FSP

Praxisbericht

Aufbau der IAM Governance und -Prozesse zur Abdeckung von VAIT-Anforderungen

Wie ein Versicherungskonzern erfolgreich das Identity & Access Management für die gesamte Unternehmensgruppe vereinheitlicht

Der Kunde: Konzern mit mehreren Millionen Versicherten

Das Kundenunternehmen zählt zu den großen Erstversicherungskonzernen auf dem deutschen Markt. Zur inländischen Gruppe des international agierenden Konzerns gehören mehrere namhafte Versicherungen.

Nachhaltige Compliance sichert das Vertrauen

Die Unternehmen der Versicherungsgruppe in Deutschland haben den Anspruch, ihre Geschäfte verantwortungsvoll und jederzeit in Übereinstimmung mit den gesetzlichen Bestimmungen zu führen. Nachhaltiges Compliance Management in der Gruppe soll Vertrauen bei Kunden und Partnern sicherstellen.

Zudem haben die Gesellschaften des Konzerns verschiedene Regelungen verabschiedet, mit deren Hilfe die Mitarbeiterinnen und Mitarbeiter bei der Einhaltung der zunehmend anspruchsvolleren gesetzlichen Anforderungen unterstützt werden.

Vereinheitlichung von IAM und VAIT für die gesamte Gruppe

Aufgrund der Historie der Konzernunternehmen existiert ein verstreutes IAM-Umfeld. Für zentrale wie dezentrale Systeme und ihre komplexen Berechtigungsprozesse und -strukturen galt es, im Rahmen der Maßnahme eine einheitliche Governance zu stellen, Prozesse zu optimieren und dabei die IAM Guideline des Headoffice zu berücksichtigen. Die grundlegende Anforderung bestand darin, alle Aspekte des IAM und der VAIT zum Benutzerberechtigungsmanagement abzudecken. Entscheidend dabei war es, den Aufbau einer vereinheitlichten IAM-Verantwortung ins Leben zu rufen und als zentrales IAM-Team zu etablieren. Dabei wurde die komplette IAM-Organisation der Gruppe beleuchtet und überprüft.

