Identity & Access Management

Einführung eines rollenbasierten IAM – Ein Praxisbericht

security-zone 2013
18. – 19. September 2013

Jürg Anderegg, Leiter Fachstelle IAM, Zürcher Kantonalbank
Adrian Bachmann, Expert IT Security Consultant, TEMET AG

Zürcher Kantonalbank

Agenda

- **Ausgangslage und Motivation**
- **IAM Zielbild**
- **IAM Programm der Zürcher Kantonalbank**
- **IAM Konzept**
- **Vorgehen IAM Erst-Rollenbildung**
- **Migration / Rollout**
- **«Lessons learned»**
- **Fragen / Diskussion**

Zürcher Kantonalbank

Ausgangslage und Motivation

Weshalb werden IAM-Projekte gestartet?

Zürcher Kantonalbank

Tages-Anzeiger «aktuell» – Freitag, 6. September 2013
Auszug zum Thema Datendiebstahl im Nachrichtendienst

Datendiebstahl

Geheimdienst ignorierte interne Warnungen

Nachrichtendienstchef Markus Seiler erfuhr lange nichts über die Verdachtsmomente gegen den IT-Mitarbeiter, der brisante Dokumente entwendete.

Zugriffsrechte trotz Zweifeln

IT-Spezialist B. trat seine Stelle beim Geheimdienst im Jahr 2007 an. Dabei genoss er offenbar viel Freiraum. Was er im Computersystem des NDB machte, war für Dritte nicht nachvollziehbar. Die GPDel schreibt:

«Die Ausnahmen bei den persönlichen Administratorenkonten wurden in der Informatik intern verwaltet, und ihre Verwendung wurde nicht kontrolliert. Diese Praxis (...) gab den betreffenden Informatikern auch uneingeschränkte Zugriffsrechte, deren Verwendung nachträglich nicht mehr persönlich zugeordnet werden konnte.»

Geschäftsprüfungsdelegation der eidg. Räte (GPDel) präsentierte am Do., 5. September 2013 ihren Bericht.

GPDel schreibt in ihrem Bericht:
…es gebe «keinen Grund zur Annahme, dass das bestenfalls ansatzweise vorhandene Überwachungs- und Kontrolldispositiv in der Informatik des NDB von sich aus einen Hinweis auf den Datendiebstahl generiert hätte.

Zitat Tages-Anzeiger vom Fr. 06.09.2013

Hier fehlte offensichtlich ein effektives **Identity & Access Management**.

Die Ausgangslage der Zürcher Kantonalbank (ZKB) war und ist glücklicherweise viel besser.

Zürcher Kantonalbank

Die Zürcher Kantonalbank ist sicher!

Fitch Ratings **AAA** seit 2009

Moody's **AAA** seit 2006

Standard & Poor's **AAA** seit 1994

WORLD'S 50 SAFEST BANKS 2013

Rank	*Group Name*	*Country*
1	**KfW**	Germany
2	**Bank Nederlandse Gemeenten**	Netherlands
3	**Zürcher Kantonalbank**	Switzerland
4	**Landwirtschaftliche Rentenbank**	Germany

Zürcher Kantonalbank

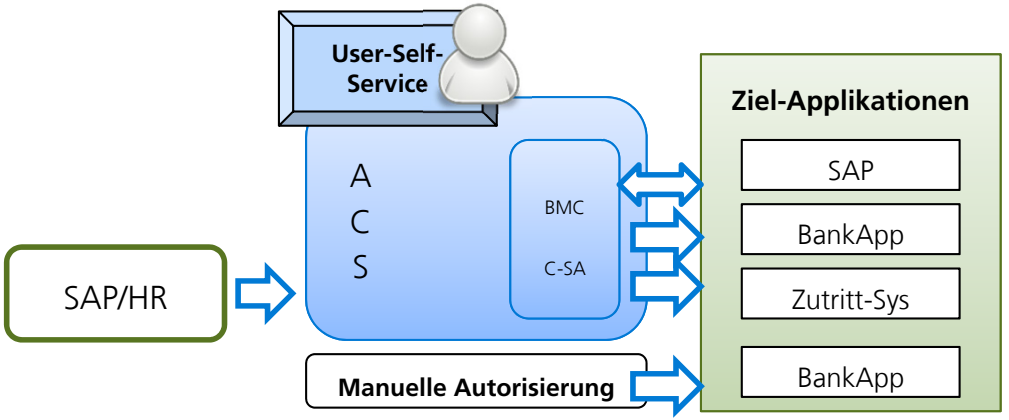
Wo sind wir gestartet? Ende 2010 verfügte die Zürcher Kantonalbank bereits über eine grundsätzlich solide Basis für Access Autorisierungen und deren Provisionierung .

Zentrales Berechtigungssystem:

- UserID-Konzept vorhanden und umgesetzt
- Verwaltung der Berechtigungs-objekte und Berechtigungen erfolgt für eine Vielzahl von Applikationen in einer zentraler IAM Lösung (ACS*)
- User Self Service: Berechtigungen können durch den Mitarbeitenden bestellt und durch Vorgesetzten und Rechteowner visiert werden
- Anbindung an SAP-HR stellt die User-Life Cycles sicher

Kritische Würdigung:

- Stabiler, tagfertiger, jedoch starrer Provisionierungsprozess
- Joiner-Changer-Leaver-Prozesse werden unterstützt
- Periodical User Access Review nur mangelhaft unterstützt
- Kumulation von Berechtigungen



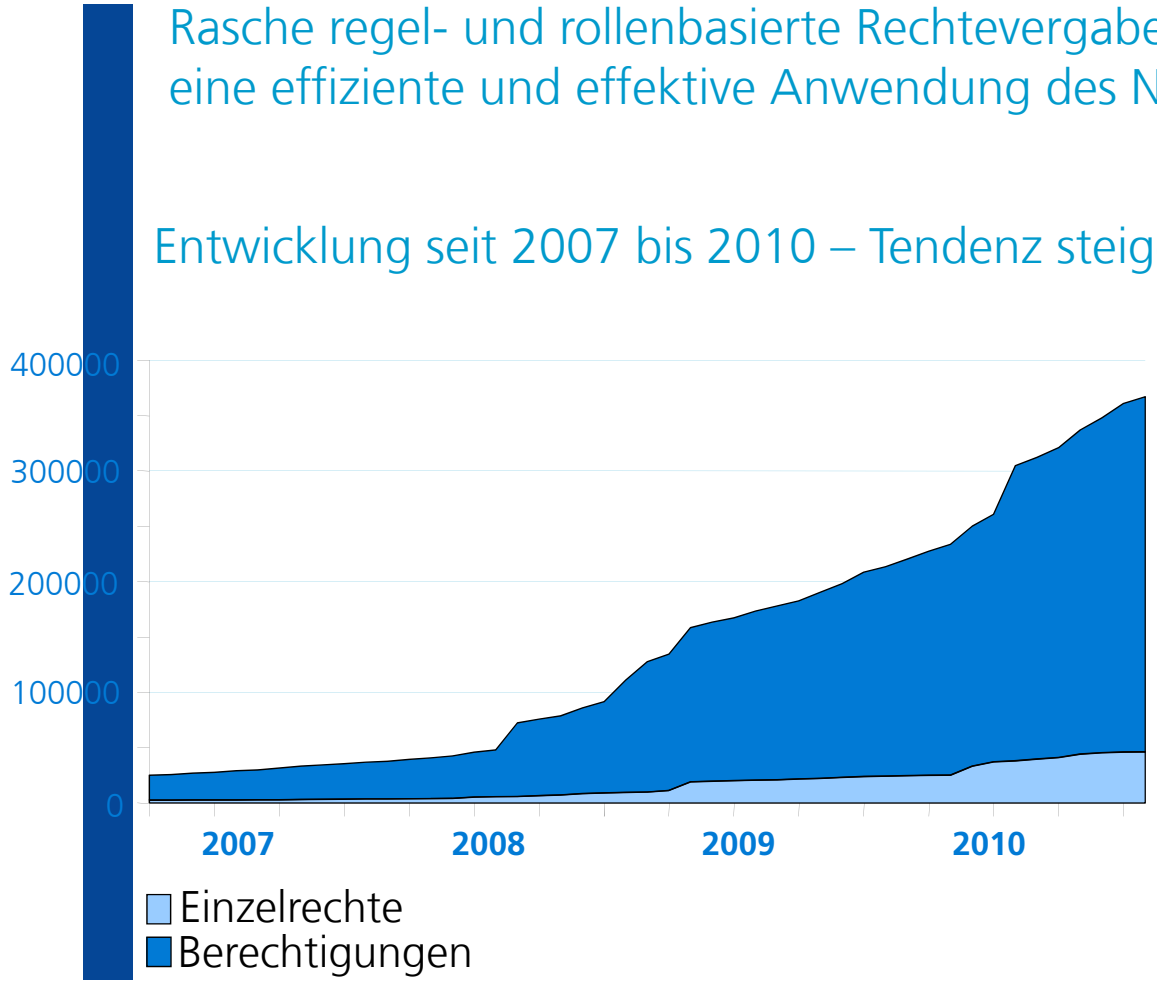
* Access Control System

Zürcher Kantonalbank

Rasanter Wachstum zwingt zur Neukonzeption des Berechtigungsmanagements.

Rasche regel- und rollenbasierte Rechtevergabe ist zwingend notwendig als Basis für eine effiziente und effektive Anwendung des Need-to-Know-Prinzips

Entwicklung seit 2007 bis 2010 – Tendenz steigend



- Zunahme der Berechtigungen über 65% p.a. auf Grund von Neu-Anbindungen und feingranularen Rechtedefinitionen geschätzt
- Das Wachstum kann nur durch eine regel- und rollenbasierte Rechtevergabe eingeschränkt werden "weg vom Einzelrecht"
- Der Fokus des Programms IAM für 2014 liegt auf dieser Massnahme.

Stand Mai 2013: 60'000 Entitlements, 650'000 Berechtigungen, >1'500 Applikationskomponenten (Provisionierungssysteme) angebunden

Zürcher Kantonalbank

Aus Sicht IKS wurde weiterer Handlungsbedarf identifiziert.

