

Machbarkeitsstudie Entwicklung von Prozessketten zwischen Wirtschaft und Verwaltung: Finanzdienstleistungen



für
Bundesministerium des Innern, Berlin

Autorenteam

Norbert Fröschle (Fraunhofer IAO)
Claus-Peter Praeg (Fraunhofer IAO)
Jürgen Baum (Fraunhofer SIT)
Manfred Gerblinger (Universität Tübingen)
Peter Heiler (Commerzbank AG)
Reiner Kraft (Fraunhofer SIT)
Klaus Kuper (GAD eG)
Lutz Nentwig (Fraunhofer ISST)
Gerhard Ringwald (Universität Tübingen)
Rainer Rosenmüller (Fraunhofer ISST)
Uwe Rubart (GAD eG)

Stuttgart, im Mai 2009

Inhalt

1	Einleitung – Zielsetzung und Fragestellung	25
2	Prozessketten zwischen Wirtschaft und Verwaltung im Bereich FDL	28
2.1	Arbeitsdefinition: Vom Prozessmanagement zum Prozesskettenmanagement	28
2.2	Die Banken-Perspektive	31
2.3	Die E-Government-Perspektive	39
3	Die FDL-Prozesskette in der IST-Situation	46
3.1	Erhebung der IST-Situation – angewandte Vorgehensweise "PRK-Screening"	46
3.2	Erhebung der IST-Situation – Ergebnisse	55
3.2.1	Ergebnis I: Prozessketten Wertschöpfungscluster	55
3.2.2	Ergebnis II: Prozessketten Generationen	59
3.2.3	Ergebnis III: Quantitative und qualitative Ergebnisse	61
3.2.4	Ergebnis IV: Prozesslandkarte und Prozessbibliothek	67
3.2.5	Ergebnis V: Best Practices Bundesbank-Extranet und Kontenstammdatenbereitstellung	72
4	Ziele und Anforderungen für Prozessketten Level-1	79
4.1	Von Prozessketten Level-3 zu Level-1 (Systemebene)	79
4.2	Entwicklung in Generationen – von der fehlenden Steckdose zwischen Wirtschaft und Verwaltung über viele unterschiedliche Steckdosen zu der einen Steckdose (Prozesskettenebene)	82
4.2.1	Das Bild der Steckdose: ...	82
4.2.2	wirtschaftlich, prozessual und organisatorisch, ...	87
4.2.3	IT-architektonisch, ...	92
4.2.4	sicherheitstechnisch und...	97
4.2.5	juristisch	100

4.3	"PRK-Scoping"	105
4.3.1	Generische Vorgehensweise "PRK-Scoping"	105
4.3.2	PRK-Scoping Matrix: Ziele, Indikatoren und Werkzeuge	108
5	Der Bauplan für Prozessketten Level-1	113
5.1	Vorgehensmodell im Überblick: PRK-Screening, PRK-Scoping, PRK-Bauplan	113
5.2	Module zur Ableitung von Handlungsempfehlungen (Selbstanleitung)	114
5.2.1	Die Module im Überblick	114
5.2.2	Modul A "eGOV-Rechner"	115
5.2.3	Modul A "Industrialisierungs-Quick-Check für Banken (IQC)"	118
5.2.4	Submodul E "Betreibermodell und Change Management"	123
5.2.5	Modul B "IT-Architektur und IT-Governance für Prozessketten"	131
5.2.6	Modul C "IT-Sicherheitsmechanismen und Regelwerke für Prozessketten"	136
5.2.7	Modul D "Die rechtssichere Prozesskette"	139
5.3	Das Vorgehen zur PRK-Levelanhebung im Überblick	142
6	Zwei Fallbeispiele: Private Immobilienfinanzierung und Geldwäscheverdachts-Anzeige	144
7	Prozesskettenanalyse I: Private Immobilienfinanzierung (IMMO)	147
7.1	Die IST-Prozesskette	149
7.1.1	Wirtschaftliche, prozessuale und organisatorische Beschreibung und Analyse	156
7.1.2	IT-architektonische Beschreibung und Analyse	182
7.1.3	Sicherheitstechnische Beschreibung und Analyse	188
7.1.4	Juristische Beschreibung und Analyse	192
7.2	Ziele und Anforderungen an die Prozesskette Level-1	196
7.3	Die Prozesskette Level-1	199
7.3.1	Wirtschaftliche, prozessuale und organisatorische Beschreibung und Analyse	201
7.3.2	IT-architektonische Beschreibung und Analyse	211
7.3.3	Sicherheitstechnische Beschreibung und Analyse	219

7.3.4	Juristische Beschreibung und Analyse	219
7.4	Handlungsempfehlungen	226
7.5	Ansätze zur Gestaltung neuer Geschäfts- und Betreibermodelle	230
8	Prozesskettenanalyse II: Geldwäscheverdachts-Anzeige (GVA)	231
8.1	Die IST-Prozesskette	231
8.1.1	Wirtschaftliche, prozessuale und organisatorische Beschreibung und Analyse	234
8.1.2	IT-architektonische Beschreibung und Analyse	239
8.1.3	Sicherheitstechnische Beschreibung und Analyse	240
8.1.4	Juristische Beschreibung und Analyse	242
8.2	Ziele und Anforderungen an die Prozesskette Level-1	248
8.3	Die Prozesskette Level-1	251
8.3.1	Wirtschaftliche, prozessuale und organisatorische Beschreibung und Analyse	252
8.3.2	IT-architektonische Beschreibung und Analyse	258
8.3.3	Sicherheitstechnische Beschreibung und Analyse	262
8.3.4	Juristische Beschreibung und Analyse	264
8.4	Handlungsempfehlungen	269
8.5	Ansätze zur Gestaltung neuer Geschäfts- und Betreibermodelle	273
9	Ausblick	275
10	Referenzen	280
11	Glossar	291
12	Abkürzungsverzeichnis	300
13	Das Autorenteam	308

Abbildungsverzeichnis

Abbildung 1: Gesamtvorgehensmodell in Wirkkreisen (Quelle: Eigene Darstellung).....	26
Abbildung 2: Schematische Darstellung eines Prozesses (Quelle: Krcmar 2003: 100).....	29
Abbildung 3: Ziele und Erwartungen von Banken hinsichtlich Industrialisierung (Quelle: Spath / Engstler / Praeg / Vocke 2008).....	33
Abbildung 4: Industrialisierungspotenziale aus Sicht von Banken (Quelle: Spath / Engstler / Praeg / Vocke 2008).....	35
Abbildung 5: Maßnahmen zur Erschließung der Industrialisierungspotenziale bei Banken (Quelle: Spath / Engstler / Praeg / Vocke 2008).....	36
Abbildung 6: Branchenkompass Finanzdienstleister (Quelle: Eigene Darstellung)	49
Abbildung 7: Die PRK Pyramide (Quelle: Eigene Darstellung)	51
Abbildung 8: Prozessorientierte Sicht auf eine Bankorganisation (Quelle: Eigene Darstellung)	56
Abbildung 9: Ergebnis – PRK Wertschöpfungscluster (Quelle: Eigene Darstellung)	59
Abbildung 10: Ergebnis – PRK Generationen (Quelle: Eigene Darstellung).....	60
Abbildung 11: Ergebnis – Häufigkeitsverteilung der Wertschöpfungscluster (Bankensektor) in der FDL-PRK (Quelle: Eigene Darstellung)	62
Abbildung 12: Ergebnis – Häufigkeitsverteilung der involvierten Akteure (Verwaltung) in der FDL-PRK (Quelle: Eigene Darstellung)	63
Abbildung 13: Ergebnis – Häufigkeitsverteilung von Generation G3, G2 und G1 in der FDL-PRK (Quelle: Eigene Darstellung).....	64
Abbildung 14: Prozesslandkarte für die identifizierten PRK zwischen Verwaltung und FDL (Quelle: Eigene Darstellung).....	68
Abbildung 15: Systematische Visualisierung von PRK mittels Prozesskettenbrowser (Quelle: Eigene Darstellung).....	69
Abbildung 16: Ergebnis – Die PRK "Geldwäscheverdachts-Anzeige" im Prozesskettenbrowser (Quelle: Eigene Darstellung).....	70
Abbildung 17: Ergebnis – Die Prozesslandkarte FDL-PRK in Deutschland im Prozesskettenbrowser (Quelle: Eigene Darstellung).....	71
Abbildung 18: Allgemeine IST IT-Architektur zwischen FDL und Verwaltung (FMC) (Quelle: Eigene Darstellung).....	73
Abbildung 19: Best Practice Architektur Bundesbank ExtraNet (FMC) (Quelle: Eigene Darstellung)	74
Abbildung 20: Best Practice PRK Meldeprozess Basel II (Process Support Map) (Quelle: Eigene Darstellung).....	75
Abbildung 21: Best Practice Architektur Abruf Konteninformationen bei Bank-Verlag (FMC) (Quelle: Eigene Darstellung).....	76
Abbildung 22: Best Practice PRK Abruf Konteninformationen (Process Support Map) (Quelle: Eigene Darstellung).....	77
Abbildung 23: PRK Levels nach BMI (Quelle: BMI 2007: 4)	80
Abbildung 24: PRK Level Anhebung auf Systemebene (Quelle: Eigene Darstellung).....	81