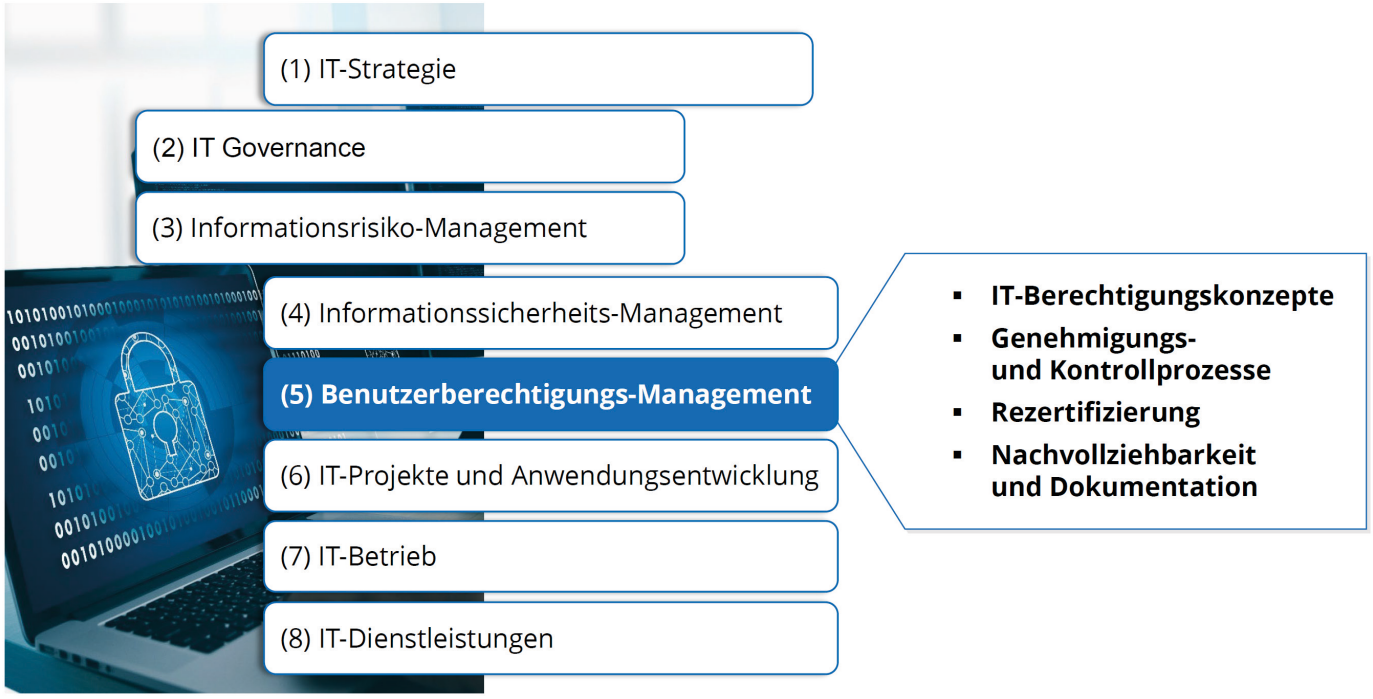
Unser Auftrag

FSP unterstützte das Projekt in der Rolle des Fachspezialisten für das Identity & Access Management. Die Aufgabe bestand darin, die vorhandenen Prozesse des Unternehmens zu analysieren, mit den Anforderungen der VAIT abzugleichen und die notwendigen Maßnahmen abzuleiten und umzusetzen.

Exkurs VAIT: Gesetzliche Regeln zur IT-Sicherheit in der Finanzwirtschaft

Unternehmen der Finanzbranche müssen zum Schutz von Daten und IT-Systemen zahlreiche Regelungen einhalten. Außer DSGVO und IT-Sicherheitsgesetz sind Anforderungen aus BAIT, VAIT und KAIT umzusetzen. Diese Verwaltungsvorschriften der BaFin geben den Rahmen für die technisch-organisatorische Ausstattung der IT in den Unternehmen der deutschen Finanzwirtschaft vor.

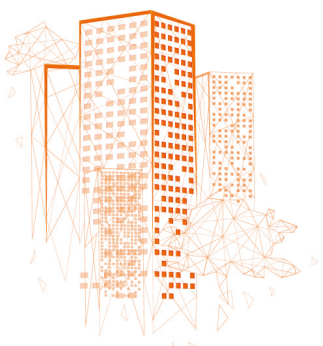
Handlungsfelder VAIT



Im Rahmen der Anwendungsentwicklung müssen nach Maßgabe des Schutzbedarfs angemessene Vorkehrungen im Hinblick darauf getroffen werden, die Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität der zu verarbeitenden Daten nachvollziehbar sicherzustellen.

Geeignete Vorkehrungen können sein:

- **Prüfung der Eingabedaten**
- **Systemzugangskontrolle**
- **Nutzer-Authentifizierung**
- **Transaktionsautorisierung**
- **Protokollierung der Systemaktivität**
- **Prüfpfade (Audit Logs)**



Anforderungen der VAIT am Beispiel Benutzerberechtigungsmanagement

„Das Unternehmen hat ein Benutzerberechtigungsmanagement einzurichten. Dieses muss sicherstellen, dass Berechtigungen so ausgestaltet sind und genutzt werden, wie es den organisatorischen und fachlichen Vorgaben des Unternehmens entspricht.

Es ist ein Berechtigungskonzept schriftlich festzulegen. Im Hinblick auf die Vergabe von Berechtigungen an Benutzer hat dieses Konzept sicherzustellen, dass jeder Mitarbeiter nur über die Rechte verfügt, die er für seine Tätigkeit benötigt. Auch das trägt zur Verbesserung des IT-Risikobewusstseins bei. Dies gilt auch für den Rezertifizierungsprozess, in dem die eingeräumten Berechtigungen regelmäßig überprüft werden.