- Mangelnde Transparenz und dadurch schlechte Überwachung und Kontrolle der vergebenen Berechtigungen (ungenügende Beschreibungen, keine appl. Berechtigungskonzepte, dadurch mangelnde Beurteilbarkeit)
- Nicht geregelte und nicht risikoorientierte Berechtigungsvergaben
- Konfliktäre Rechte (Identifikation / 'Toxische Kombinationen')
- Fehleranfällig (nicht gepflegte Rechte, falsche oder fehlende Owner)
- Hohe Durchlaufzeiten von Berechtigungsanträgen
- Starrer (HR-prozessgetriebener) Ablauf – mangelnde Intervention

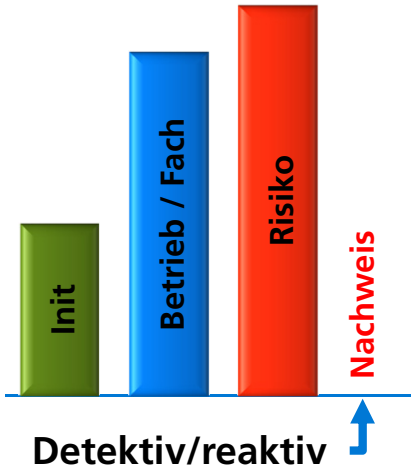
Zürcher Kantonalbank

IAM Zielbild

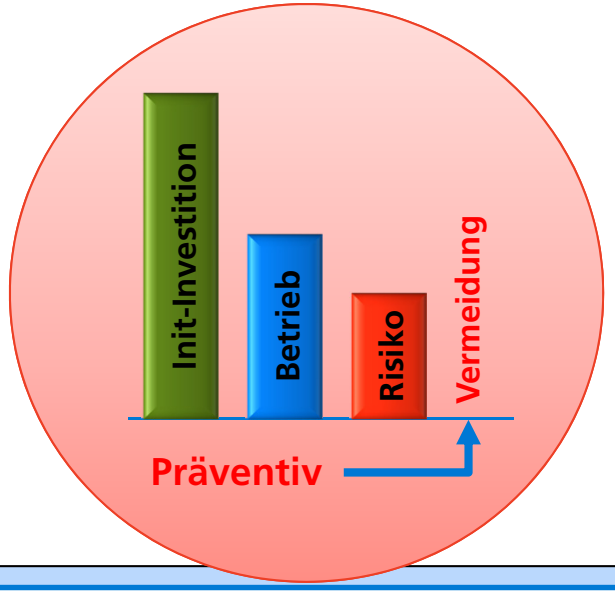
Eckwerte der neuen Identity & Access Governance

Zürcher Kantonalbank

Paradigma-Wechsel: Das IAM Fachkonzept definierte den grundsätzlichen Wechsel von IAM als Management-Aufgabe.



Risikovermeidung anstelle Schadens- und Verursachernachweis



User-Self-Service auf Einzelrechtebasis

Die in Selbst-Bestellung erhaltenen, dutzenden von Einzelberechtigungen müssen alljährlich nach IKS-Auftrag von den Vorgesetzten überprüft werden. Transparenz! Rechte-Konflikte!

Manager-Assignment-Service auf Rollenbasis

Zuweisung von betrieblich-erforderlichen IAM Rollen regelbasiert oder durch den Vorgesetzten und zyklische Rezertifizierung resp. eventbasiert nach Änderungen.

WICHTIG: **Denken in FUNKTIONEN** und nicht mehr in Einzelberechtigungen!
Vorgesetzte bestimmen, wer im Team welche Funktionen ausübt.

Zürcher Kantonalbank

Berechtigungen werden überschaubar und kontrollierbar, die Effizienz kann gesteigert werden.

Was wird mit der Umsetzung des Programms IAM erreicht?

Der Vorgesetzte beurteilt IAM Rollen statt Einzelrechte

IAM Rollen können gruppiert und als Gruppe zugewiesen werden

Neue Einzelrechte werden in IAM Rollen integriert

Berufsbild- und OE abhängige IAM Rollen können automatisch vergeben werden

Es ist definiert, welcher Mitarbeitende welche IAM Rolle erhält

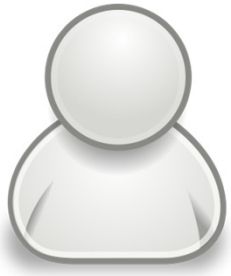
Konfliktäre Zuweisungen können definiert werden und sind technisch erkenn- und vermeidbar

Die Beantragung von falschen Rechten durch Mitarbeitende wird verhindert (eingeschränkte Sicht)

Mitarbeitende und Vorgesetzte müssen massiv weniger Rechte beantragen und visieren

Zürcher Kantonalbank

Die Berechtigungsverwaltung wird massiv vereinfacht und transparenter.



Hans Muster (sanitized)

IST
66 Einzelberechtigungen

- AGR:Z:BC__BAS_E01_COMMON
- AGR:Z:BI__BAS_E001_001_COMMON
- AGR:Z:BI__HR__E018_001_SEL
- AGR:Z:BI__HR__E028_001_REP
- AGR:Z:BI__HR__E042_001_DIS
- AGR:Z:BI__PS__E001_001_REP
- AGR:Z:BI__PS__E002_001_DIS
- AGR:Z:BI__PS__S001_001_ITPRJ
- ASY 1
- BRR_KOMMERZ_FILIALE0FL
- CN=G-A-BRRSEMIDEZ-SSO,OU=resourcegroups,OU=zgroups,…
- CN=G-A-WDMSCLIENT20,OU=resourcegroups,OU=zgroups,…
- CN=G-A-WEXCEED14,OU=resourcegroups,OU=zgroups,DC=…
- CN=G-A-WEXEEDONDEMAND70,OU=resourcegroups,OU=zg…
- CN=G-A-WFWS30,OU=resourcegroups,OU=zgroups,DC=…
- CN=G-A-WMLDSCLIENT20,OU=resourcegroups,OU=zgro…
- CN=G-A-WRATINGBRRKOMMERZ25,OU=resourcegroups…
- CN=G-A-WRISKVISION55,OU=resourcegroups,OU=zgroups,…
- CN=G-A-WZKBPERIPHERALCONTROLLER10,OU=resourcegro…
- CN=G-G-FSL,OU=resourcegroups,OU=zgroups,DC=prod,DC=…
- CN=G-L-STETTBACH-CONBA,OU=resourcegroups,OU=zgro…
- CN=G-M-DPADVISGEF-READ,OU=resourcegroups,OU=zgro…

Usw.

SOLL
7 IAM-Rollen und
2 Einzelberechtigungen

- IAM Rolle (5 Einzelberechtigungen) **Rule**
  Basisrolle interner Mitarbeitender
- IAM Rolle (7 Einzelberechtigungen) **Rule**
  Basisrolle Linienvorgesetzter
- IAM Rolle (1 Einzelberechtigungen) **Rule**
  Organisationsrolle Kundenrating
- IAM Rolle (27 Einzelberechtigungen) **Rule**
  Funktionsrolle Rating Risk
- IAM Rolle (7 Einzelberechtigungen) **manual**
  Gremium Ratingmodelle
- IAM Rolle (3 Einzelberechtigungen) **manual**
  Spezialrolle Remote Access
- IAM Rolle (5 Einzelberechtigungen) **manual**
  Projektrolle security-zone 2013

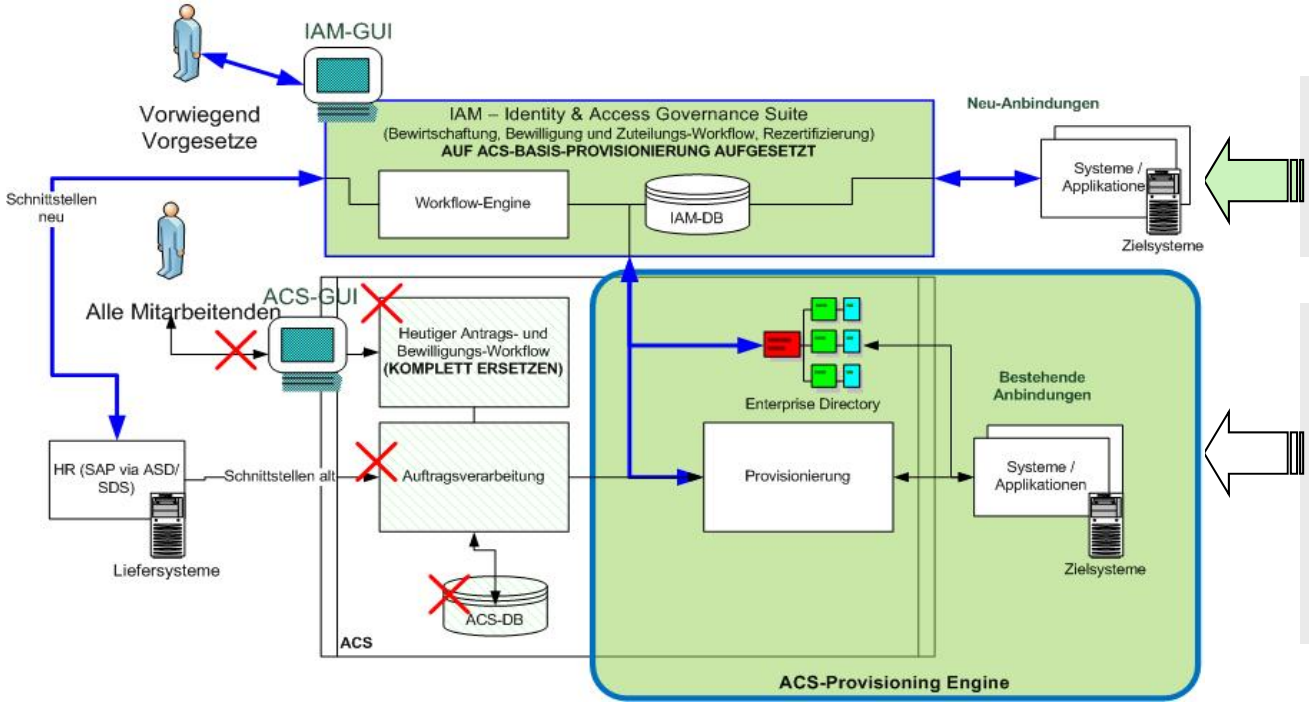
- Laufwerk TOP-SECRET
- Zutrittsrecht Parkhaus City

Zürcher Kantonalbank

Der technische Lösungsansatz basierte auf der bestehenden ACS-Lösung.

Lösungsprinzip Technik – «Investitionsschutz und Kontinuität» sicherstellen

- Eine Identity & Access Governance Suite (Legislativer Layer) soll **auf bestehendes Provisionierungssystem** ACS aufsetzten. Dieses IAM stellt Rollenbewirtschaftung / - zuteilung, SoD-Konfliktmanagement und Rezertifizierung sicher.
- Die **Schnittstellen (Inbound) sollen weitestgehend beibehalten** werden, jedoch den Möglichkeiten der neuen Suite angepasst werden.
- **Auftragsabwicklungsprozesse sollen mittels flexiblen Workflows** in der neuen IAM-Suite abgebildet werden.
- Die technische Machbarkeit dieses Lösungsprinzips sollte in einem **Proof-of-Concept** verifiziert werden.

