organizational unit Corporate Board, Corporate Board Finance
Recertified by: Line manager
Interval: Yearly
Start: 15.12.17

Summarized results

Recertified employees:	1886
Recertification processes:	83
Accepted entitlements:	4825
Rejected entitlements:	75
Accepted rule violations:	0
Resolved rule violations:	0