Abbildung 25: PRK der Generation G1 (Quelle: Eigene Darstellung)	84
Abbildung 26: PRK der Generation G2 (Quelle: Eigene Darstellung)	85
Abbildung 27: PRK der Generation G3 (Quelle: Eigene Darstellung)	86
Abbildung 28: Prozessoptimierung durch Innovation (Quelle: Mormmann / Hillesheimer / Metzler / Zahn 2006).....	90
Abbildung 29: Allgemeine Architektur von Trust-Domains (Quelle: SAFE 2007: 18).....	94
Abbildung 30: Tokenvermittlung im System SAFE (Quelle: SAFE 2007: 30).....	95
Abbildung 31: Architektur der Standards für sichere Webservices (Quelle: Kulisch 2007).....	96
Abbildung 32: Phasen des IT-Sicherheitsprozesses (Quelle: BSI 2008b)	98
Abbildung 33: Die IT-Grundschatz-Kataloge mit dem Schichtenmodell (Quelle: BSI 2008b).....	99
Abbildung 34: PRK Levels und Generationen (Quelle: Eigene Darstellung).....	105
Abbildung 35: Gesamtvorgehensmodell in Wirkkreisen (Quelle: Eigene Darstellung).....	113
Abbildung 36: Werkzeug-Module des Anhangs im Überblick (Quelle: Eigene Darstellung)	115
Abbildung 37: Struktur des IQC (Quelle: Praeg 2008c).....	119
Abbildung 38: Vorgehensschritte zur Nutzung des IQC (Quelle: Eigene Darstellung).....	121
Abbildung 39: Überblick und Struktur des Moduls Betreibermodelle und Change Management (Quelle: Eigene Darstellung).....	123
Abbildung 40: Vorgehensmodell zur Gestaltung von Betreibermodellen	127
Abbildung 41: Vorgehen im organisatorischen Change Management (Quelle: Eigene Darstellung)....	129
Abbildung 42: Vorgehen IT-Transformation (Quelle: Eigene Darstellung)	132
Abbildung 43: Die Architekturpyramide - IT-Architektur nach Architekturkonzept des Bundes (Quelle: KBSSt 2007: 5)	133
Abbildung 44: Beispiel für eine Process Support Map (Quelle: Eigene Darstellung)	135
Abbildung 45: Arbeitsschritte zur Levelanhebung im Überblick (Quelle: Eigene Darstellung)	142
Abbildung 46: IMMO IST-Situation Lebenszyklus Kreditbearbeitung (Quelle: Eigene Darstellung)	149
Abbildung 47: IMMO IST-Prozesskette Immobilienfinanzierung Neugeschäft (I) (Quelle: Eigene Darstellung).....	151
Abbildung 48: IMMO IST-Prozesskette Immobilienfinanzierung Neugeschäft (II) (Quelle: Eigene Darstellung).....	152
Abbildung 49: IMMO IST-Prozesskette Immobilienfinanzierung Pflege (Quelle: Eigene Darstellung) .	153
Abbildung 50: IMMO IST-Prozesskette Immobilienfinanzierung Pflege Rückständigkeit (Quelle: Eigene Darstellung).....	154
Abbildung 51: IMMO IST-Prozesskette Immobilienfinanzierung Pflege Vertragsauflösung (Quelle: Eigene Darstellung).....	155
Abbildung 52: IMMO Überblick Prozesskette Immobilienfinanzierung mit Teilprozessen (Quelle: GAD eG).....	156
Abbildung 53: IMMO Teilprozess Kundenberatung (Quelle: GAD eG)	160
Abbildung 54: IMMO Teilprozess Kreditantrag (Quelle: GAD eG)	163
Abbildung 55: IMMO Teilprozess Kreditvertrag (Quelle: GAD eG)	165
Abbildung 56: IMMO Teilprozess Kreditgenehmigung (Quelle: GAD eG).....	168
Abbildung 57: IMMO Teilprozess Kreditabschluss (Quelle: GAD eG).....	171
Abbildung 58: IMMO Teilprozess Bonitätsunterlagen (Quelle: GAD eG).....	174
Abbildung 59: IMMO Teilprozess Rückständigkeit (Quelle: GAD eG).....	177
Abbildung 60: IMMO Teilprozess Vertragsauflösung (Quelle: GAD eG).....	180

Abbildung 61: IMMO und die beteiligten Parteien (Quelle: Eigene Darstellung).....	183
Abbildung 62: IMMO Process Support Map für die Prozesskette "Private Immobilienfinanzierung" (Quelle: Eigene Darstellung).....	184
Abbildung 63: IMMO IST-Architektur Förderinstitut (Quelle: Eigene Darstellung)	185
Abbildung 64: IMMO IST-Architektur Grundbuchamt (Einsicht) (Quelle: Eigene Darstellung).....	186
Abbildung 65: IMMO IST-Architektur des Grundbuchamt (Grundschild) (Quelle: Eigene Darstellung).....	187
Abbildung 66: IMMO Datenaustausch zwischen Bank und Förderinstitut (Quelle: Eigene Darstellung).....	189
Abbildung 67: IMMO Dateneinsicht Grundbuch (Quelle: Eigene Darstellung)	190
Abbildung 68: IMMO Datenaustausch Grundbuch (Quelle: Eigene Darstellung).....	191
Abbildung 69: IMMO SOLL-Prozesskette zur privaten Immobilienfinanzierung (Quelle: Eigene Darstellung).....	200
Abbildung 70: IMMO SOLL-Prozesskette private Immobilienfinanzierung I (Quelle: Eigene Darstellung).....	201
Abbildung 71: IMMO SOLL-Prozesskette private Immobilienfinanzierung II (Quelle: Eigene Darstellung).....	202
Abbildung 72: IMMO SOLL-Prozesskette private Immobilienfinanzierung III (Quelle: Eigene Darstellung).....	203
Abbildung 73: IMMO Prinzipbild Fördermittelberatung-Beantragung (Quelle: Eigene Darstellung)	204
Abbildung 74: IMMO SOLL-Prozesskette private Immobilienfinanzierung Pflegeprozess (Quelle: Eigene Darstellung).....	208
Abbildung 75: IMMO Teilprozess Rückständigkeit (Quelle: Eigene Darstellung).....	209
Abbildung 76: IMMO SOLL-Prozess Vertragsauflösung (Quelle: Eigene Darstellung).....	210
Abbildung 77: IMMO SOLL-Architektur Förderinstitut (Quelle: Eigene Darstellung).....	212
Abbildung 78: IMMO Das Architekturmuster für die Kommunikation mit dem Förderinstitut (Quelle: Eigene Darstellung).....	214
Abbildung 79: IMMO Das Architekturmuster für die Kommunikation mit dem Grundbuchamt (Quelle: Eigene Darstellung).....	217
Abbildung 80: IMMO SOLL-Architektur Grundbuchamt (Quelle: Eigene Darstellung).....	218
Abbildung 81: GVA IST-Verfahrensübersicht (Quelle: BKA 2008b).....	233
Abbildung 82: GVA IST-Prozesskette (EPK) (Quelle: Eigene Darstellung).....	235
Abbildung 83: GVA IST-Architektur (FMC) (Quelle: Eigene Darstellung).....	239
Abbildung 84: GVA Gang des Strafverfahrens – Kenntniserlangung der Strafverfolgungsorgane (Quelle: Eigene Darstellung).....	245
Abbildung 85: GVA SOLL-Verfahrensübersicht nach Projekt eVA (Quelle: Eigene Darstellung)	251
Abbildung 86: GVA Prozesskette Level-1 (EPK) (Quelle: Eigene Darstellung)	254
Abbildung 87: GVA Architektur Level-1 für Projekt eVA (FMC) (Quelle: Eigene Darstellung)	260

Tabellenverzeichnis

Tabelle 1: Wissenschaftlicher Ansatz von PRK-Screening am Beispiel der Untersuchung der FDL-Prozesskette in Deutschland	48
Tabelle 2: Legende zu den Architekturdarstellungen (FMC)	54
Tabelle 3: Legende zur Prozessmodellierung mittels EPK.....	55
Tabelle 4: Wertschöpfungskuster Banksektor	58
Tabelle 5: PRK-Scoping Matrix: Ziele, Indikatoren und Werkzeuge.....	112
Tabelle 6: Betreibermodelle: Anbieter- vs. Nachfragerseite	125
Tabelle 7: Gestaltungsfelder von Betreibermodellen (Quelle: Eigene Darstellung, in Anlehnung an Schulz et al. 2008: 69)	126
Tabelle 8: Vorgehensweise für Change Management.....	131
Tabelle 9: Systematische Beschreibung der PRK IMMO im Überblick	159
Tabelle 10: Systematische Beschreibung TP "Kundenberatung und –bewertung"	162
Tabelle 11: Systematische Beschreibung des TP "Kreditantrag bearbeiten"	165
Tabelle 12: Systematische Beschreibung des TP "Kreditvertrag erstellen"	167
Tabelle 13: Systematische Beschreibung des TP "Kreditantrag genehmigen und Kundenunterschrift einholen"	170
Tabelle 14: Systematische Beschreibung des TP "Kreditvertrag bearbeiten"	173
Tabelle 15: Systematische Beschreibung des TP "Bonitätsunterlagen auswerten"	176
Tabelle 16: Systematische Beschreibung des TP "Rückständigkeit bearbeiten"	179
Tabelle 17: Systematische Beschreibung des TP "Darlehnsvertrag auflösen"	182
Tabelle 18: Empirische Varianten der Kommunikation in Prozessketten	216
Tabelle 19: Prozesszeiten für die Prozesskette "Private Immobilienfinanzierung" (Quelle: BVR Projekt "VR-Process").....	225

Anhang

Anhang I - Prozessbibliothek

FDL-Prozesskette in Deutschland – Ergebnistabelle des PRK-Screenings

Anhang II – Werkzeuge für Prozessketten

Modul A "eGOV-Rechner"

Modul A Industrialisierungs-Quick-Check für Banken ("IQC")

Submodul E "Betreibermodell und Changemanagement"

Modul B "IT-Architektur und IT-Governance für Prozessketten"

Modul C "IT-Sicherheitsmechanismen und Regelwerke für Prozessketten"

Modul D "Die rechtssichere Prozesskette"

Dank

Wir bedanken uns beim Auftraggeber, dem Bundesministerium des Innern, für die gute und konstruktive Zusammenarbeit.