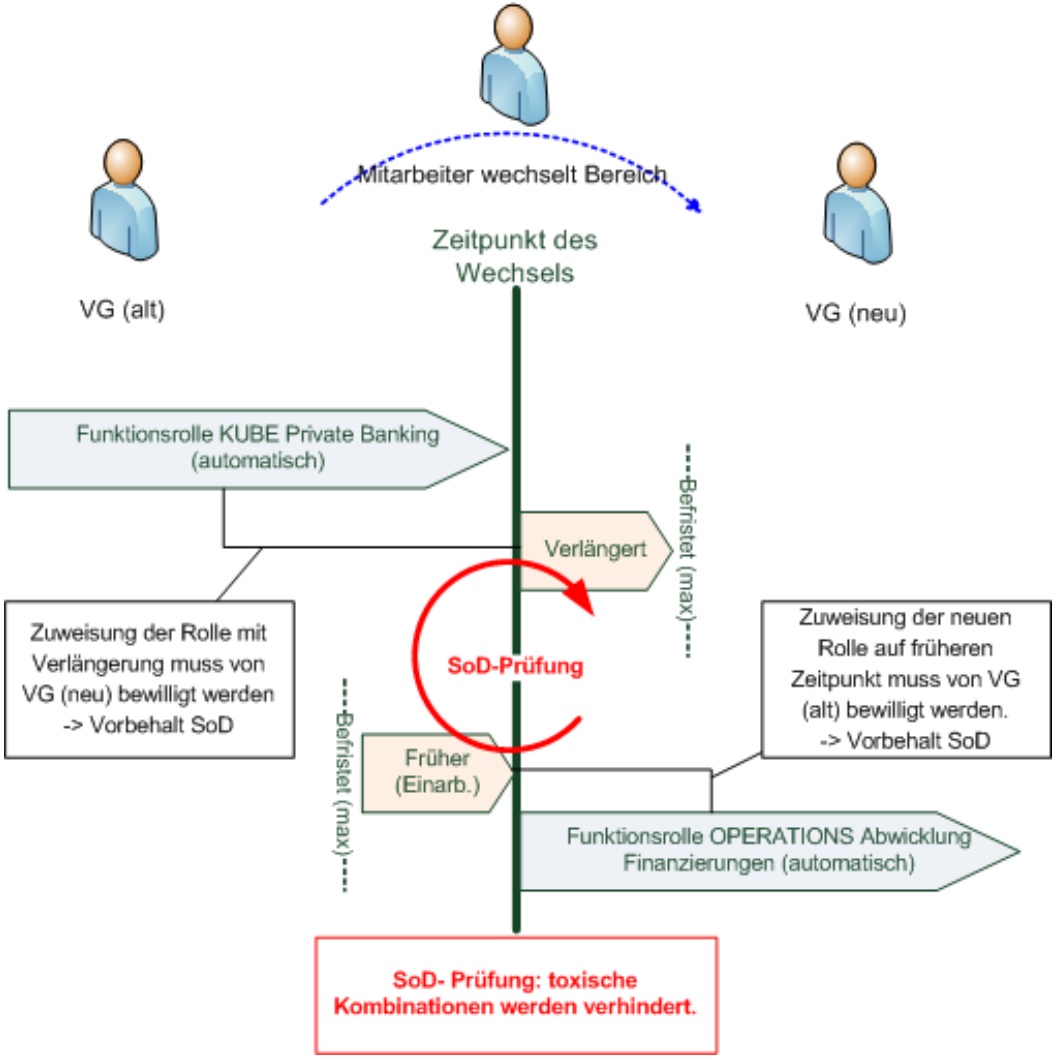


Neues Identity & Access Management – regel-/rollen-basierend. (Legislative Layer)

ACS-Provisioning-Engine mit zahlreichen Anbindungen ist vorerst beizuhalten (Executive Layer), um den Parallelbetrieb während der Umstellung sichergestellt ist.

Zürcher Kantonalbank

Wechseln Mitarbeitende die Organisationseinheit («Changer»-Thematik) ist oftmals eine flexible betriebliche Lösung erforderlich, ohne die Sicherheit zu gefährden.



Prinzipien des OE-Wechsels:

- Berechtigungen werden bei OE-Wechsel entzogen resp. Standard-IAM-Rollen des neuen Bereiches werden automatisch zugeteilt
- VG (alt) hat die Möglichkeit befristet eine IAM-Rollenzuteilung zu verlängern («Aufräumarbeiten»). Der VG (neu) muss bewilligen.
- VG (neu) hat die Möglichkeit einer vorzeitige IAM-Rollenzuteilung («Einarbeitung»). VG (alt) muss bewilligen.
- Bei überlappenden IAM-Rollenzuteilungen werden SoD-Konflikte geprüft. Ein SoD-Konflikt kann (sofern nicht «restricted») temporär zugelassen werden, indem beide VG zustimmen.

Zürcher Kantonalbank

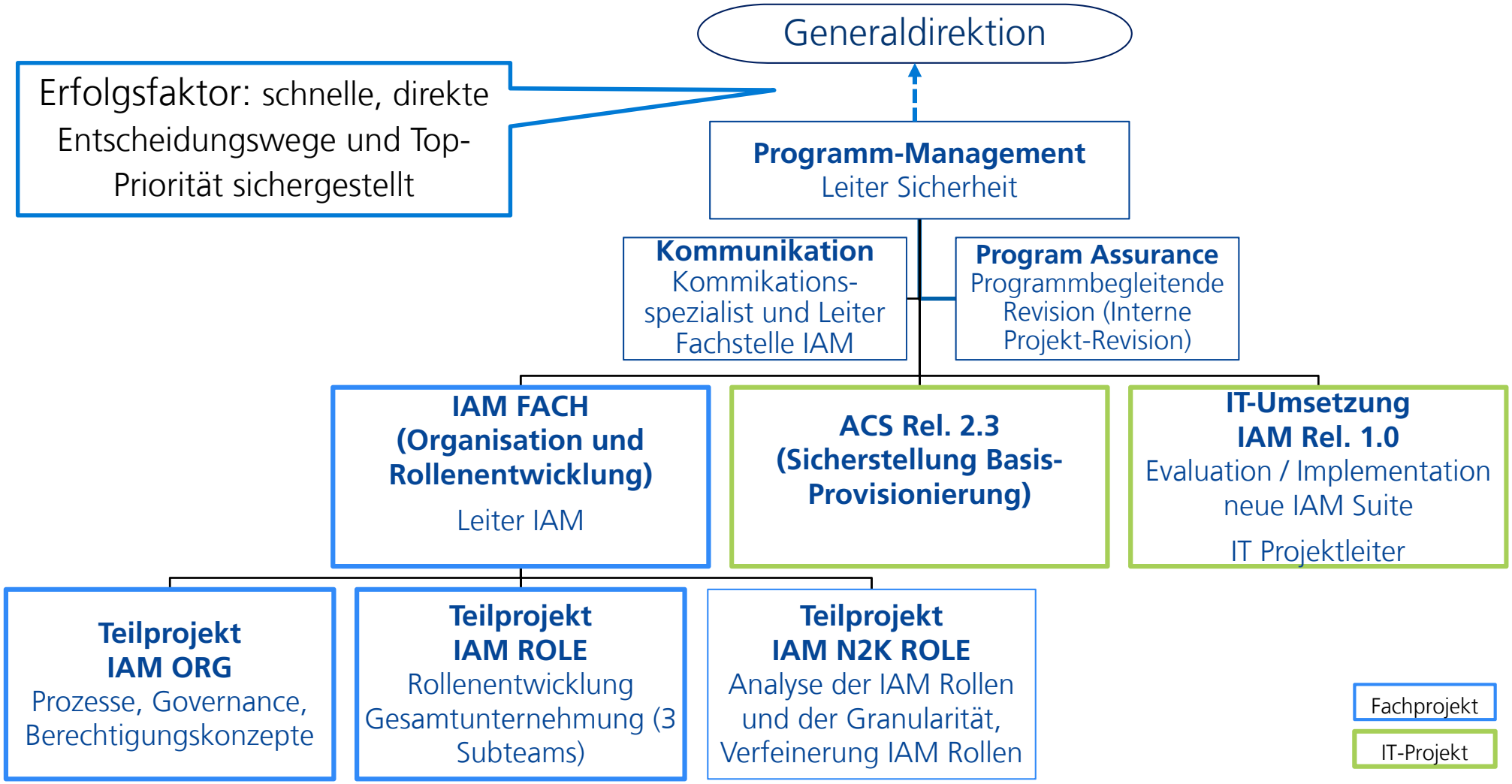
IAM Programm der Zürcher Kantonalbank

Organisation und Masterplan

Zürcher Kantonalbank

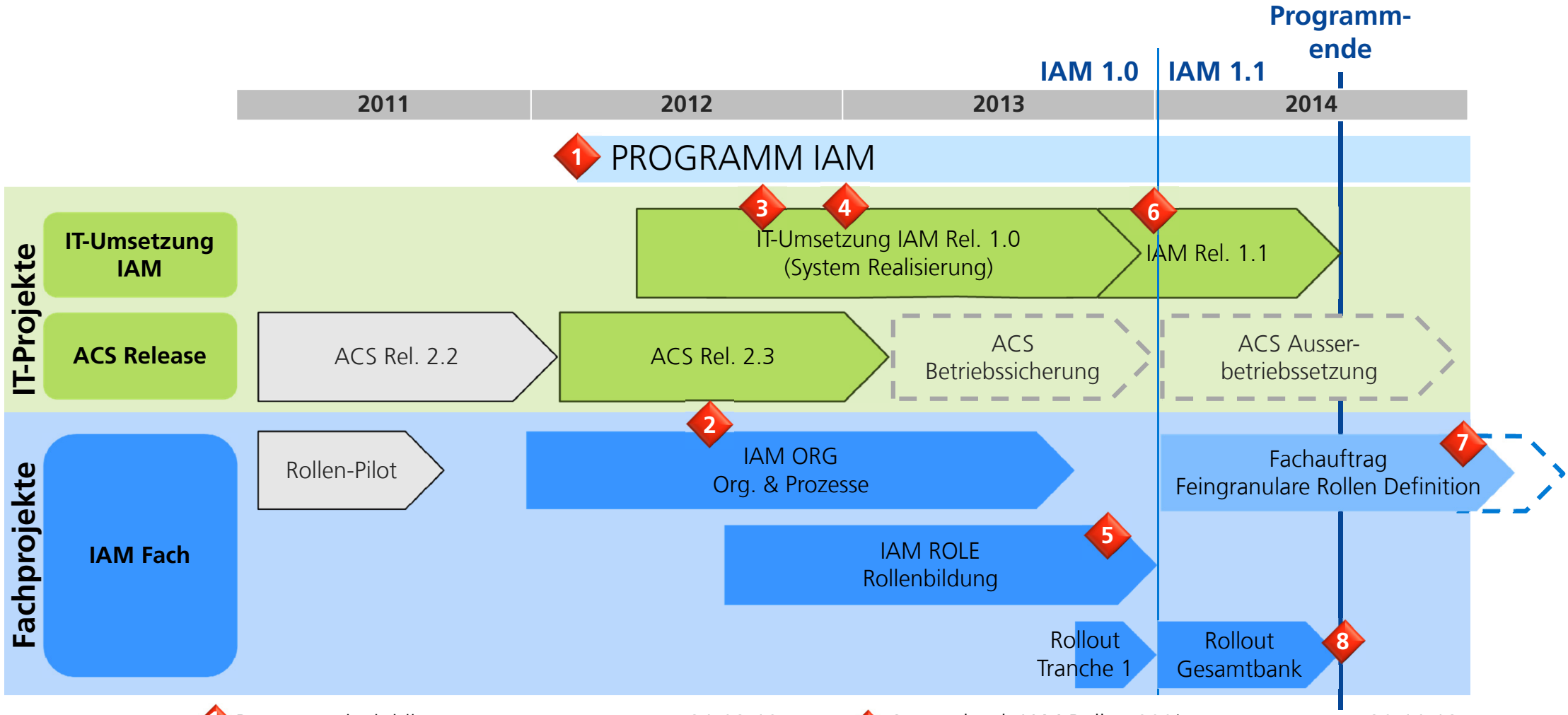
Das Programm IAM ist primär eine Fachinitiative.