Dies ermöglicht es, Abweichungen von den genannten Maßgaben zu identifizieren und Berechtigungen gegebenenfalls anzupassen.“

- **BAIT/VAIT/KAIT schreibt unternehmensweites Rollenmodell vor**
- **Manuelle Berechtigungs-administration erfordert präzise Anforderungen**
- **Rezertifizierung der Berechtigungen**

- **Rollenmodell teilweise vorhanden**
- **Ist der Beantragungsprozess für Berechtigungen transparent und nachvollziehbar?**
- **Wie werden Rezertifizierungen durchgeführt und wird vollständig rezertifiziert?**

Unternehmensweites Rollenmodell mit

- **Organisationsstruktur**
- **fachlichen und technischen Rollen**
- **fachlichen und technischen Zuständigkeiten**
- **Rezertifizier- und Auditierbarkeit**

Vorgehen und Lösung zur Vereinheitlichung der IAM Governance

Im Projekt galt es nicht nur, eine effiziente und VAIT-konforme IAM Governance zu etablieren. Vielmehr waren auch bestehende Prozesse zu optimieren und ein einheitlicher Sprachgebrauch sicherzustellen.

Ein IAM-Glossar für alle Konzernunternehmen

IAM wurde bisher verstreut in der Unternehmensgruppe betrieben. Viele Beteiligte haben daher mit unterschiedlichen Begriffen über dasselbe geredet.

Um hier die notwendige Klarheit und ein gemeinsames Verständnis herzustellen und auch Missverständnisse zu vermeiden, musste zunächst ein einheitlicher Sprachgebrauch entwickelt werden. Dabei wurden Begrifflichkeiten angeglichen sowie ein zentrales IAM-Glossar und eine zentrale IAM-Dokumentation als Einstiegsseite im Intranet des Kunden aufgebaut. Mit fortlaufendem Projektfortschritt befüllten die Projektbeteiligten diese Dokumentationsseite sukzessive mit den notwendigen und hilfreichen IAM-Informationen.

Dies umfasste das Glossar, die Darstellung sämtlicher Prozessgebiete des IAM und die gültigen IAM-Organisations- und Rollenbeschreibungen des Auftraggebers.

Etablierung der IAM Governance

Das Projektteam entwickelte ein Rollenkonstrukt für die IAM-Organisation. Dafür war es erforderlich, die Anforderung der IAM Guideline des Headoffice zu berücksichtigen. Sämtliche VAIT-Aspekte zum Benutzerberechtigungsmanagement mussten abgedeckt werden.

Im Mittelpunkt standen dabei z. B. die Sicherstellung des Zusammenspiels mit den dezentralen Businesskomponenten wie etwa SAP sowie die Integration der an IT-Dienstleister ausgelagerten Systeme in die übergreifenden IAM-Prozesse.

Für Systeme mit einem integrierten IAM wurden beispielsweise Genehmigungsverfahren zur Sicherstellung der IAM-Anforderungen und dezidierte Berechtigungskonzepte etabliert.

Für sämtliche sich aus dem Rollenkonstrukt ergebenden Rollen erfolgten Beschreibungen mit der Definition der jeweiligen Aufgaben und Verantwortlichkeiten. Die Etablierung in der Linie – z. B. mit Einweisungen und Rollenschulungen – war ebenso Aufgabe des Projektteams.

Die Neumodellierung und Umsetzung der IAM-Prozesse

Sämtliche IAM-Prozesse wurden erhoben und für die relevanten Standardprozesse wie Eintritt, Änderung, Austritt sowie Rezertifizierung und Kontrolle auf Basis der Modellierungsrichtlinien des Unternehmens neu modelliert. Im Anschluss startete die Umsetzung der definierten und abgestimmten Sollprozesse.