Ebenso bedanken wir uns bei der Vielzahl von Personen und Institutionen, die uns auf Banken- und Verwaltungsseite mit Rat, Tat und Expertise beim Gelingen der Studie unterstützt haben.

Unser besonderer Dank gilt dem Statistisches Bundesamt, Arbeitsbereich I - SKM, namentlich Herrn Vorgrimler, Herrn Zipse und Frau Grabow, für die Beratung und Datenanalyse in Sachen Standardkosten-Modell.

Wir bedanken uns besonders bei der Commerzbank AG und ihrem Zentralen Stab Zentrale- und Filialorganisation und ihrer Group Compliance für die gewährten Einblicke und die wertvollen Beiträge für diese Machbarkeitsstudie.

Weiterhin bedanken wir uns bei den Mitarbeiterinnen und Mitarbeitern der GAD eG aus den Bereichen Portfoliomanagement, Risiko- und Qualitätsmanagement und ebenso bei den Mitarbeiterinnen und Mitarbeitern des Rheinisch-Westfälischen Genossenschaftsverbandes e.V. aus dem Bereich "Prüfung Banken" für die wertvolle Unterstützung.

Des weiteren möchten wir uns für die Mitarbeit bedanken bei Ruslana Brull, Achim Gölz, Elena Elyas, Björn May, Florian Schmid, Susann Schreckebach (Fraunhofer IAO), Mechthild Stöwer (Fraunhofer SIT) und Alexander Auch (Uni Tübingen).

Zweck des Dokuments

Zweck des Dokuments ist es, der interessierten Öffentlichkeit das Konzept und die Anwendung von organisations- und branchenübergreifenden "Prozessketten" (PRK) nahe zu bringen.

Das Management von organisationsübergreifenden Prozessketten wird eine der zentralen Herausforderungen sowohl für Unternehmen als auch für die öffentlichen Verwaltungen in den kommenden Jahren darstellen. Obwohl das Management von Geschäftsprozessen seit Jahren und Jahrzehnten zum Repertoire vieler Unternehmen zählt, werden zukünftige Effizienz- und Effektivitätssteigerungen vor allem durch die Optimierung von organisationsübergreifenden Prozessketten erreicht werden können. Um diese Potenziale identifizieren und beschreiben zu können, werden im Rahmen dieser Machbarkeitsstudie verschiedene Methoden und Instrumente aufgezeigt, die den Entscheidungsträgerinnen und Entscheidungsträgern¹ in Wirtschaft und Verwaltung entsprechend Hilfestellung bei dieser komplexen Herausforderung geben sollen.

Wesentliche Elemente der Machbarkeitsstudie sind die zwei im Projektverlauf entwickelten Methoden "PRK-Screening" und "PRK-Scoping", die Anwenderinnen und Anwendern im Zusammenspiel mit den Werkzeugen im Anhang II bei der Konzeption einer Prozesskette (Herausforderung Neugestaltung und Optimierung) und der damit verbundenen Chancen und Risiken unterstützen sollen (Prinzip Self-Customisation und Selbstanwendung).

¹ Die Studie bemüht sich, die sprachliche Gleichbehandlung von Männern und Frauen im Text des Dokuments durchgängig umzusetzen. Grundlage bietet hierbei das BBB-Merkblatt "Sprachliche Gleichbehandlung von Frauen und Männern. Hinweise, Anwendungsmöglichkeiten und Beispiele" von Bundesverwaltungsamt – Bundesstelle für Büroorganisation und Bürotechnik (BVA BBB 2002). Dies gilt auch für die Abbildungen und Tabellen soweit in der Darstellung möglich.

Von der Erhebung der Prozessketten in der IST-Situation (PRK-Screening) über Ziele und Anforderungen für Prozessketten Level-1 (PRK-Scoping) zur Ableitung eines strategischen Bauplans und operativen Handlungsempfehlungen (PRK-Bauplan) – dieser Gedankenschlag bildet den übergreifenden roten Faden der Studie. Die Theorie wird empirisch angewandt auf die existierende gesamte FDL-Prozesskette in Deutschland in der IST-Situation sowie fallstudienbezogen auf zwei ausgewählte Prozessketten zwischen Wirtschaft und Verwaltung, nämlich die Prozessketten "Private Immobilienfinanzierung" und "Geldwäscheverdachts-Anzeige".

Diese Studie adressiert folgende Zielgruppen:

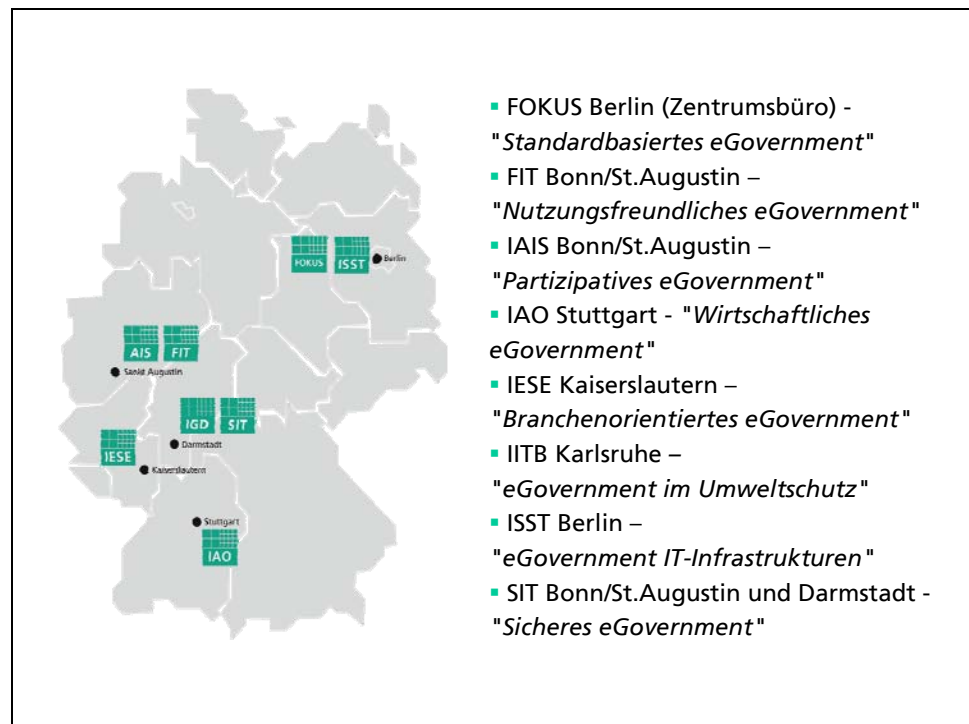
- Entscheidungsträgerinnen und Entscheidungsträger in E-Government und E-Business
- Praktikerinnen und Praktiker in E-Government und E-Business
- Prozessverantwortliche bei Finanzdienstleistern und in öffentlichen Verwaltungen
- Wissenschaftlerinnen und Wissenschaftler in Forschung und Lehre

Das Autorenteam bedankt sich bei der geneigten Leserin und dem geneigten Leser. Wir sind stets bemüht die Qualität unserer wissenschaftlichen und praktischen Ergebnisse zu verbessern. Vielen Dank im voraus wenn Sie uns bitte Ihre Kritikpunkte und Anregungen zu dieser Studie mitteilen.

Über uns

Das Autorenteam der Machbarkeitsstudie stammt aus zwei großen Netzwerken, zum einen dem "Fraunhofer eGovernment Zentrum", zum anderen dem Innovationsforum "Bank & Zukunft".