Auf einen separaten Steuerungsausschuss konnte verzichtet und Eskalationen können direkt an die Generaldirektion gerichtet werden.



Zürcher Kantonalbank

Das Programm IAM ist in IT- und Fach-Projekte gegliedert und ist aktuell in der Phase «Realisierung/Testing».



Meilensteine

1	Programm ist initiiert	31.03.12	5	Gesamtbank-IAM Rollen 80%	30.11.13
2	IAM Organisation und Prozesse sind definiert	31.08.12	6	IAM IT System rollenbasiert ist eingeführt	31.12.13
3	IT Anforderungsspezifikation	30.09.12	7	Anforderung feingranulare Rollen sind definiert	31.12.14
4	PPH liegt vor	31.12.12	8	Transformation abgeschlossen	30.06.14

Zürcher Kantonalbank

IAM Konzept

Prinzipien der Identity und Access Governance

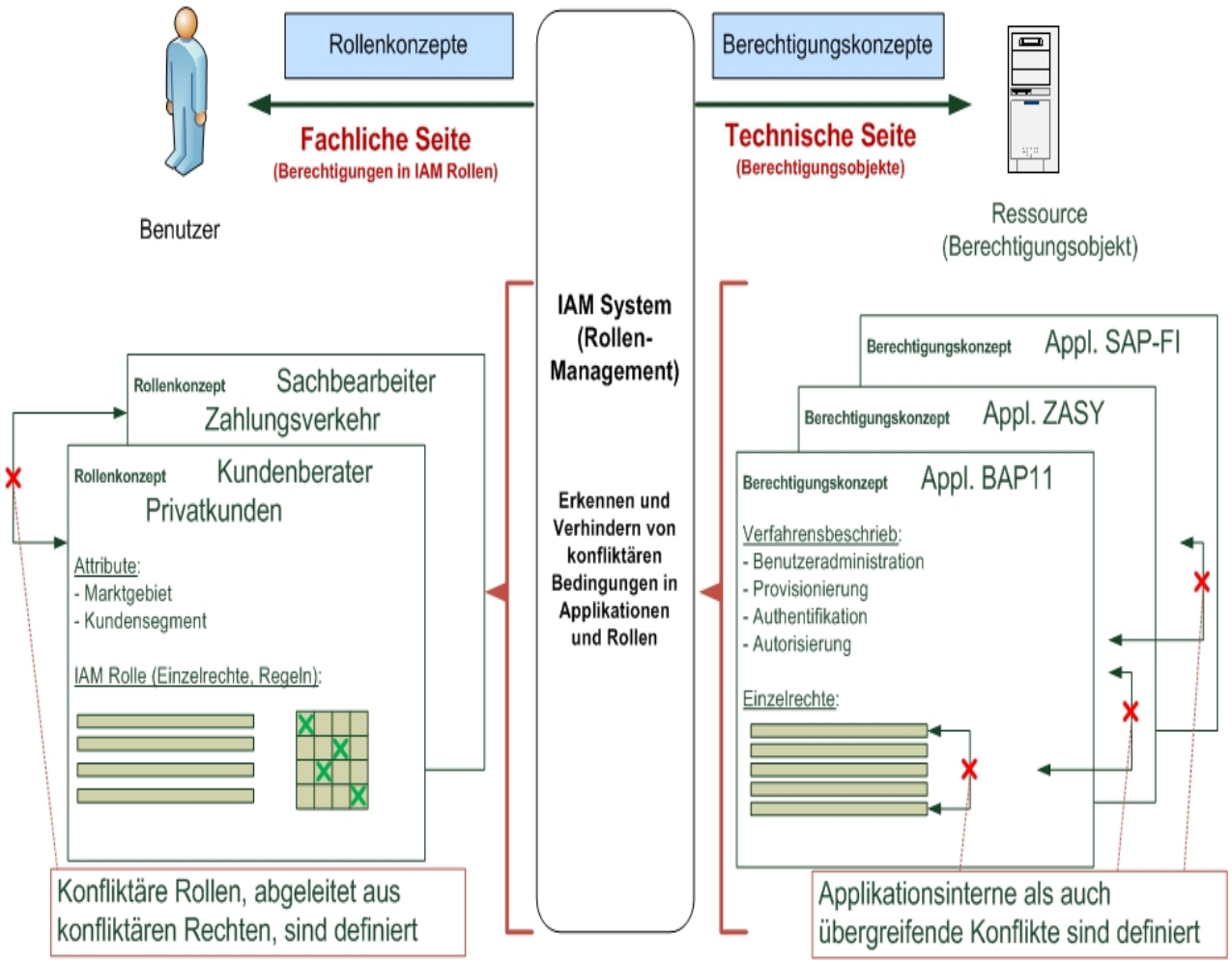
Zürcher Kantonalbank

Das IAM Big Picture umfasst mehrere Grundsätze.

- Unternehmensweite Berechtigungssteuerung durch Berücksichtigung aller **geschäftsrelevanten IT Systeme**
- Pro berücksichtigtem IT System ein **Berechtigungskonzept** (Definition der Berechtigungsobjekte, SoD auf Ebene Berechtigungsobjekt)
- **Bündelung** von Berechtigungsobjekten in **IAM-Rollen**; **Mehrfachzuweisungen** sind möglich
- **Mehrere Rollen** pro User möglich (und nötig)
- Das IAM Rollenmodell sieht **unterschiedliche Rollentypen** vor
- Kombination von **automatisierter** und **manuelle Rollenvergabe** in Abhängigkeit zur **Kritikalität** sowie des **Einsatzgebiets** der Berechtigungen
- Automatische **SoD-Überprüfungen** (SoD = Segregation of Duties)
- Der **IAM-Rollen-Katalog** verschafft **Übersicht** und schränkt die **Sichtbarkeit/Zuteilbarkeit** der IAM-Rollen ein

Zürcher Kantonalbank

Die Berechtigungsbeschreibungen sind wesentliche Voraussetzung, dass überhaupt Rollenkonzepte erstellt werden können.



Berechtigungskonzepte dienen unter anderem der Definition der Berechtigungsobjekte (Entitlements):

- Logische Bezeichnung
- Kurzbeschreibung
- Funktionsbeschreibung (anzeigen – anlegen – ändern – löschen – exportieren etc.)
- Nutzergruppen
- Berechtigungstyp (Fachrecht, IT-Recht, etc.)
- Prozessbezug
- Datendomänen
- Konfliktäre Rechte (SoD)
- Etc.

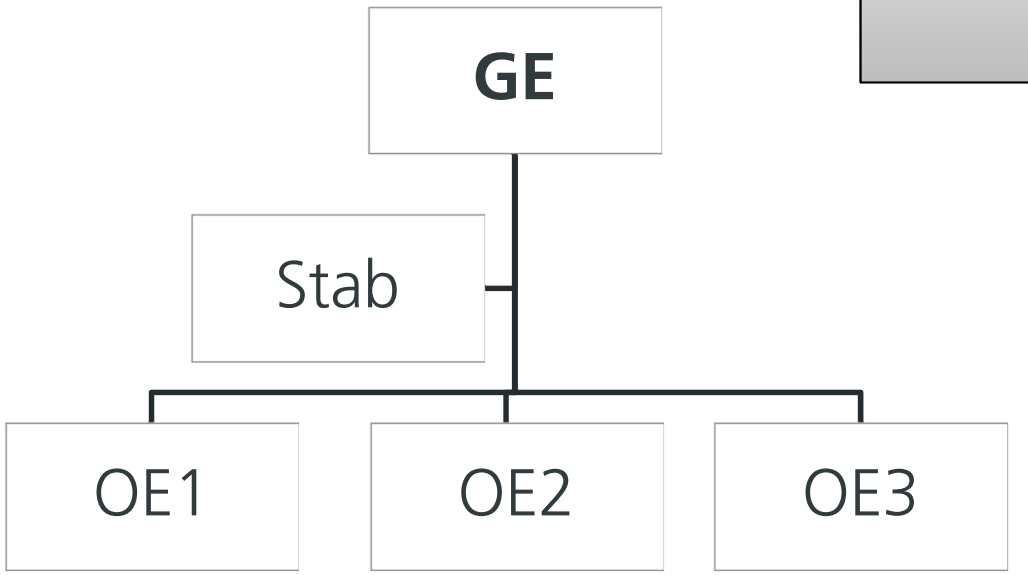
Zürcher Kantonalbank

Es gibt IAM Rollen entlang der Hierarchie oder aufgrund von übergreifenden Funktionen.

Gesamtbankrollen
- Basisrollen
- Spezialrollen
- GB-Funktionsrollen

Organisationsrollen
- Generelle Rechte der OE (Shares)
- Vererbungsmodell

Funktionsrollen
- Aufgaben und Aktivitäten der MA
- Aufgaben des (Funktions-)Bereichs



Projektrollen
- Projektspezifische Aufgaben und Zuständigkeiten

Querschnittsrollen
- OE übergreifende Tätigkeiten
- Gremien
- Spezialtätigkeiten

Zürcher Kantonalbank

Die Rechteverteilung erfolgt teilautomatisiert, nachvollziehbar und mit erhöhter Transparenz.