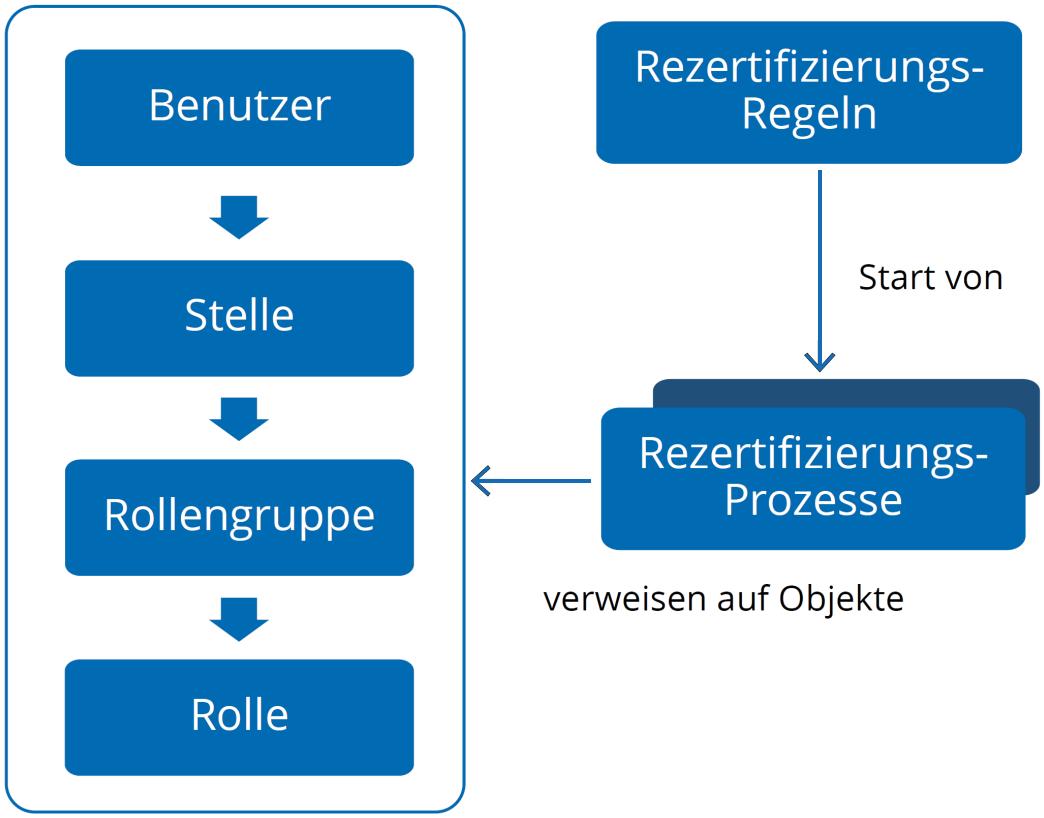
Beispiel 1: Nachvollziehbarkeit der Berechtigungsvergabe

Nach erfolgter Bedarfsanalyse wurden Optimierungen in der Linie zur toolunterstützten Steuerung und Dokumentation der Berechtigungsbeantragungen und -vergaben angestoßen.

Beispiel 2: Rezertifizierung

Die Rezertifizierung wird für alle kritischeren Systeme gemäß ihres Schutzbedarfs und in Abhängigkeit der Kritikalität der Berechtigungen in den von der VAIT vorgeschriebenen Zyklen durchgeführt.