Fraunhofer eGovernment Zentrum (www.egov-zentrum.fraunhofer.de)



Das Fraunhofer eGovernment Zentrum bündelt die Kompetenzen von acht Fraunhofer-Instituten in einem bundesweiten Netzwerk. Jedes der Institute verfügt über langjährige Erfahrungen mit jeweils unterschiedlichen technologischen und organisatorischen Schwerpunkten im Anwendungsbereich "Öffentliche Verwaltung". Das Zentrum unterstützt die Konzeption und die Umsetzung ganzheitlicher zukunftsweisender Lösungen. Das Fraunhofer eGovernment Zentrum berät Politik, Verwaltung und Wirtschaft bei der Konzeption und der strategischen Entwicklung von E-Government sowie bei der Umsetzung von Architekturen und Standards. Das Fraunhofer eGovernment Zentrum ist unabhängig von herstellereinspezifischen Lösungen und politischen

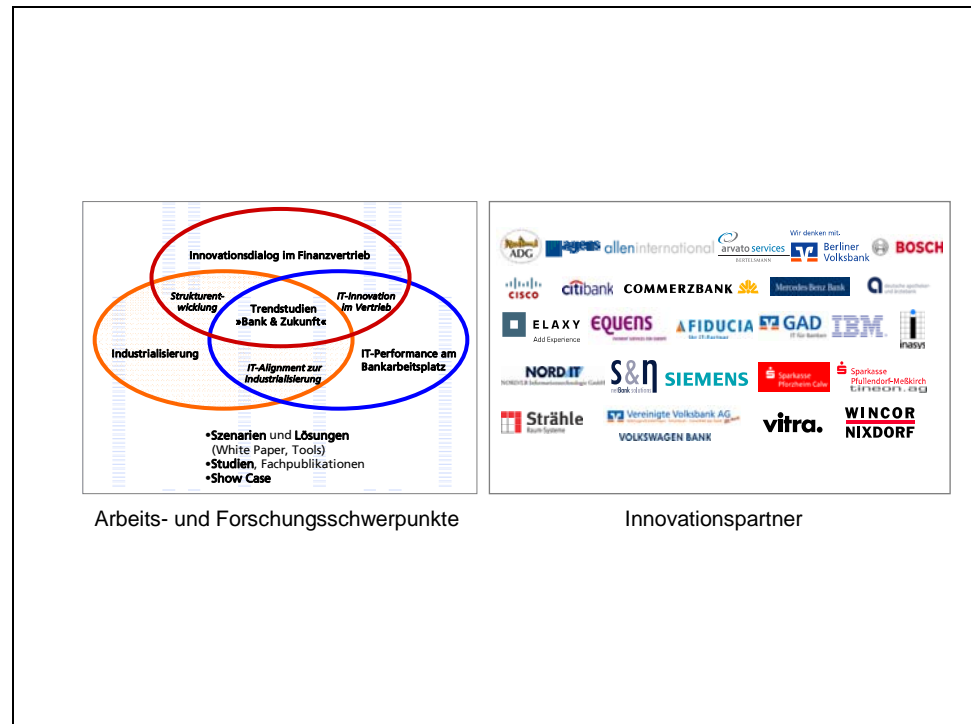
Entwicklungen. Beratung und Lösungsentwicklungen erfolgen eng an den Bedürfnissen der jeweiligen Zielgruppe und Anwendungsdomäne.

Die Mitgliedsinstitute des Fraunhofer eGovernment Zentrums führen gemeinschaftlich E-Government Projekte durch und bringen dabei ihre spezifischen Kernkompetenzen ein.

An dieser Studie haben aus den Fraunhofer eGovernment Zentrum die drei Institute mit folgenden inhaltlichen Schwerpunkten mitgearbeitet:

- Fraunhofer-Institut für Arbeitswirtschaft und Organisation IAO:
Prozesskettenanalyse und Projektleitung
- Fraunhofer-Institut für Software- und Systemtechnik ISST:
IT-Architekturen und -Infrastrukturen
- Fraunhofer-Institut für Sichere Informationstechnologie SIT:
Sicherheit

Innovationsforum "Bank & Zukunft" (www.bankundzukunft.de)



Das Innovationsforum "Bank & Zukunft" richtet sich an interessierte Unternehmen, die ein vitales Interesse an der Weiterentwicklung bestehender Geschäftsmodelle sowie an der Ausschöpfung der Innovationspotenziale neuer Technologien haben. Es ist als Verbundforschungsprojekt konzipiert, das unter der Leitung von Fraunhofer IAO einen moderierten Innovationsprozess unter Einbeziehung von Wissenschaft und Praxis initiiert und konstruktiv fördert. Hierzu werden Strategien und Konzepte für die Bank der Zukunft aus Sicht der Banken und der IT-Lösungsanbieter im Innovationsforum "Bank & Zukunft" kombiniert.

Unter wissenschaftlicher Leitung von Fraunhofer IAO bündeln im Innovationsforum "Bank & Zukunft" zahlreiche Banken und IT-Dienstleister der Finanzbranche ihre Kompetenzen zu Zukunftsfragen im Bankensektor. Ziel ist es, gemeinsam marktorientierte Gestaltungschancen sowie strukturelle und technische Optimierungspotenziale zu identifizieren. Es werden Anwenderinnen und Anwender mit Herstellern von Technologien im Bankenbereich zusammengeführt und die notwendigen Innovationsprozesse initiiert.

Im Rahmen der Machbarkeitsstudie zur Entwicklung von Prozessketten zwischen Banken und öffentlicher Verwaltung waren die Commerzbank AG, die GAD eG und das Fraunhofer IAO an den Projektarbeiten wesentlich beteiligt.

Zusammenfassung

Die Gestaltung von branchenübergreifenden Prozessketten (PRK) trägt entscheidend zur Verbesserung der Zusammenarbeit von Wirtschaft und öffentlicher Verwaltung bei. Dadurch wird es allen beteiligten Akteuren ermöglicht, wahrnehmbare Effizienzpotenziale zu erschließen.

Im Rahmen der Machbarkeitsstudie "Entwicklung von Prozessketten zwischen Wirtschaft und Verwaltung: Finanzdienstleistungen" haben das Fraunhofer-Institut für Arbeitswirtschaft und Organisation IAO, das Fraunhofer-Institut für Software- und Systemtechnik ISST und das Fraunhofer-Institut für Sichere Informationstechnologie SIT, die Commerzbank AG, die GAD eG und die Universität Tübingen die Potentiale für die Konzeption und Umsetzung von Prozessketten zwischen Finanzdienstleistern und Verwaltungen systematisch analysiert und evaluiert. Der Fokus der Untersuchung lag dabei auf einer branchenweiten Prozessintegration, bei der Prozessketten, die sich über mehrere Wertschöpfungsstufen erstrecken, mit Informationspflichten und Verfahren von Banken und Behörden verknüpft wurden.

Zu Beginn wurden 154 Prozessketten anhand eines Untersuchungsmodells analysiert und mittels eines definierten Rasters beschrieben. Auf Grundlage dieser Erkenntnisse wurde ein mehrstufiges Vorgehensmodell zur Identifikation, Gestaltung und Optimierung von Prozessketten entwickelt. Dieses unterstützt die Evaluation von branchenübergreifenden (sogenannten Level-1) Prozessketten im Finanzwesen hinsichtlich deren Machbarkeit und Potenziale. Das Vorgehensmodell beinhaltet ein Screening und Scoping von PRK und zeigt anhand eines Bauplans gezielte Gestaltungsansätze von organisationsübergreifenden Prozessketten auf.

Das Screening ist eine wissenschaftliche und praxisorientierte Methode, um Prozessketten in Bezug auf deren wichtigsten Merkmale und Ausprägungen zu analysieren und zu beschreiben. Dabei werden unterschiedliche Sichten auf die Prozessketten berücksichtigt (fachlich, IT-architektonisch, IT-sicherheitstechnisch und juristisch). Die entwickelte Methode lässt sich je nach Einsatzzweck auf unterschiedliche Analyseebenen anpassen.

Das Scoping adressiert eine Methode, um geeignete Ziele für Prozessketten auswählen bzw. beschreiben zu können. Bei der Anwendung der Methode werden unterschiedliche Zieldimensionen berücksichtigt (wirtschaftlich/organisatorisch, IT-architektonisch, IT-sicherheitstechnisch und juristisch).

Die IST-Analyse zeigt, dass einerseits bei Banken eine Vielzahl verschiedener Organisationsbereiche involviert ist, andererseits eine große Anzahl unterschiedlicher Einrichtungen der öffentlichen Verwaltung adressiert wird. Dabei zeigen die Analysen, dass bei den meisten PRK Informationen, mangels nicht vorhandener Infrastrukturen und gesetzlicher Regelungen, zwischen Banken und der Verwaltung noch immer auf traditionelle Weise mit Papierdokumenten ausgetauscht werden. Dagegen werden in einigen Bereichen von Seiten der Bundesbank und BaFin schon leistungsfähige Portallösungen bereitgestellt, welche einen medienbruchfreien Ablauf der PRK ermöglichen können. Konkret stellte sich heraus, dass Banken eine große Anzahl von Interaktionen mit der Bundesbank (44,2 Prozent) und der BaFin (40,8 Prozent) besitzen. Beide Institutionen bieten bereits heute über ein Extranet bzw. ein Portal Dienste für die Meldung von Daten der Banken an. Dabei werden vordefinierte Datenschnittstellen (XML-Schemata) zugrunde gelegt, die eine hervorragende Voraussetzung für die Weiterentwicklung der IT-Infrastruktur darstellen.

Zur Evaluierung des entwickelten Modells wurden zwei Fallstudien (Private Immobilienfinanzierung und Geldwäscheverdachts-Anzeige) erstellt und sowohl das Vorgehen zur Gestaltung als auch zur Optimierung von PRK angewendet.