Automatische
(regelbasierte) Zuteilung aufgrund Berufsbild und Teamzugehörigkeit

Manuelle
(dedizierte) Zuteilung durch Rollenowner und Vorgesetzten

Ressourcen/Spezialzutritte
Beantragung durch Mitarbeiter direkt

Erhöhte Transparenz Need-to-Know/Do: Vergabe von Berechtigungen aufgrund ausgeübter Tätigkeiten/Funktionen

Basisrolle ZKB
(Grundzutritt, Outlook etc.)

Organisationsrolle
(Rolle der Geschäftseinheit, in der sich MA befindet)

Standardfunktionsrolle
(Grundfunktionen, die alle im Team ausführen)

Funktionsrolle xy
(Für die Ausübung einer bestimmen Funktion, dediziert)

Projektrolle xy
(Für die Mitwirkung in einem Projekt)

Gremium xy
(Für Mitarbeit in Gremium, z. B. Notfallorganisation)

Workstation-Pakete. (z.B. MS Visio)
Spezialzutritte (z.B. Tiefgarage Hard)

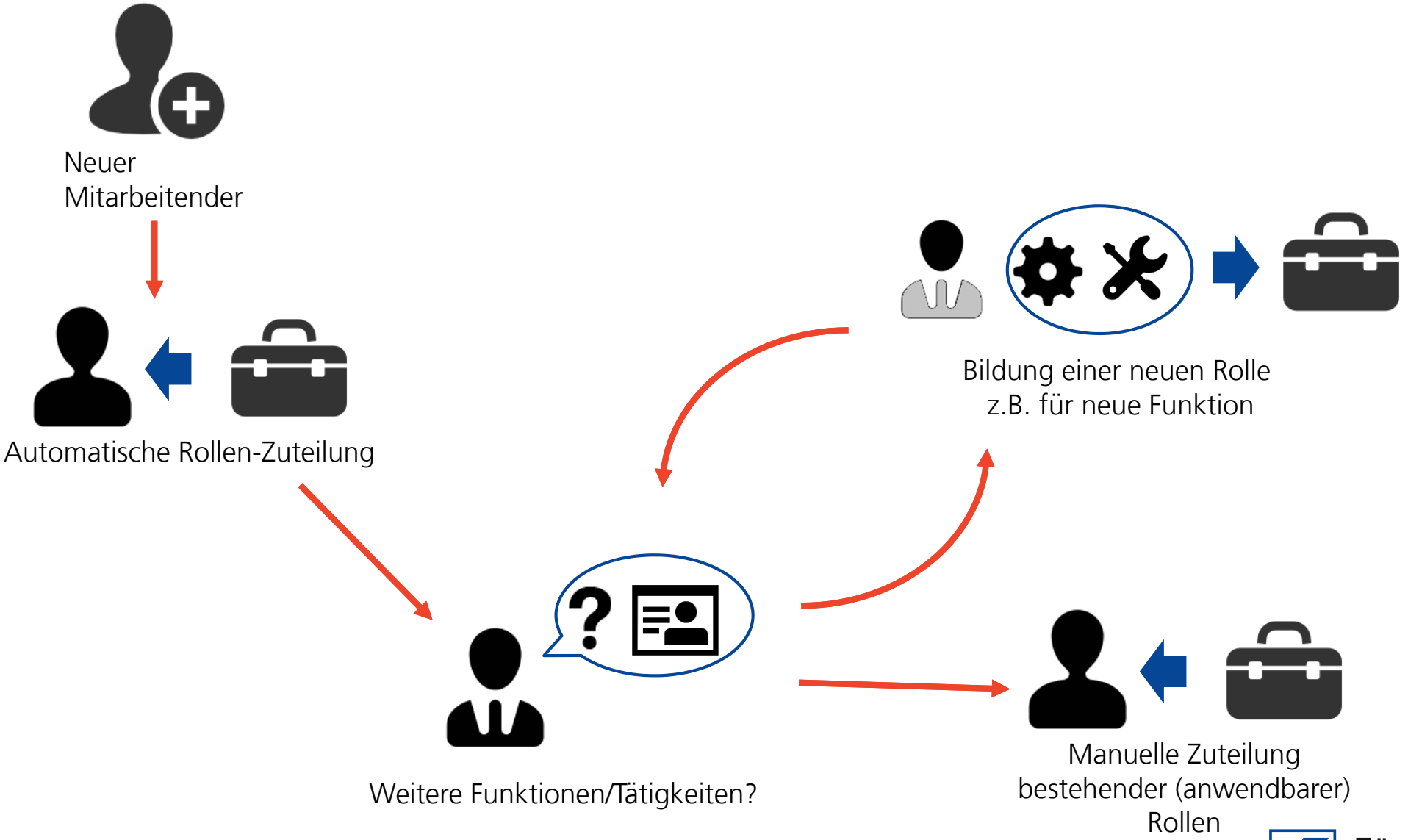
→ Sind unabhängig von Funktion bzw. lizenzabhängig

Berechtigungsvergabe an Mitarbeitende mit dem neuen IAM System

- Mitarbeitende erhalten die Grundrollen, die sie für die Ausübung ihrer Tätigkeit benötigen, automatisiert
- Die IAM Rollen für zusätzliche/spezielle Funktionen werden durch den Vorgesetzten oder Rollenowner (befristet) zugewiesen (Manager-Assignment-Service)
- Ressourcen (arbeitsplatz-abhängig/Softwarepakete) und spezifische Zutrittsrechte werden individuell durch den Mitarbeitenden mittels einer Kioskfunktion (User-Self-Service) beantragt

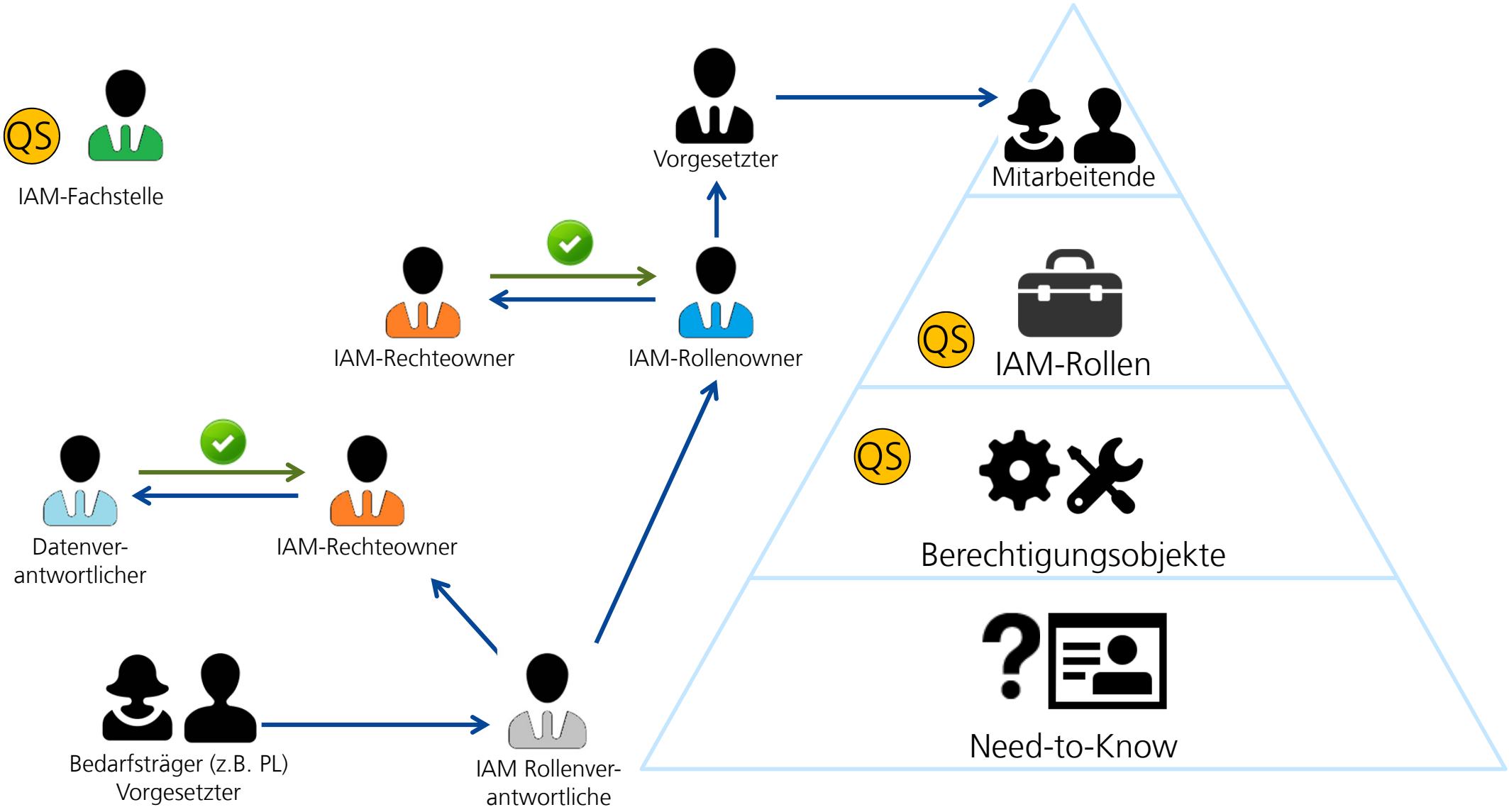
Zürcher Kantonalbank

Eintritt neuer Mitarbeitender: Die Rollenzuteilung erfolgt teilautomatisch entlang des Need-to-Know/Do-Prinzips.