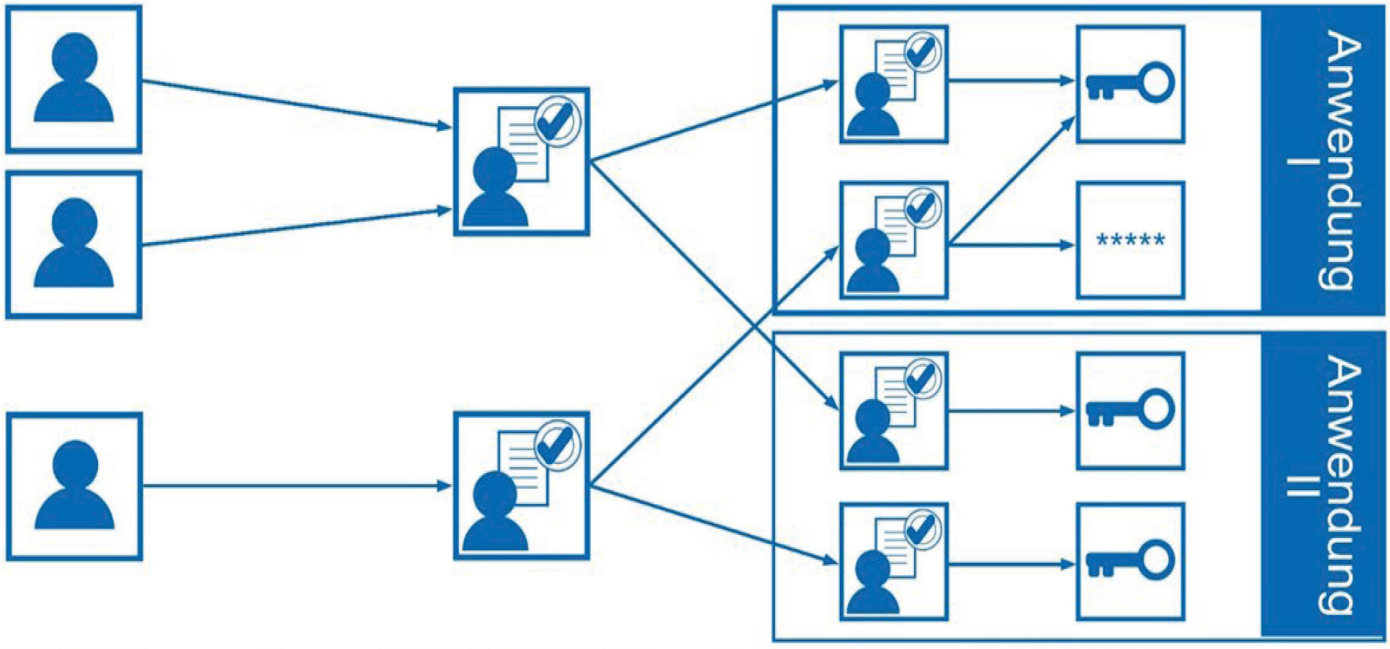
Handlungsfelder VAIT



Der Weg zu erfolgreichen Berechtigungskonzepten

Anhand einer mittelfristigen Roadmap wird derzeit die Erstellung der Berechtigungskonzepte für ca. 300 der insgesamt 650 Anwendungen der Gruppe durchgeführt. Mittels eines standardisierten Templates werden sämtliche Aspekte der VAIT berücksichtigt und abgefragt. Dabei gilt es nicht nur die individuellen Berechtigungsregeln zu dokumentieren, sondern auch die Einbettung in die IAM-Landschaft zu beachten.

Allgemeiner Ansatz zur Rollenmodellierung



BENUTZER

Fachliche Rollen je Fachbereich

Owner: Fachbereiche

Quelle: Top-down

Technische Rollen je Anwendung

Owner: AE

Quelle: Bottom-up

Zu schützende Objekte

Zwecks transparenter Dokumentation wurde ein Zentralregister zur Ablage der erstellten Berechtigungskonzepte aufgebaut. So können definierte Kontrollprozesse der IAM-Governance, z. B. für jahresbezogenene Checks, durchgeführt und zentral dokumentiert werden.