Im ersten Fallbeispiel wurde eine organisationsübergreifende Prozesskette für einen privaten Immobilienkredit entwickelt, da diese viele verschiedene Akteure aus dem Finanzdienstleistungsbereich sowie der öffentlichen Verwaltung (Bundesanzeiger, Amtsgericht, Grundbuchamt, Finanzamt, Kreditanstalt für Wiederaufbau etc.) adressiert. Durch die Anwendung der oben genannten Methoden konnten in der Beschreibung der SOLL-Prozesskette erhebliche Optimierungspotentiale in Bezug auf Kosten, Zeit und Qualität aufgezeigt werden. Als Ergebnis lässt sich festhalten, dass insbesondere die Schnittstellen zum Nachweis des Einkommenssteuerbescheids und Einkommensnachweises (Finanzamt / Elster, IT-Verfahren ELENA) und zum Grundbuchamt (siehe dazu auch Arbeiten im Rahmen der "Initiative Finanzstandort Deutschland") zu optimieren sind. Ergänzend dazu ist der Aufbau einer Sicherheitsinfrastruktur notwendig, da sie eine Grundlage für andere Prozessketten darstellt (u. a. Einführung und angemessene Nutzung fortgeschrittener und qualifizierter elektronischer Signaturen, Einführung einer auf Trusted Domains basierenden standardisierten Sicherheitsinfrastruktur mit einem flexiblen verteilten Identity-Management). Um diese Prozesskette wie in der Fallstudie dargestellt nachhaltig betreiben zu können, ist die Einführung und Nutzung des elektronischen Personalausweises (ePA) erforderlich. Dieser bietet die Möglichkeit zur Bereitstellung und Anwendung der elektronischen Signatur.

Im zweiten Fallbeispiel wurde eine medienbruchfreie Prozesskette für Verdachtsanzeigen zur Meldung eines Geldwäschestraftatbestands entwickelt. Ausgangspunkt für dieses Fallbeispiel war das Projekt elektronische Verdachtsanzeige (eVA), in dem bereits ein Grobkonzept für eine elektronische Verdachtsanzeige entworfen worden war. Dort wurde eine Portallösung konzipiert, welche Banken die Möglichkeit eröffnet, ihre Verdachtsanzeigen ausschließlich auf elektronischen Weg an das Bundeskriminalamt zu melden. Von Seiten der Banken besitzen die Erfüllung hoher Sicherheitsanforderungen und die Möglichkeit der Informationstransparenz über den aktuellen Stand des Verfahrens oberste Priorität bei der Realisierung der Portallösung.

Die Erkenntnisse aus den beiden Fallstudien sind in mehreren Handlungsfeldern sowohl für Banken als auch öffentliche Verwaltungen dokumentiert. Unter anderem beziehen sich diese auf die Professionalisierung des Managements von Prozessketten sowie den Aufbau geeigneter Infrastrukturen. Diese unterstützen bzw. ermöglichen die Umsetzung von organisationsübergreifenden und medienbruchfreien PRK.

Ferner ist es möglich, aufgrund von Synergien mit anderen Deutschland-Online Projekten die Realisierung der infrastrukturellen Voraussetzungen beschleunigen zu können, welche bereits heute geeignete Basisdienste einer deutschlandweiten IuK-Infrastruktur geschaffen haben, die bei der Umsetzung von Prozessketten zwischen Banken und Einrichtungen der öffentlichen Verwaltungen genutzt werden können. Ebenso kann bei der Definition von Datenübergabestellen zwischen Prozessketten auf Arbeiten aus den Deutschland-Online Vorhaben zur Standardisierung (XÖV-Standards) zurückgegriffen werden. Entsprechend lassen sich die prototypischen Umsetzungen von ausgewählten Verfahren (z. B. Umsetzung Teile der Prozesskette Kreditvergabe unter Einbeziehung des ePA und der IT-Verfahren Elster und ELENA bzw. der Grundbuch-Verfahren) als Blaupause für weitere Prozessketten und Verfahren dienen, welche die Machbarkeit von Level-1 Prozessketten zeigen.

Neben den identifizierten IT-bezogenen Handlungsfeldern werden in der Machbarkeitsstudie Ansätze für neue Betreiber- und Geschäftsmodelle im Rahmen des Managements von PRK skizziert.

Um das Ziel der praktischen Implementierung von Level-1 PRK erreichen zu können und damit die Realisierung einer im übertragenen Sinne, elektronischen Steckdose zwischen Wirtschaft und Verwaltung zu schaffen, ist die Visualisierung von Prozessketten ("Prozesslandkarte") ein weiterer wichtiger Aspekt. Diese Prozesslandkarte ermöglicht die Erschließung von Wissen über die Prozesskette sowie Informationen über die Zusammenhänge mehrerer PRK in einer "Prozessbibliothek" abzubilden. Diese können von Ent-

scheidungsträgerinnen und Entscheidungsträgern, Anwenderinnen und Anwender, Kundinnen und Kunden sowie der interessierten Öffentlichkeit genutzt werden.

Zusammenfassend kann festgestellt werden, dass Level-1 Prozessketten zwischen Finanzdienstleistern und Einrichtungen der öffentlichen Verwaltung nicht nur von der Wirtschaftsseite gewünscht, sondern auch, wie in den beiden Fallbeispiele gezeigt, notwendig und machbar sind. Die Level-1 PRK helfen, vorhandene Ineffizienzen in der Zusammenarbeit zwischen Wirtschaft und Verwaltung zu beseitigen und einen schnelleren und reibungslosen Betrieb ermöglichen. Die Studie empfiehlt daher, möglichst schnell die fachlichen und technischen Voraussetzungen für die Umsetzung der genannten Handlungsempfehlungen zu schaffen und die Realisierung von Level-1 PRK voran zu treiben.

Management Summary

Designing interorganisational process chains contributes to the improvement of the cooperation between companies and public administration. Due to the realisation of cross organisational process chains all participants are enabled to realize observable efficiency potentials.

Within the scope of the feasibility study "Development of cross organisational process chains between companies and public administration: Financial Services" the Fraunhofer Institute for Industrial Engineering IAO, Institute for Software and Systems Engineering ISST, Institute for Secure Information Technology SIT in cooperation with Commerzbank AG, GAD eG and the University of Tuebingen identified business potentials of cross organisational process chains between banks and public organisations based on a systematic analysis and evaluation. The focus of the analysis was a cross sectoral integration of business processes (level-1) where process chains runs along several value-added areas of banks and organization of the public administration which are linked by reporting required information and procedures between these organizations.

At the beginning 154 process chains were scrutinised by an analysis model and specified by a pre-defined matrix. Based on these findings a multi-level procedure model was developed for identifying, structuring and optimizing process chains. The model supports the evaluation of intersectoral (so called Level-1) process chains in banking and finance in regard to feasibility and potentials. The procedure model contains a screening a scoping of PRK and, based on a blueprint, pinpoints an approach to cross-organisational process chains.

Screening is a science-based but pragmatic approach to analyse process chains regarding to their most important characteristics. In doing so, different views of the process chains are being considered (functional, IT architecture-related, IT safety-related and legal). The developed approach can be adjusted to varying levels of analysis depending on the application purpose.

Scoping applies to an approach of identifying and characterising appropriate objectives for process chains. Its application incorporates varying target dimensions (organisational, IT architecture-related, IT safety-related and legal)

The actual state analysis illustrates that on one hand the process chains covers numerous organisational areas in banks and on the other hand there are a high number of public government organisations involved in the identified process chains. Further the analysis shows that most of the process interfaces between private and public organisations are operated manually and paper based. In many cases, information between banks and public government is transmitted on a traditional and paper based way because of missing adequate IT-infrastructure and necessary governmental regulations. In some cases the German Central Bank (Deutsche Bundesbank) and Federal Financial Supervisory Authority (BaFin) offers high performance portal solutions which are enablers for the realisation of an integrated and media discontinuity free processes.

The feasibility study also shows that there is a concentration of process chains between private banks and the Bundesbank (44,2%) and BaFin (40,8%) as representatives of the public sector. Both institutions offer an extranet and portal service for required messages and data flows. These are based on standardised data interfaces (XML schemes) which are suitable sources for the further development of necessary IT-Infrastructures and also for the design and realisation of level-1 process chains.

For the evaluation of the research model the consortium prepared two case studies (for "real estate credit" and "suspicious money laundering complaint" process chain). The previously developed methods and research models are used in the cases studies.

The first case study focuses on the design of an integrated process chain for a private real estate process. This process chain was selected based on the high number of different involved participants from the public organisations (German federal Gazette, Local Court, Registry of deeds, fiscal authorities, KfW Bankengruppe etc.). Due to the use of the developed research methodologies and based on cost-benefit and performance analysis a target real estate process chain where developed. The results showed that there is a high potential for cross organisational process optimisation in case of costs, time and quality.

A further result of the analysis highlights the importance and need for optimization of process interfaces between banks and public government organisations in case of confirmation about income tax certificates (fiscal authorities/ ELSTER, IT-procedure ELENA) and to the Registry of deeds (see also "Initiative Finanzstandort Deutschland"). Additionally to this the implementation of this process chain is correlated with the construction of a suitable IT security infrastructure, which can also be used in other process chains (i.e. Implementation and usage of advanced and qualified electronic signature, Im-

plementation of security infrastructures based on trusted domains with flexible distributed security identity management). To realize the cross organisational process chain for private real estate credit the introduction and usage of the planned electronic identification card is necessary. This ID card enables the provision of a electronic signature.