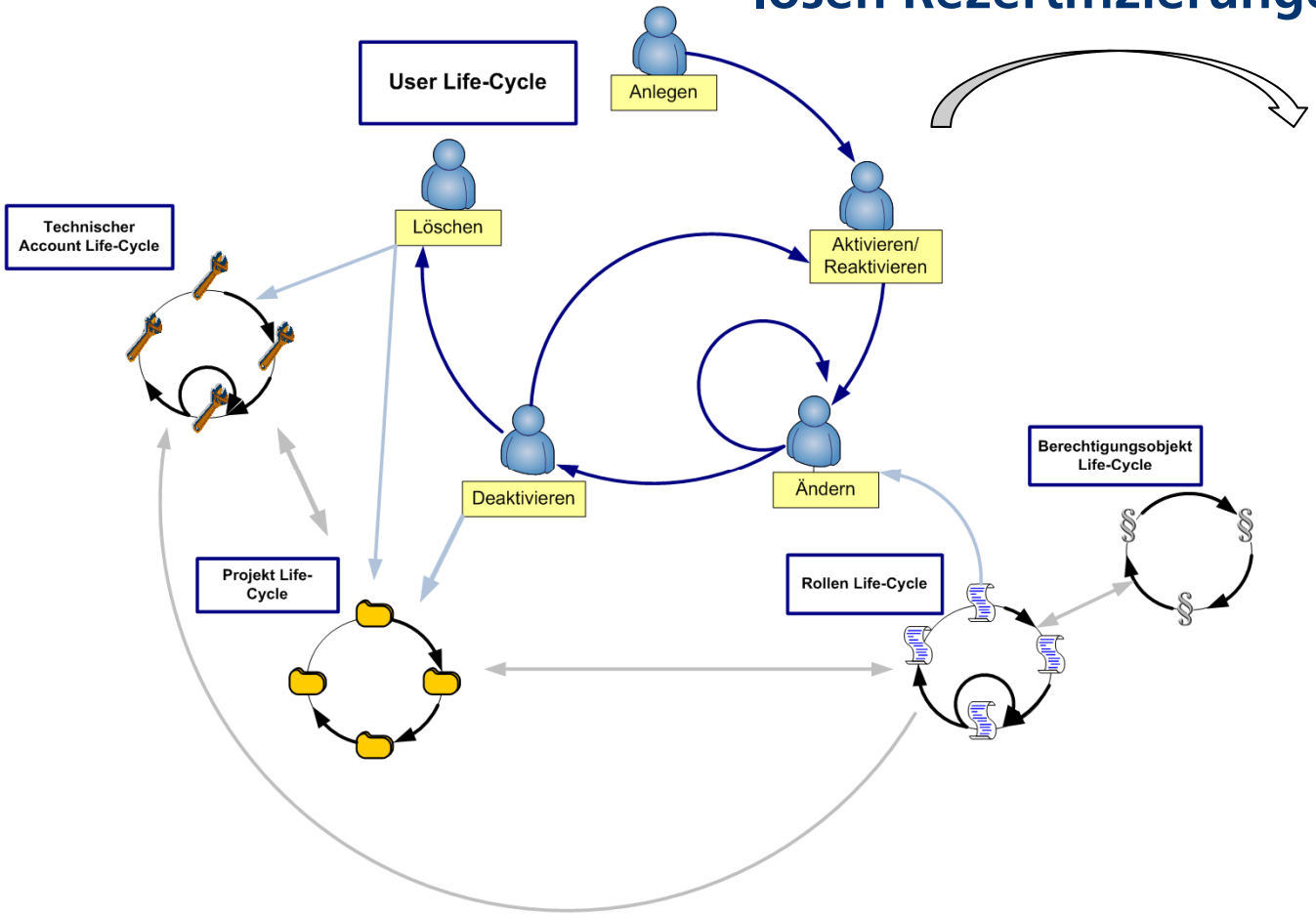
Zürcher Kantonalbank

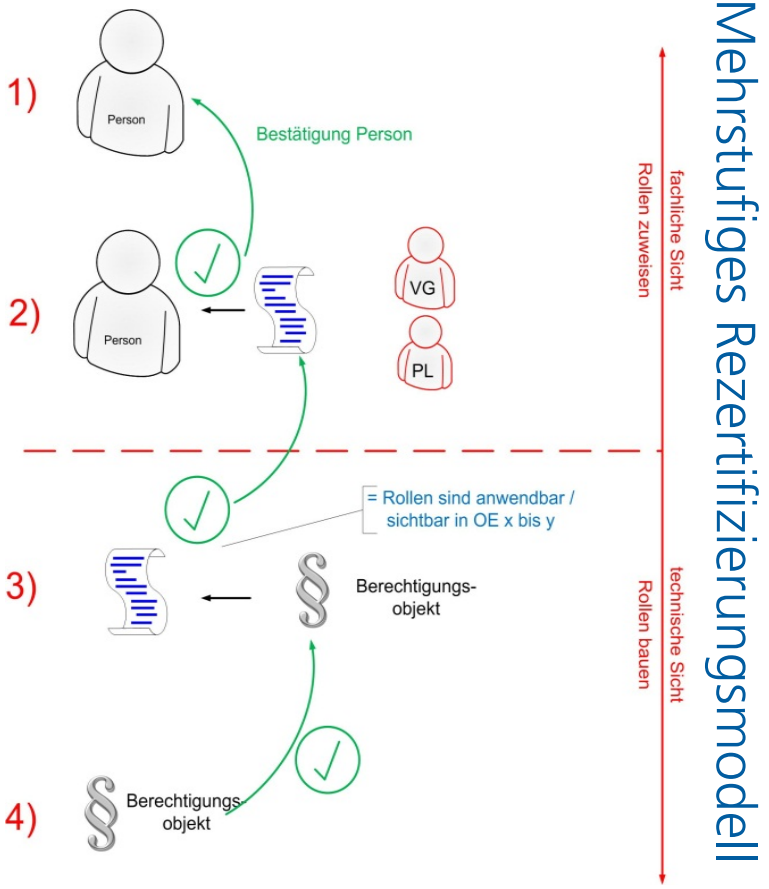
Der Rollenbildungsprozess umfasst mehrere Aufgaben und Verantwortlichkeiten.



Die enge Verknüpfung der Life-Cycles sowie die (periodischen) Rezertifizierungen stellen den Need-to-Know/Do sicher.

Änderungen sowie periodische Events lösen Rezertifizierungen aus

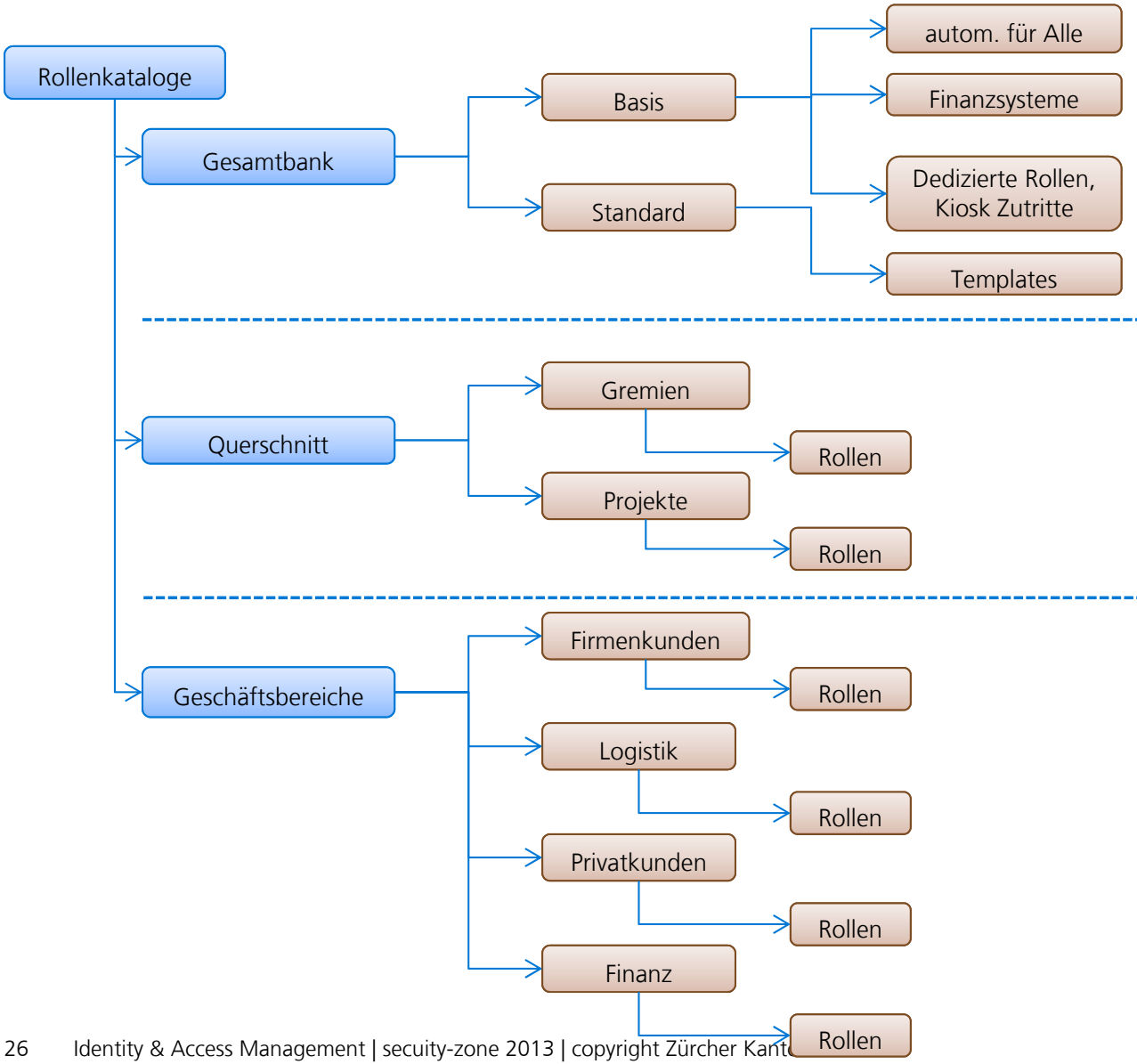




Mehrstufiges Rezertifizierungsmodell

Zürcher Kantonalbank

Der Rollenkatalog stellt sicher, dass die Gesamtheit der Rollen überhaupt verwaltbar wird. Er definiert Sichtbarkeit und Zuteilbarkeit der Rollen.



Gesamtbank-Katalog umfasst:
- Automatische Basisrollen (nicht sichtbar)
- Dedizierte, lizenzpflichtige Finanzsysteme
- Dedizierte Gesamtbankrollen (manuell zuteilbar)
- Kiosk Zutritte (bestellbar im User-Self-Service)
- Templates (nicht sichtbar, als Vererbung für Fachrollen verwendet)

Querschnitts-Katalog umfasst:
- Gremiumsrollen (NOFOR, IT-Steuerungs-ausschuss, etc.) – permanente Zuteilung
- Projektrollen – zeitlich begrenzte Zuteilung

Rollen in diesem Katalog sind nur von den Rollenverantwortlichen (Gremien- und Projektleiter) sichtbar und zuteilbar.

Bereichs-Katalog umfasst:
- Die den Geschäfts- und Organisationseinheiten zugeteilten Business-Rollen.

Dieser Katalog enthält die Funktionsrollen, welche den Organisationseinheiten für die fachlichen Standard- als auch Spezialfunktionen zur Verfügung stehen. Dabei stehen einem Vorgesetzten nur diejenigen Rollen zur Verfügung, die seinem Scope (OE) entsprechen.