Die wichtigsten Highlights und Ergebnisse auf einen Blick

Analyse und Umsetzung der VAIT-Anforderungen erfolgt

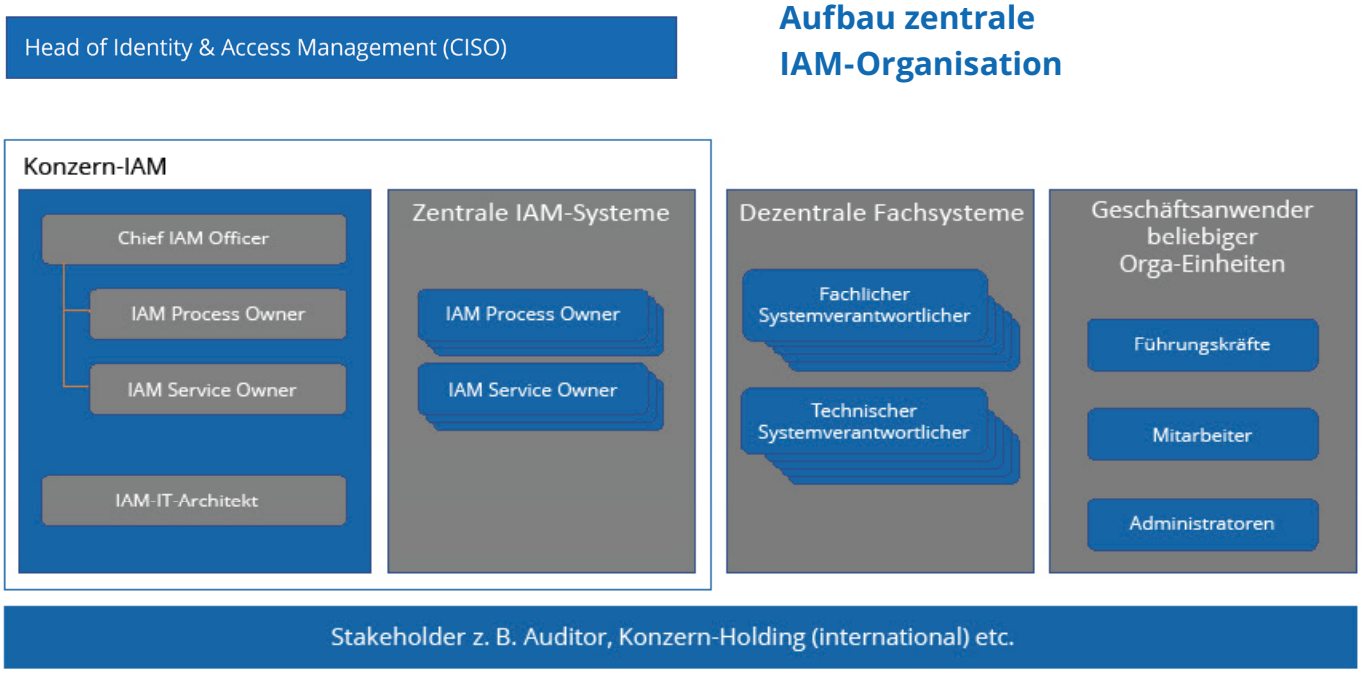
Entwicklung einer zentralen IAM-Organisation mit Process Owner und Service Owner für das Gesamt-IAM inklusive eines übergreifenden IAM-Architekten sowie für jede IAM-Plattform (z. B. div. Benutzerberechtigungssysteme, RACF, Windows AD, SAP etc.)

Etablierung der Plattform-Process-Owner und Plattform-Service-Owner sowie Integration der bereits bestehenden Rollen der fachlichen und technischen Systemverantwortlichen

Zentrales IAM-Team unter der Gesamtverantwortung des IT Security Officers (CISO) sowie des Chief Identity Accessmanagement Officers etabliert

Verankerung in der Linie durch Entwicklung der Aufgabenbeschreibungen der neuen Rollen sowie Einweisung zu den anstehenden Aufgaben für die übergreifenden IAM-Prozesse

Aufbau zentrale IAM-Organisation



Fazit

Die umfassende Dokumentation führte dazu, dass die KRITIS-Prüfung (Kritische Infrastrukturen) des Bundesamtes für Sicherheit in der Informationstechnik (BSI) reibungslos absolviert werden konnte.