The second case study in the feasibility study highlights an integrated, cross organisational process chain for the "suspicious money laundering complaint process". This case study is based on a project for the "electronic suspicious money laundering complaint", in which a proofed concept was developed for a equal process. In this project a concept for a portal solution was developed, which is actually in the implementation phase. This portal solution enables banks to provide the suspicious money laundering complaint" to the Federal Criminal Police Office (Bundeskriminalamt) on a completely electronically integrated and secured channel. The highest priorities addressed during the development and operation phase is focussed on extremely high security functions and the possibility to provide information about the actual status of the information flow in the process chain.

The consolidated findings from the case studies are summarized in several recommendations which are focussed on banks and public administrations perspectives. Among other things the recommendations refers to an increased professionalization of business process management in banks as well in government organisations and the implementation of adequate infrastructures, which enables the realization of the described cross organisational and media discontinuity free process chains.

Furthermore it is possible to use findings from other Germany-Online projects, which supports the accelerated implementation of infrastructure components, to provide basic services for a nationwide IT-Infrastructure. The infrastructure can also be used for other process chains. Similar to the existing standards from the Germany Online Project regards to the definition of data interfaces along the process chain can be used in this context (XOEV-Standards). According to the prototypes of several services (i.e. usage of the electronic ID card and IT-services like ELSTER and ELENA can be used als service blueprints for further processes and procedures in the to realize Level-1 process chains between companies and government organisations.

Beside the identified IT related recommendations the feasibility study contains approaches and ideas for operation and business models in the context of cross organisational process chain management.

To achieve the goal of implementation of Level-1 process chains the visualization of process chains as process landscapes is an important factor. This

process landscape enables and supports the access of knowledge about the process and the context between several processes. These information can be used by executives, users, customers and other target groups of the process chain.

In summary the feasibility study highlights that there is a great demand for cross organisational process chains between financial service companies and government organisations and that these process chains are feasible for realization. The level-1 process chains supports the avoidance of existing inefficiencies in the cross sectoral cooperation and enables the realization of integrated and efficient operation. Therefore the study recommends the implementation and realization of the organisational and technical requirements described above to provide the basis for the realization of cross sectoral level-1 process chains.

1 Einleitung – Zielsetzung und Fragestellung

Sowohl die rasante Entwicklungen im Finanzdienstleistungsmarkt, als auch die Entwicklungen in der öffentlichen Verwaltung zeugen von einer anhaltenden und nachhaltigen Veränderung in der Wirtschaft. In den kommenden Jahren ist davon auszugehen, dass die Bereiche der öffentlichen Verwaltung und des Finanzdienstleistungsbereiches noch stärker zusammenwachsen, als sie dieses in den vergangenen Jahren getan haben.

Durch die Umsetzung zahlreicher Maßnahmen zum E-Government auf Bundes-, Landes- und kommunaler Ebene werden von Seiten der öffentlichen Verwaltungen die Voraussetzungen geschaffen, um die Integration mit verschiedenen Wirtschaftszweigen voranzutreiben.

Andererseits sind auf Seite der Banken vielfältige Aktivitäten gestartet worden, um die Optimierung von Wertschöpfungsprozessen nicht mehr nur innerhalb der eigenen Organisation voranzutreiben, sondern diese auch auf ihre Kooperationspartner auszudehnen.

Eine große Herausforderung für die beiden genannten Wirtschaftsbereiche stellt nun die Konzeption, Gestaltung und Umsetzung von Prozessketten dar, welche zwischen Banken und der öffentlichen Verwaltung existieren. Diese Machbarkeitsstudie adressiert diesen Themenkomplex und zeigt Potenziale und Möglichkeiten auf, die sich im Kontext des Prozesskettenmanagements sowohl für Banken als auch für die öffentliche Verwaltung ergibt. Neben einem Vorgehensmodell zur Konzeption und Umsetzungsplanung von Prozessketten, werden Hinweise bezüglich Wirtschaftlichkeitspotenzialen und Ansatzpunkten für neue Geschäfts- und Betreibermodelle zwischen Banken und öffentlichen Verwaltungen skizziert.

Diese Machbarkeitsstudie ist im Zuge des Projekts "Entwicklung von Prozessketten zwischen Wirtschaft und Verwaltung - Los 2: Finanzdienstleistungen" im Zeitraum von Juni 2008 bis Januar 2009 im Auftrag des Bundesministeriums des Innern (BMI) entstanden.

Im Zuge dessen adressiert das Projekt folgende zwei Zielsetzungen:

1. Die Entwicklung einer wissenschaftlichen und praktisch orientierten Prozesskette zwischen Banken und öffentlichen Verwaltungen (Level-1)
2. Die Entwicklung eines generischen Bauplans zur Gestaltung von Prozessketten zwischen Banken und öffentlichen Verwaltungen (Level-1)

Dabei signalisiert "Level-1" als SOLL die branchenweite bzw. branchenübergreifende Prozessintegration.²

Die Machbarkeitsstudie schlägt den folgenden Weg ein (siehe Abbildung 1):

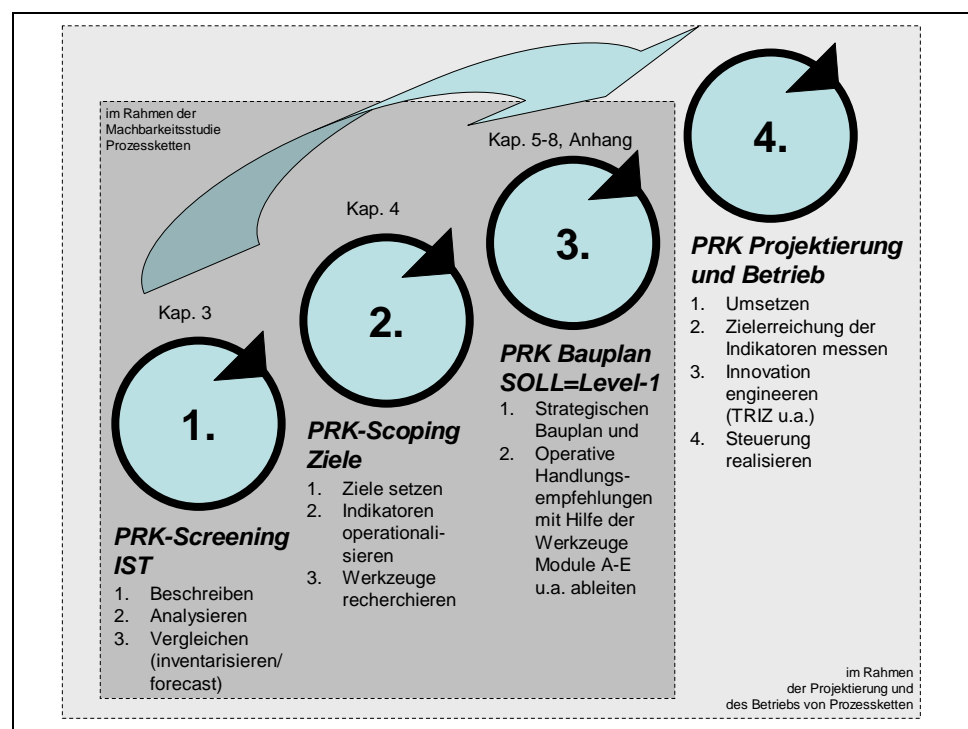


Abbildung 1: Gesamtverfahrensmodell in Wirkkreisen (Quelle: Eigene Darstellung)

² siehe dazu ausführlich Kap. 4.1

In einem ersten Schritt wird eine Methode entwickelt und angewandt, um die FDL-Prozesskette in ihrem IST-Zustand, mit ihren Akteuren, Schnittstellen etc. zu untersuchen und systematisch zu beschreiben ("PRK-Screening"). In einem zweiten Schritt wird eine Vorgehensweise entwickelt, um systematisch Ziele, Indikatoren und Werkzeuge für die Gestaltung einer "Prozessketten Level-1" zu gewinnen ("PRK-Scoping") – wirtschaftlich / prozessual / organisatorisch, IT-architektonisch, sicherheitstechnisch und juristisch. Auf deren Basis können dann in tragfähiger Art und Weise ein strategischer Bauplan und operative Handlungsempfehlungen abgeleitet werden, was die Studie für die Fallbeispiel-Prozessketten "Private Immobilienfinanzierung" und "Geldwäscheverdachts-Anzeige" durchführt (PRK-Bauplan).

Die Studie gibt der Zielgruppe des Dokuments Antworten auf folgende Fragestellungen:

1. Was sind Prozessketten und in welchem Verhältnis stehen sie zu aktuellen Marktentwicklungen und Forschungsständen im Bereich FDL – aus Banken- und aus E-Government Perspektive (Kap. 2)?
2. Wie kann die FDL-Prozesskette in der IST-Situation beschrieben und analysiert werden und wie sieht die Prozesskette in Deutschland aus (Kap. 3)?
3. Was sind mögliche Ziele und Anforderungen für Prozessketten Level-1 (Kap. 4)?
4. Wie lassen sich im Hinblick auf Ziele und Anforderungen mit der Hilfe von unterschiedlichen Werkzeugen strategische Baupläne und operative Handlungsempfehlungen für Prozessketten Level-1 generieren (Kap. 5)?
5. Welche Baupläne und Handlungsempfehlungen können durch den Methodeneinsatz der Studie für die Fallbeispiel-Prozessketten "Private Immobilienfinanzierung" und "Geldwäscheverdachts-Anzeige" gewonnen werden (Kap. 6-8)?