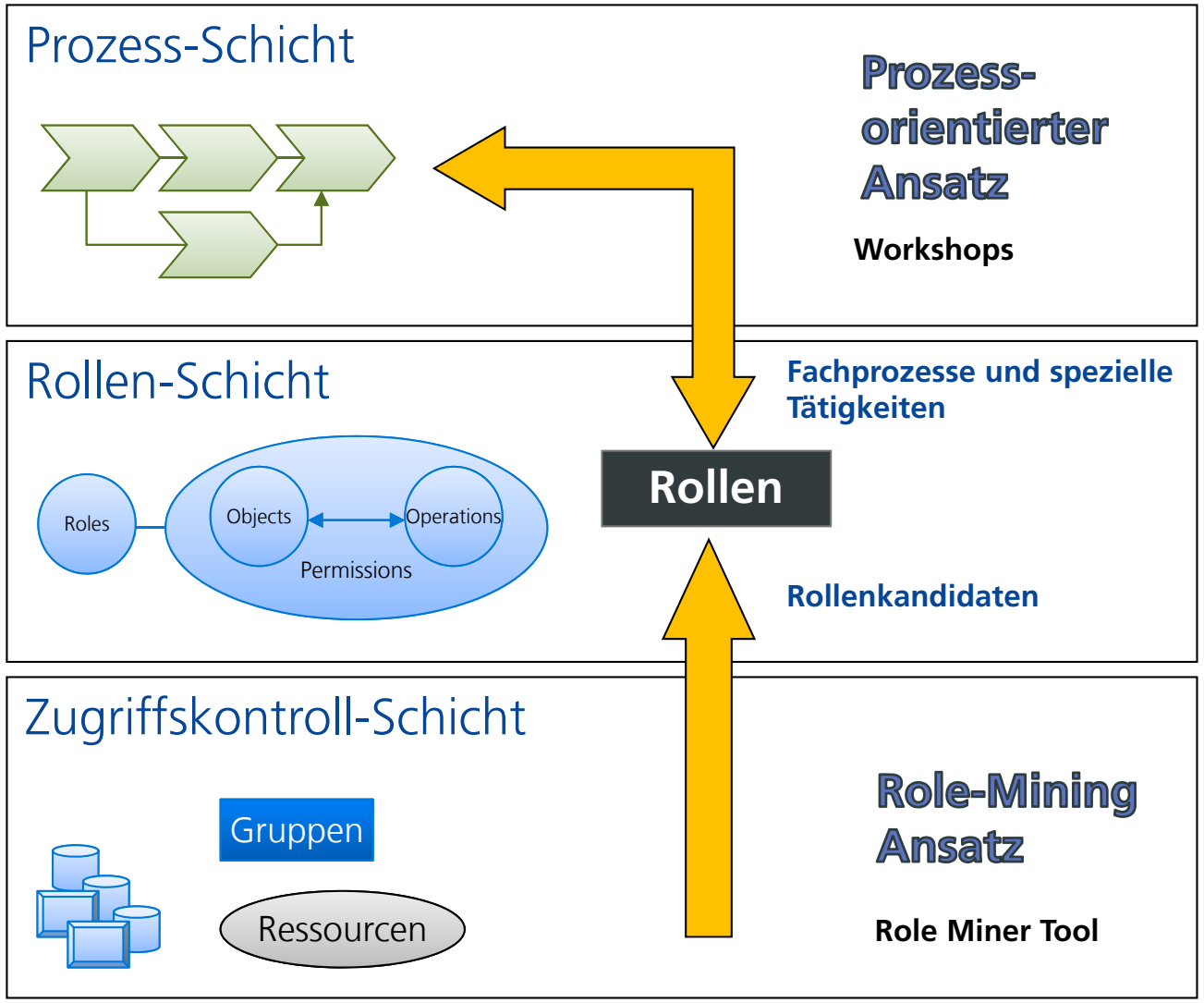
Zürcher Kantonalbank

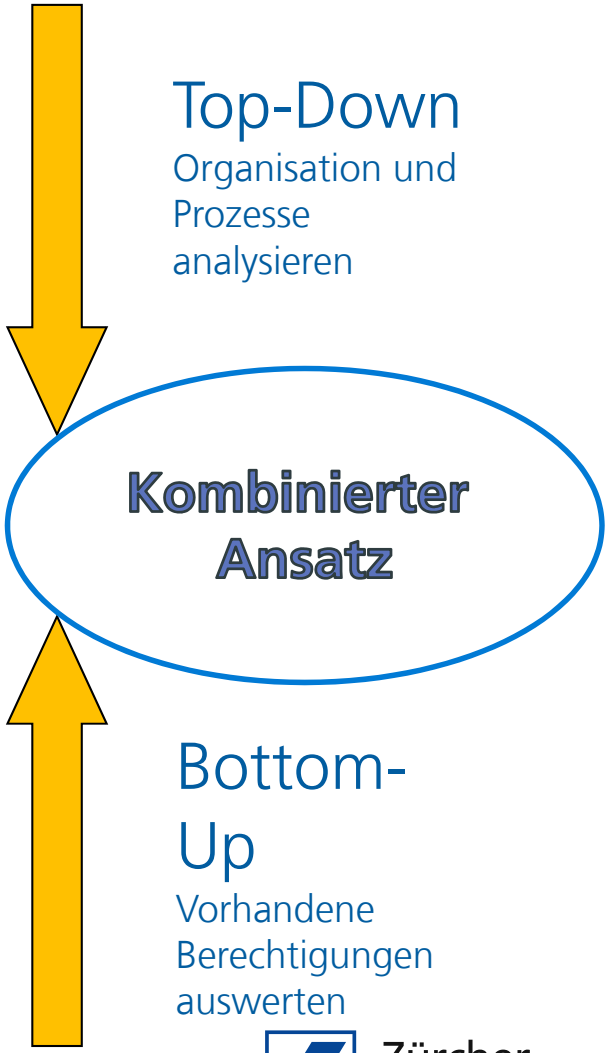
Vorgehen IAM Erst-Rollenbildung

Effizientes Rollenbildungsmodell

Zürcher Kantonalbank

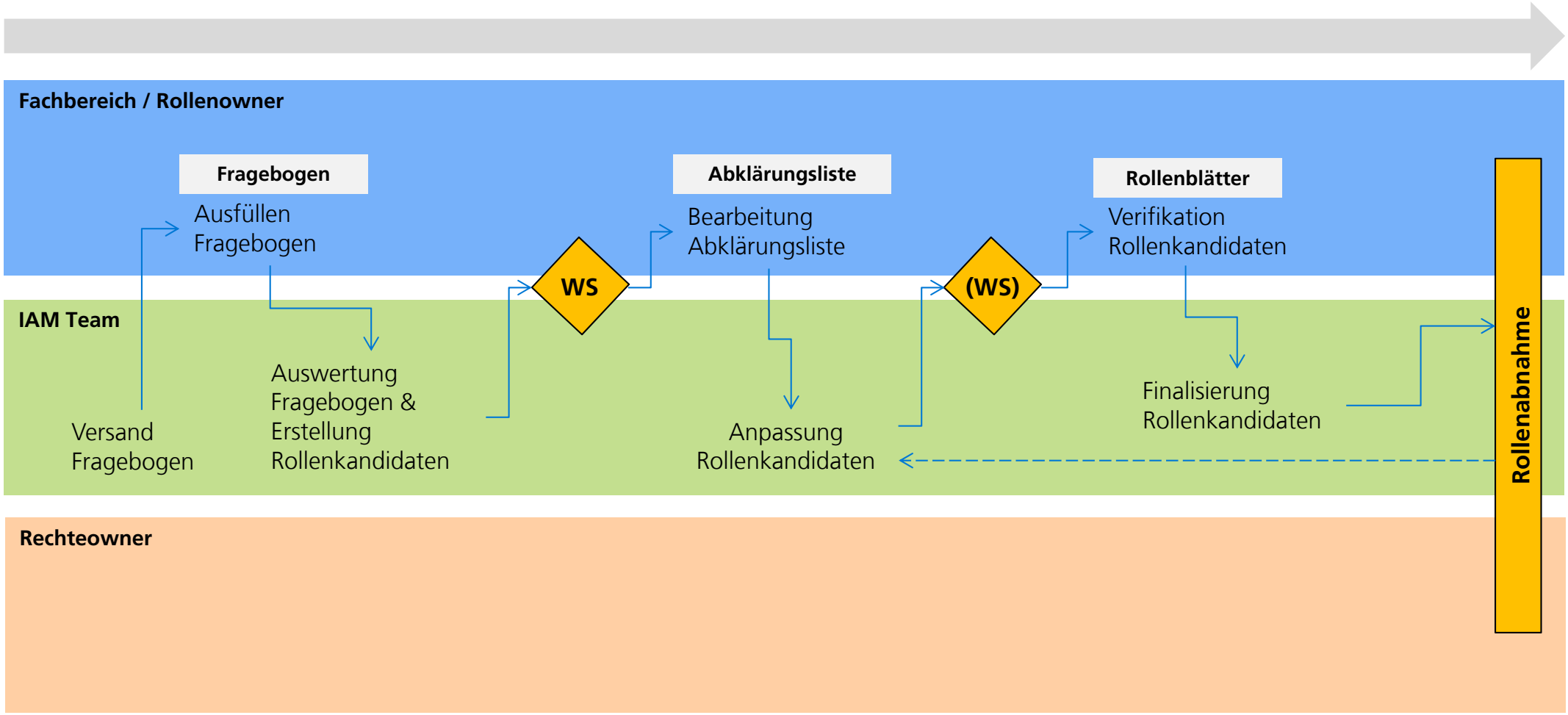
In der Erstrollen-Entwicklung kommt der kombinierte Ansatz zum tragen. Mit Toolunterstützung (Role-Mining) werden Rollenkandidaten gebildet, die in Workshops verifiziert werden.





Zürcher Kantonalbank

Die IAM Erst-Rollenentwicklung erfolgt in enger Zusammenarbeit mit den Geschäftseinheiten. Die Abnahme Erfolgt durch die Rollen- und Rechteowner.



Hinweis: Die Erstzuteilung der IAM-Rollen erfolgt im Rahmen der Migration

Zürcher Kantonalbank

Migration / Rollout

Umstellung der Geschäftseinheiten – gestaffelt

Zürcher Kantonalbank

Die Umstellung der Geschäftsbereiche erfolgt zeitlich gestaffelt und nach einem definierten Vorgehen ab Januar 2014.