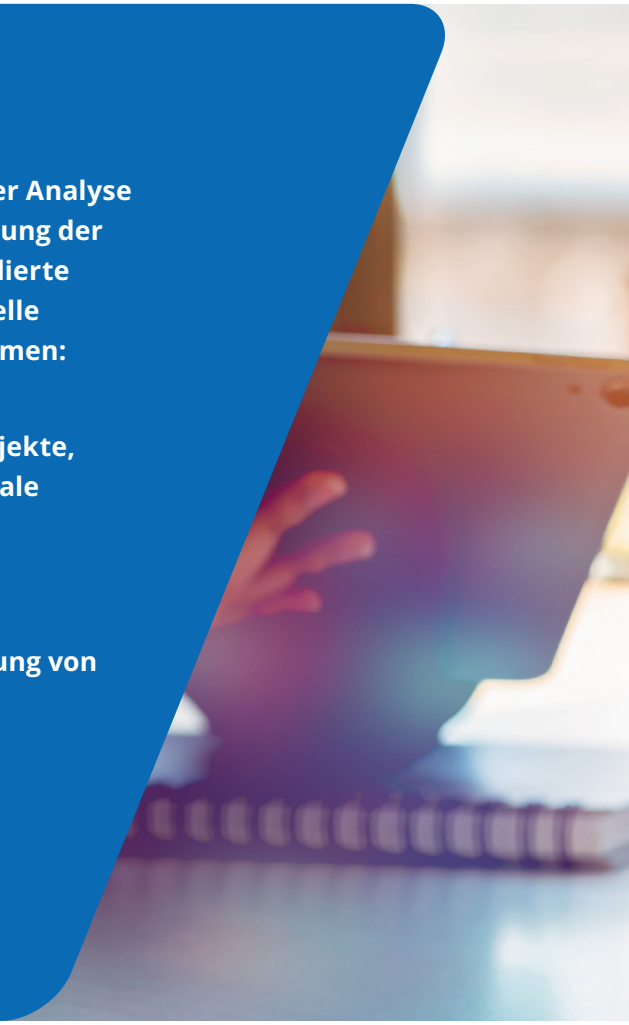
FSP – Ihr starker Partner für die sichere Digitalisierung

Alle reden über die Digitalisierung – wir packen sie an: Die FSP GmbH bietet seit 2001 Consulting & IT-Services für sichere digitale Kunden- und Geschäftsprozesse. Als anerkannter Partner namhafter mittelständischer und großer Unternehmen aus unterschiedlichen Bereichen beraten wir mit fachlicher, IT- und methodischer Kompetenz und schaffen so die richtigen Lösungen für IAM und sichere Digitalisierung. Von unserem Standort Köln aus sind wir mit einem hoch qualifizierten 50-köpfigen Team deutschlandweit für Sie aktiv.

Wir gestalten Ihre digitale Zukunft

FSP unterstützt Sie ganzheitlich in allen Projektphasen – von der Analyse und Beratung über das Projektmanagement und die Bereitstellung der richtigen Produkte bis zum Support. Dabei greifen wir auf etablierte Standardsoftware zurück oder entwickeln bei Bedarf individuelle Lösungen für Sie. Unsere Schwerpunkte sind die folgenden Themen:

- **Konzeption und Umsetzung innovativer Digitalisierungsprojekte, z.B. auf den Gebieten digitale Geschäftsprozesse, RPA, digitale Kommunikation und sichere Digitalisierung**
- **Ganzheitliches Identitäts- und Berechtigungs-Management (Identity & Access Management – IAM)**
- **Operative und steuernde Unterstützung bei der Durchführung von Projekten oder IT-Umsetzungsmaßnahmen**
- **Branchen- und versicherungsfachliche Beratung**
- **Optimierung von Prozessen und Maßnahmen zur Effizienzsteigerung**
- **Projekt-, Test- und Anforderungsmanagement**



Ihr Ansprechpartner

Jörg Riedel
Mitglied der Geschäftsleitung
Telefon: +49 (0) 2203 37 10 00 0
Mail: j.riedel@fsp-gmbh.com

Kontaktdaten FSP GmbH

FSP GmbH Consulting & IT-Services
Albin-Köbis-Straße 8 | 51147 Köln
Telefon: +49 (0) 2203 37 10 00 0
E-Mail: info@fsp-gmbh.com | www.fsp-gmbh.com