2 Prozessketten zwischen Wirtschaft und Verwaltung im Bereich FDL

2.1 Arbeitsdefinition: Vom Prozessmanagement zum Prozesskettenmanagement

Im Rahmen dieses Abschnittes wird ein kurzer Überblick zum Thema Geschäftsprozessmanagement und der Gestaltung von Prozessketten gegeben. Die Zielsetzung besteht in der Schaffung einer gemeinsamen Sichtweise auf das Themenfeld des Managements von Prozessketten zwischen Finanzdienstleistern und Einrichtungen der öffentlichen Verwaltung.

Das Konzept des Geschäftsprozessmanagements sowie der Prozessketten sind grundsätzlich keine neuen Themen und Managementkonzepte in Wissenschaft und Praxis. Seit Beginn der 1980er Jahre wird die Gestaltung von Unternehmensorganisationen von einer funktionalen und verrichtungsorientierten Form hin zu einer prozessorientierten Gestaltung diskutiert und in vielen Branchen umgesetzt (siehe Gaitanides 1983, Davenport 1993, Picot / Reichwald / Wigand 2001: 231).

Vorrangiges Ziel der prozessorientierten Ansätze ist die Reduktion organisatorischer Schnittstellen im Wertschöpfungsprozess. Dabei sind Schnittstellenprobleme, wie beispielsweise Liegezeiten, Kommunikationsbarrieren und unzureichend abgestimmte Ziele an den Grenzen zwischen Fachabteilungen als eine der wichtigsten Gründe für Ineffizienzen in Organisationen erkannt worden (Picot / Reichwald / Wigand 2001: 231). Erfahrungen aus verschiedenen Branchen zeigen, dass diese Barrieren in den verschiedenen Wirtschaftszweigen unterschiedlich gut beseitigt worden sind.

Was sind Prozesse und Prozessketten? Nach Krcmar wird eine Folge von logischen Einzelfunktionen, zwischen denen Verbindungen bestehen, als **Prozess** bezeichnet. Krcmar definiert weiter: "Unter Prozessmanagement wird deshalb in diesem Zusammenhang die Gestaltung, Ausführung und Beurteilung von Funktionsfolgen, nämlich Prozessen, verstanden. Prozesse transformieren Inputfaktoren zu einem Outputfaktor. Deshalb kann allgemein von einem Transformationsprozess gesprochen werden, der entweder Materie bearbeitet (materielle Prozesse) und / oder Informationen verarbeitet (informativische Prozesse)." (Krcmar 2003: 99 f.).

Die nachfolgende Grafik zeigt nach Schwarzer (Schwarzer 1994: 12), wie Prozess-Inputs und ein Trigger (Startereignis) zum Zeitpunkt t_0 eine Funktion F_1 , F_2 usw. anstoßen, die nach erfolgreichem Durchlauf zu einem Output als Prozess-Ergebnis führen (siehe Abbildung 2).

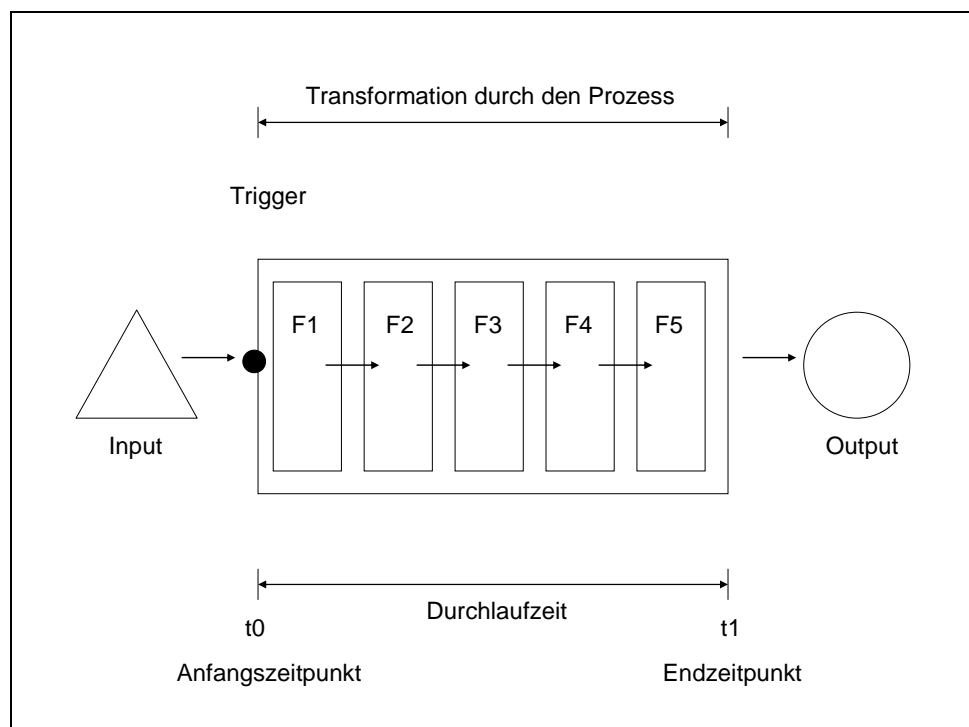


Abbildung 2: Schematische Darstellung eines Prozesses (Quelle: Krcmar 2003: 100)

Aufbauend auf der Definition von Krcmar können "**Prozessketten**" als eine logische Verknüpfung von Prozessen gesehen werden. Prozessketten stellen damit eine Kette zusammenhängender Prozesse dar, die zur Erstellung einer Dienstleistung oder eines Produktes dienen (Wertschöpfungsorientierung). Diese können sowohl innerhalb einer Organisation als auch zwischen verschiedenen, rechtlich selbstständigen Organisationen etabliert sein.

Das Bundesministerium des Innern definiert Prozessketten wie folgt: "Eine Prozesskette ist somit eine zielgerichtete Bündelung einzelner Transaktionsdienstleistungen entlang einer definierten Wertschöpfungskette. Entscheidend ist die Kenntnis der Zusammenhänge, damit diese Weiterentwicklung zielgerichtet betrieben werden kann. Eine Realisierung einzelner Transakti-

onsdienstleistungen ohne diesen "Bauplan" ist nicht zielführend" (BMI 2007: 4).

Der marktliche Wettbewerb fordert von allen Organisationen eine Fortführung von Effizienzsteigerungen und eine Erhöhung der Integration der gesamten Wertschöpfung. Aus diesem Grund wird die Identifikation, Konzeption und Umsetzung von organisationsübergreifenden Prozessketten zu einem zentralen Aspekt des zukünftigen Wettbewerbs sowohl auf nationaler Ebene als auch im internationalen Kontext.

Die Gestaltung und das Management von organisationsübergreifenden Prozessketten stellen das zentrale Gestaltungselement von zukünftigen, sektorübergreifenden und integrierten Organisationsformen dar. Sie ermöglichen und integrieren eine organisationsübergreifende sektorale Wertschöpfung und bilden die Basis neuer Geschäfts- und Betreibermodelle für Banken und Einrichtungen der öffentlichen Verwaltung.

Im Rahmen dieser Machbarkeitsstudie spielen Prozessketten als Handlungsfelder im Programm der Bundesregierung "E-Government 2.0" eine sehr wichtige Rolle. Dabei werden Konzepte der (betrieblichen) Prozesse und deren Management auf Prozessketten übertragen:

- Der Ansatz hebt auf die **relative Länge und höhere Komplexität** von durchgängigen Prozessen ab, wenn mehrere Akteure auf Wirtschaftsseite und mehrere Akteure auf staatlicher Seite zur Erreichung eines Zieles **über die organisatorischen Grenzen ihrer Institutionen** hinaus interagieren.
- In der vorliegenden Studie fokussieren Prozessketten und die Analyse derselben vor allem auf die **Schnittstellen zwischen den Akteuren auf Wirtschaftsseite und den staatlichen Akteuren**. Vor- und nachgelagerte Teilprozesse – beispielweise bei gesetzlichen Meldepflichtenprozessen in Banken und Finanzaufsichtsbehörde – werden nachvollzogen und in die Analyse in den Modellrahmen einbezogen oder externalisiert, wenn sie in ihrer wahrgenommenen Relevanz für das wissenschaftliche und praktische Erkenntnisziel ausgeklammert werden können.

Aufgrund der dargestellten Bedeutung von Prozessketten an der Schnittstelle zwischen Finanzdienstleister und Einrichtungen der öffentlichen Verwaltung, stellt sich nun die Frage, wie gut diese beiden Bereiche auf die Herausforderungen zur Umsetzung von organisationsübergreifenden Prozessketten vorbereitet sind. Vor dieser Fragestellung werden in den folgenden Abschnitten dieser Machbarkeitsstudie aktuelle Marktentwicklungen und For-

schungsstände aus dem Bankenmarkt und aus eGovernment Perspektive skizziert.

2.2 Die Banken-Perspektive

Die aktuelle Finanzmarktkrise und die von Politik und Wirtschaft getroffenen Maßnahmen zeigen, dass der Finanzdienstleistungsmarkt einerseits eine sehr große Wirkung auf die Realwirtschaft besitzt und andererseits veränderte ordnungspolitische Rahmenbedingungen entworfen werden, um diesen sehr dynamischen und komplexen Markt gestaltbarer zu machen. Diese Entwicklungen zeigen jedoch auch die Stärke in der Struktur des deutschen Bankenmarktes auf. Vor allem die regionalen Institute sind aufgrund ihrer Geschäftstätigkeit weit weniger von den negativen Entwicklungen betroffen, als international agierende Großbanken.