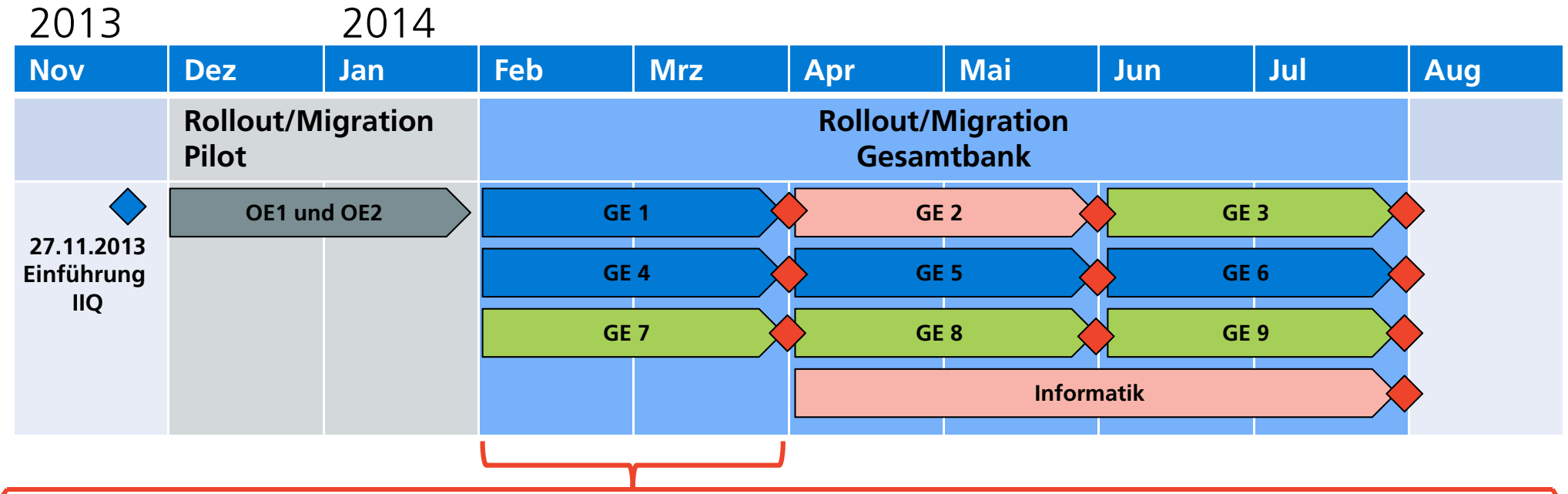
Das Vorgehen im Rollout orientiert sich an folgenden Prinzipien:

- Die Definition der Umstellung inkl. Reihenfolge und Zeitpunkt erfolgt in **Abstimmung** mit den **Stabsleitern** der Geschäftseinheiten
- Es erfolgt eine **zeitnahe Kommunikation** über die bevorstehende Umstellung
- Die **Erstzuteilung** der IAM-Rollen an Mitarbeitende wird **durch die Linie bestätigt**
- Die Geschäftseinheiten werden **während der Umstellung unterstützt** und betreut. (separater Helpdesk, Floorwalker)
- **Kurze Entscheidungswege** wie auch Anpassungen an IAM-Rollen sind gewährleistet.

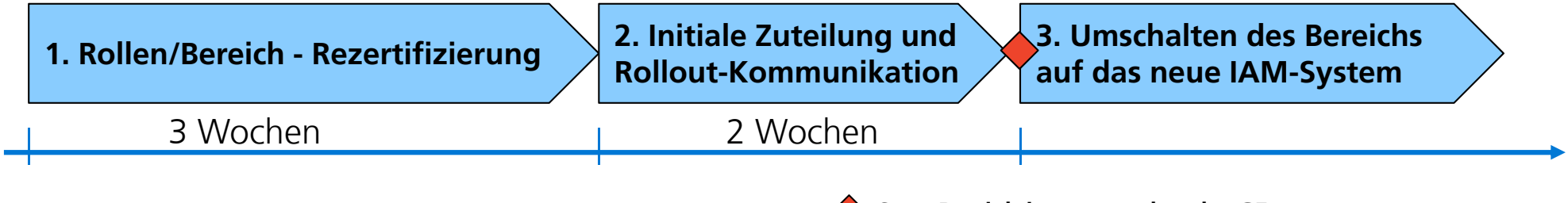
Zürcher Kantonalbank

Der Rollout/Migration durchläuft drei Phasen und dauert in der Regel pro Bereich zwei Monate.

Plan Rollout/Migration (schematisch)



Plan für Vorbereitungsaktivitäten für Rollout/Migration in der einzelnen GE



Zürcher Kantonalbank

«Lessons learned»

Erkenntnisse - was ging gut / wo hatten wir Probleme

Zürcher Kantonalbank

Die Umsetzung eines rollenbasierten IAM bedarf vieler Voraussetzungen, in erster Linie aber der Unterstützung des Top-Managements.

- Top-Management Support ist essentiell
- Fach- und Rollenkonzept muss vorliegen
- Wesentlicher Aufwand fällt auf Fachseite im Projekt an (ohne IT)
- Notwendigkeit von parallelen Teams mit klaren Verantwortlichkeiten
- Kommunikationskonzept unabdingbar
- Mitarbeit der einzelnen Business Units (Bereichsspezialisten) ist essentiell
- «Kenne deine Berechtigungsobjekte» (Berechtigungskonzepte inkl. Klassifikation und Beschreibung)
- Bedarf nach vernünftigen Hilfsmittel (Role-Mining)
- Support durch internal Audit (z.B. im Programm Management Team oder als Programme-Assurance)

Zürcher Kantonalbank

«Lessons learned»

Thema		Positiv	Negativ/Schwierig
Stakeholder-Management, Kommunikation	Geschäftseinheiten wurden via Stäbe frühzeitig einbezogen und in periodischen Meetings und 1Pager «IAM in Kürze» auf dem laufenden gehalten. Ein detailliertes Kommunikationskonzept wurde erarbeitet und wird gelebt. Gesamtbankinfo über IAM-Homepage.	• Top-Down-Kommunikation • Einbezug von Benutzervertretern und Fachbeirat • Zielgruppenorientierte Kommunikation	• Thema IAM auf einfache und verständliche Art zu kommunizieren nicht immer glücklich
Programm-Organisation und Steuerung	Das Programm-Management mit Vertretern aus Fach, IT Lieferant, Entscheidungsträgern und Audit weist umfangreiche Entscheidungskompetenzen auf. Im Eskalationsfall kann (ohne Zeitverzug) direkt das oberste Leitungsgremium einbezogen werden.	• Direkte, schlanke Führung • Schnelle Entscheidungen • Kein Management-Overhead • Key Success Factor = Verzicht auf PSA	• Entscheidungsträger (2. Führungsstufe) fühlten sich teilweise übergangen (da PSA aufgelöst wurde).
Programm-Planung, Termine	Auftrag der GD innerhalb von weniger als 2 Jahren ein neues IAM (gem. Konzept) umzusetzen, führte dazu, dass Fachprojekte und IT Projekte fast gleichzeitig starten mussten. Zudem musste IT-seitig mit Projekt ACS 2.3 eine techn. Basis geschaffen werden.	• Abgestimmte Fach- und IT Projekte • Herausforderung wirkt motivierend auf Teams	• Kein Zurück möglich • Verzögerungen in einem Projekt wirken sich unweigerlich auf den Endtermin aus (zum Glück nicht eingetreten)

Zürcher Kantonalbank

«Lessons learned»

Thema		Positiv	Negativ/Schwierig
Anforderungs-Management	Parallel zum Projekt IAM-ORG, welches die eigentlichen, prozessualen Anforderungen bereitstellte, wurde innert kürzester Zeit (1 Monat) ein umfangreicher Anforderungskatalog (172 Anforderungen) erstellt. Auf diesem Katalog wurde aufgebaut (inkl. Change Management).	• Flexibles Anforderungs-Tool • Kompletter IAM-Afo-Katalog (funktional, nicht funktional) • Change Management Prozess im Projekt	• Prozessuale Anforderungen (Life-Cycle-Modelle) wurden erst sehr spät eingeliefert • Priorisierung für funktionale Anforderungen nicht durch IT Personen
Evaluationsprozess	Innert kürzester Zeit wurde ein kompletter Evaluationsprozess (RfI, PoC, RfP) durchgeführt. Im PoC musste ein kompletter Life-Cycle demonstriert werden.	• Shortlisting Verfahren effektiv • PoC mit funktionalen und nicht funktionalen Kriterien • PPH-Erstellung mit 2 Anbietern	• Zeitlicher Rahmen schränkte Teilnehmer-zahl ein. Wichtige Anbieter konnten nicht berücksichtigt werden. • Paralleler PoC (Kontrahenten im selben Raum)
IAM Organisation, Prozesse und Verantwortliche	Eine umfassende IAM Organisation mit Prozessen und Verantwortlichkeiten wurde parallel zur IT Spezifikation erstellt. Diese Prozesse bildeten die Basis für die zu implementierenden Workflows. Zudem mussten die Berechtigungskonzepte der Applikationen erstellt werden.	• Umfassende Beschreibung der Berechtigungsobjekte und damit Basis für Klassifikation und Rollenbildung	• Operationalisierung (Benennung und Instruktion von neuen Verantwortlichen) verläuft schwierig • Technische Unterstützung Workflows im IAM Tool

Zürcher Kantonalbank

«Lessons learned»

Thema		Positiv	Negativ/Schwierig
Technische Lösung (IAM Tool)	Auf der bestehenden Provisionierungs-Plattform wurde die neue, moderne IAG-Lösung aufgesetzt. Die Implementation der neuen Lösung (Standard) erfolgte in 3 produktiven Einführungen.	• IAM-Suite mit state-of-the-art IAM-Prozessen. • Architektur-Konformität • Rollenimportierungs-Funktionalität aus Offline-Role-Miner-Tool	• «Glaube nicht den Hochglanzprospekten» • Späte Erkenntnisse bezüglich Umsetzbarkeit der IAM Prozesse • User-Interface: erste Eindrücke sollten stärker berücksichtigt werden
Rollenbildung – Methodik und Vorgehen	In Pilot-Versuchen wurde das Rollenbildungs-Verfahren (Combined Approach) bereits vorgängig verifiziert und im IAM Konzept niedergeschrieben. Zudem wurde ein sehr flexibles Role-Miner-Tool entwickelt. Das Rollenbildungsverfahren wurde industrialisiert, damit in der kurzen Zeit alle Bereiche entwickelt werden .	• Flexibles Role-Miner-Tool basierend auf aktuellen Berechtigungsinforma-tionen • Rollenteams und Termin-koordination • GE-Koordinatoren • Industrialisierter Entwicklungsprozess	• Reorganisationen während der Rollen-Entwicklung • Beurteilung der Fachbereiche (wofür wird was benötigt, Spezialfunktionen innerhalb der OE) öfters mangelhaft und führt zu Mehraufwendungen in den Role-Miner-Teams

Zürcher Kantonalbank

Fragen / Diskussion

Stand September 2013: Wir sind in Time / Budget / Quality und werden die Bank im 1. Halbjahr 2014 in eine neue Ära des Berechtigungsmanagements überführen.

Zürcher Kantonalbank

Die nahe Bank

Zürcher Kantonalbank