TIMETOACT GROUP
SOFTWARE & CONSULTING

Customer Case Study

Neue Rezertifizierungslösung von FI-TS zur Erfüllung von Governance- und MaRisk-Anforderungen

Mit Unterstützung der TIMETOACT GROUP gelang es dem IT-Dienstleister, die Qualität der Berechtigungs-rezertifizierung auf eine neue Stufe zu heben.

Als zentraler IT-Dienstleister der Sparkassen-Finanzgruppe bietet die Finanz Informatik den kompletten IT-Service – von Anwendungsentwicklung über Infrastruktur- und Rechenzentrumsbetrieb bis hin zu Beratung, Schulung und Support. Dabei wird sie vom Tochterunternehmen Finanz Informatik Technologie Service (FI-TS) unterstützt, dem größten IT-Dienstleister für Landesbanken. Ihre 1.000 Beschäftigten arbeiten täglich in den IT-Systemen der Finanzinstitute, der Finanz Informatik sowie in eigenen Systemen – ein hochsensibler Bereich, in dem klar geregelt sein muss, wer welche Rechte zur Administration der jeweiligen Software hat. Die von FI-TS betreuten Finanzinstitute unterliegen den entsprechenden aufsichtsrechtlichen Anforderungen, insbesondere den Mindestanforderungen an das Risikomanagement, abgekürzt MaRisk, der BaFin (BA), deren Erfüllung auch regelmäßig behördlich überprüft wird. Die Finanzinstitute sind verpflichtet, diese Regularien an ihre Subunternehmer weiterzugeben, sodass FI-TS alle Leistungen, auch den Zugriff auf Software, aufsichtsrechtlich konform zu erbringen hat.

Für das interne Berechtigungsmanagement kommt seit mehreren Jahren eine spezielle Identity-Access-Governance (IAG)-Software zum Einsatz. „Die Zugriffsberechtigungen sind jedoch nicht in Stein gemeißelt", weiß Christian Rothlauf: „Sie müssen im Zuge strenger werdender Governance-Vorgaben vielmehr regelmäßig überprüft werden." Aus diesem Grund findet eine sogenannte Rezertifizierung statt. Sie stellt sicher, dass jeder Nutzer der IT-Systeme in diesen zu jedem Zeitpunkt nur genau die Berechtigungen hat, welche zur Durchführung seiner Aufgaben notwendig sind, wobei das Sparsamkeitsprinzip (Need-to-know) angewendet wird. Dabei prüfen die Führungskräfte für jeden der ihnen zugeordneten Beschäftigten, welche Berechtigungen er behalten kann und welche zu entziehen sind. Ebenso werden Rollen, in denen mehrere Rechte gebündelt sind, rezertifiziert. Es muss also geprüft werden, ob jede Rolle zu jedem Zeitpunkt auch die richtigen Rechte enthält.

Rezertifizierung per Excel unübersichtlich und fehleranfällig

Solche Rezertifizierungen führt FI-TS im halbjährlichen Turnus durch. Dafür nutzt sie die Software Nexis Controle, implementiert durch ihren Projektpartner, die Business Unit IAG (Identity & Access Governance) der TIMETOACT Software & Consulting GmbH. Mit ihr wurde die bisherige Excel-basierte Arbeitsweise ersetzt und auf die heutigen fachlichen Anforderungen hin zugeschnitten. Zuvor war nicht zwingend sichergestellt, dass die Führungskräfte bzw. Rechteverantwortlichen im Zuge ihrer Bestätigung tatsächlich alle Rechte sehen. Governance-Richtlinien fordern jedoch einen technischen Nachweis darüber, dass die Führungskraft auch das letzte Excel-Tabellenblatt gesichtet und in der Tabelle bis ganz nach unten gescrollt hat. Ein weiterer Nachteil Excel-basierten Arbeitens: Nicht alle User-Typen werden vollständig rezertifiziert. Man unterscheidet zwischen persönlichen und technischen Usern sowie verschiedenen Klassen. Die MaRisk fordert hier Vollständigkeit: Alle Berechtigungen müssen geprüft werden.

Umfassende Rezertifizierung: Exklusiv- und Zwillingsrollen sowie User ohne Account

Mit ihrer neuen Rezertifizierungssoftware kann FI-TS die beschriebenen Anforderungen erfüllen. Sie ermöglicht unter anderem auch eine Rezertifizierung von Exklusivrollen, wie sie

finanz **informatik** **technologie** service

FI-TS ist innovativer IT-Partner für Unternehmen aus dem Finanz- und Versicherungssektor.

Branche:	IT Services für Banken, Versicherer und Finanzdienstleister
Mitarbeiter:	ca. 1000
Standorte:	Haar bei München (Hauptsitz), Hannover, Nürnberg, Offenbach und Fellbach bei Stuttgart

Standort Haar bei München ©FI-TS

das IAG-System von FI-TS kennt. Solche Rollen werden zur Steuerung von Attributen bei Beschäftigten genutzt. Es lassen sich außerdem auch solche User rezertifizieren, die keinerlei Accounts haben.

Für die temporäre Aktivierung von Rechten verwendet FI-TS das sogenannte HPU-Verfahren (hochprivilegierte User). Dabei wird eine bestimmte Berechtigungsrolle normal beantragt, mit der jedoch zunächst keine Rechte verbunden sind. Über einen separaten Workflow kann man diese Rechte dann aktivieren und der User erhält eine sogenannte Zwillingsrolle. Auch diese spezielle Rechtekonstellation vermag die neue Rezertifizierungslösung abzubilden. Architektonisch als Web-Applikation konzipiert, arbeitet es mit einem universell einsetzbaren Datenmodell. Dieses bildet die Entitäten eines normalen IAG-Systems ab.

Nexis Controle verknüpft Drittsysteme mit der IAG-Software

Die Daten aus der IAG-Lösung (Garancy IAM der Beta Systems Software AG), in der alle Rollen und User, Verantwortlichen und Organisationsstrukturen enthalten sind, können somit einfach in die Rezertifizierungslösung übertragen werden. Nächtlich werden sie exportiert und lassen sich an der Schnittstelle nochmals anpassen, aggregieren oder filtern. So wird das Konstrukt mit Zwillingsrollen und HPU-Rechten elegant abgebildet. Auch Systeme von FI-TS, die nicht mit der IAG-Software kommunizieren, liefern Daten sämtlicher Accounts und Berechtigungen an die Zertifizierungslösung. Diese verknüpft sie mit der IAG-Lösung und findet damit die zuständige Führungskraft. Die integrative Verbindung zwischen den einzelnen Systemen hat TIMETOACT für FI-TS geschaffen.

Schon bei der ersten Rezertifizierung zeigte sich, wie die MaRisk-Anforderung der Vollständigkeit bei FI-TS gelöst wird: Im neuen System sieht die Führungskraft immer nur einen bestimmten Ausschnitt, kann für die dort angezeigten Objekte eine Entscheidung treffen und muss dann weiterklicken. So ist sichergestellt, dass für wirklich jeden Beschäftigten und seine Rechte und Rollen aktiv eine Entscheidung getroffen wird. Dank der Flexibilität des Herstellers Nexis Controle gelang es dem Team von TIMETOACT, aktuelle Anforderungen des Kunden sehr schnell umzusetzen und neue Features binnen weniger Wochen im Standard einsatzfähig zu machen. Projektleiter Christian Höfs: „Die Software erfordert quasi keine Programmierung, sondern kommt mit reiner Konfiguration in der Oberfläche und dem Zusammenklicken von Einstellungen aus. Darüber lässt sich granular steuern, was rezertifiziert und angezeigt werden soll."

Weiterer Schritt von FI-TS zur Erfüllung der BaFin Anforderungen im Berechtigungsmanagement

- Mit der Implementierung von Nexis Controle für die Rezertifizierung durch das IAG-Team der TIMETOACT GROUP arbeitet FI-TS beim Berechtigungsmanagement konform zu den Regularien der Branche.
- Vollständigkeitsprinzip wird durch ein zweistufiges Rollenmodell mit Fach- und Komponentenrollen erfüllt.
- Ständige Aktualisierungen der Rezertifizierung durch permanenten Abgleich mit der IAG-Software statt stichtagsbezogenes Arbeiten
- Besserer Überblick bei der Prüfung von Nutzerrechten und Rollen erhöht insgesamt die Rezertifizierungsqualität.
- Potenzial für weiteren Einsatz der Rezertifizierungssoftware für die Rollenmodellierung.

TIMETOACT GROUP
SOFTWARE & CONSULTING

Die TIMETOACT GROUP umfasst acht Unternehmen mit über 550 Mitarbeitern an 13 Standorten in Deutschland, Österreich und der Schweiz.

Die Unternehmen der TIMETOACT GROUP – ARS, CLOUDPILOTS, edcom, GIS, novaCapta, synaigy, TIMETOACT, X-INTEGRATE – erbringen Leistungen in den Bereichen Digital Workplace, Business Process Integration & Automation, Mathematical Optimization, Data Warehouse & Governance, Business Intelligence und Predictive Analytics, Identity & Access Governance sowie Commerce und Customer Experience.

Ihr Ansprechpartner:

Karl-Heinz Masser
Head of IAG Sales &
Partner Management

+49 172 3093037
karl-heinz.masser@timetoact.de

www.timetoact-group.de