Ungeachtet der Entwicklungen auf den internationalen Finanzmärkten, müssen und werden sich jedoch zukünftig alle Banken in ihrer Organisationsstruktur auf neue Herausforderungen einstellen. Dabei wird als oberstes Ziel die bedarfsgerechte Befriedigung von Kundenbedürfnissen, sowohl von Privat- als auch von Geschäftskunden, sein. Um dieses erreichen zu können, müssen Banken ihre gesamte Wertschöpfungsprozesse kritisch analysieren und an die neuen Anforderungen anpassen. Hierbei gibt es im deutschen und europäischen Bankenmarkt sehr unterschiedliche Entwicklungsstände, wie die Ergebnisse der Marktstudie "Bank & Zukunft 2008" zeigen (Spath / Engstler / Praeg / Vocke 2008).

Dabei ist im Rahmen dieser Machbarkeitsstudie vor allem die Entwicklung und der Stand im Bereich der Gestaltung und Umsetzung von Prozessketten, bzw. des internen Geschäftsprozessmanagements bei Banken von Bedeutung. Diese Entwicklungen werden im Rahmen der Marktstudie "Bank & Zukunft 2008" unter dem Oberbegriff der "Bankenindustrialisierung" adressiert und beschrieben.

Bankenindustrialisierung

Unter dem Begriff "Bankenindustrialisierung" wurden in den vergangenen Jahren eine große Anzahl von Ideen und Konzepten entwickelt, wie Banken ihre Wertschöpfungsprozesse verbessern können. Das Innovationsforum "Bank & Zukunft" hat unter der Leitung des Fraunhofer IAO, folgende Definition geprägt (Engstler / Makram / Vocke 2004: 9 f.):

"Demnach kann unter Industrialisierung die Optimierung der gesamten Wertschöpfungskette verstanden werden. Mit einer Optimierung geht auch die Möglichkeit des Aufbrechens und der Neuformulierung der Wertschöpfungskette einher, was die Fokussierung auf Kernkompetenzen fördert. Ob im Rahmen der Optimierung und des Aufbrechens der Wertschöpfungskette und der Konzentration auf Kernkompetenzen eine veränderte interne Arbeitsteilung oder eine veränderte externe Arbeitsteilung in Form von vertikalen oder horizontalen Wertschöpfungs Kooperationen erfolgen, ist bankindividuell zu prüfen. [...]"

Industrialisierung ist optimierte Wertschöpfung durch Gestaltung

- der gesamten Wertschöpfungskette und Hinterfragen der Arbeitsteilung (kooperativer Ansatz, Insourcing / Outsourcing ist dabei eine "Option"),
- der Serien- / Massenprozesse (Skaleneffekte, Lernkurveneffekte, Komplexitätseffekte / -management),
- der Arbeitsorganisation (Aufgaben-Kompetenz-Verantwortung im Einklang),
- der Systemunterstützung (IT-Einsatz, Standards, Schnittstellen),
- der Personalwirtschaft (Qualifikation und Entlohnung (Modelle, Eingruppierung, Lohnniveau), flexible Arbeitszeit, verschiedene Personalkonzepte für die Mitarbeitergruppen je nach Qualifikations- und Anforderungsprofil) sowie
- des Produktes (Kundenorientierung) und des Preises (Verursachungsprinzip, risikoorientierte Preiskalkulation, erklärbare Regeln).

Diese Definition zeigt, wie vielfältig die Facetten der Bankenindustrialisierung sind. Im Vordergrund stehen dabei die Optimierung der internen Wertschöpfungsprozesse. Eine wesentliche Grundlage dafür besteht in der Einführung und dem Betrieb eines professionellen Geschäftsprozessmanagement in Banken, welches weder an Bereichsgrenzen noch an den Grenzen der Bank als Organisation halt machen darf. Dies verdeutlicht die große Bedeutung der Gestaltung von organisations- und branchenübergreifenden Prozessketten.

Ziele und Erwartungen im Bereich der Bankenindustrialisierung

Bezogen auf die Ziele und Erwartungen der Bankenindustrialisierung ist nach wie vor der Aspekt der Effizienzsteigerung das dominierende Ziel der Banken (siehe Abbildung 3). Bei fast 90 Prozent der Studienteilnehmerinnen und Studienteilnehmern ist die Steigerung der Effizienz das wichtigste Ziel (Spath et al. 2007). Dabei unterscheiden sich die Einschätzungen zwischen den jeweiligen Bankengruppen nur geringfügig. Vor allem bei den Universalbanken und Spezialinstituten ist zu vermuten, dass aufgrund der tendenziell größeren Erfahrung mit Maßnahmen zur Industrialisierung die Erwartungen in diesem Bereich, aufgrund der erzielten Erfolge, nicht mehr so hoch gewertet werden, wie dies bei den anderen Teilnehmerinnen und Teilnehmern der Fall ist (Spath et al. 2008).

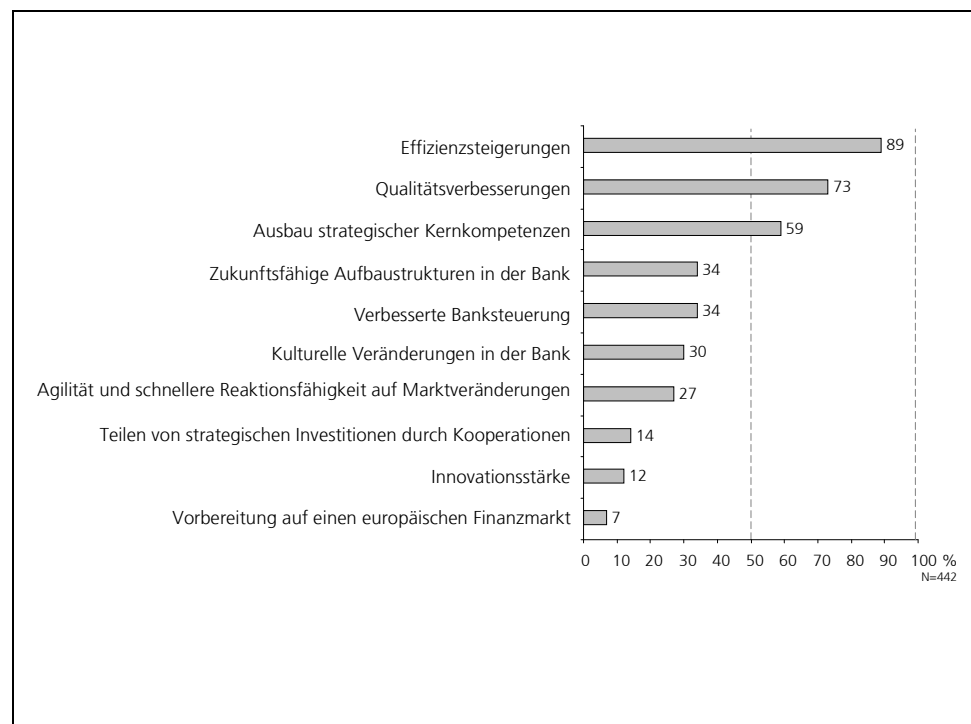


Abbildung 3: Ziele und Erwartungen von Banken hinsichtlich Industrialisierung (Quelle: Spath / Engstler / Praeg / Vocke 2008)

Der Aspekt der "Qualitätsverbesserung" wird von den Studienteilnehmerinnen und Studienteilnehmern ebenfalls hoch bewertet. Hier sehen 73 Prozent der befragten Banken ein bedeutendes Ziel und erwarten durch den Einsatz von Industrialisierungsmaßnahmen eine wahrnehmbare Steigerung der Qualität. Der Oberbegriff "Qualität" umfasst sowohl die Sicherstellung einer zu-

gesicherten Eigenschaft auf Produktseite, als auch die Gewährleistung von hochwertigen Dienstleistungen und die Verlässlichkeit der bankinternen Prozesse und Leistungen. Für den Bereich gibt es Qualitätsverbesserungen deutliche Unterschiede in der Einschätzung der Bedeutung zwischen den einzelnen Bankengruppen. Im Gegensatz zu den Genossenschaftsbanken und den Geschäftsbanken, ist der Aspekt der Qualitätsverbesserung bei den Sparkassen mit einer erheblich geringeren Erwartung verbunden. Dies könnte ein Indiz dafür sein, dass Sparkassen in der Entwicklung und dem Reifegrad der Industrialisierung tendenziell noch nicht so weit fortgeschritten sind wie die anderen Bankengruppen und sich daher noch eher mit der Prozessgestaltung aufgrund der Veränderungen am Markt befassen, bevor sie sich Aspekten des Qualitätsmanagements zuwenden (Spath et al. 2008).

Bereiche für Industrialisierungspotenziale in Banken

Aufbauend auf den zuvor illustrierten Zielen und Erwartungen, ist die Identifikation und Analyse von Industrialisierungspotenzialen, die aus Sicht der Studienteilnehmerinnen und Studienteilnehmern in den Banken vorhanden sind, erfolgt. Von den Banken wurde dazu eine Einschätzung bezüglich hoher, mittlerer und geringer Industrialisierungspotenziale vorgenommen (siehe Abbildung 4).

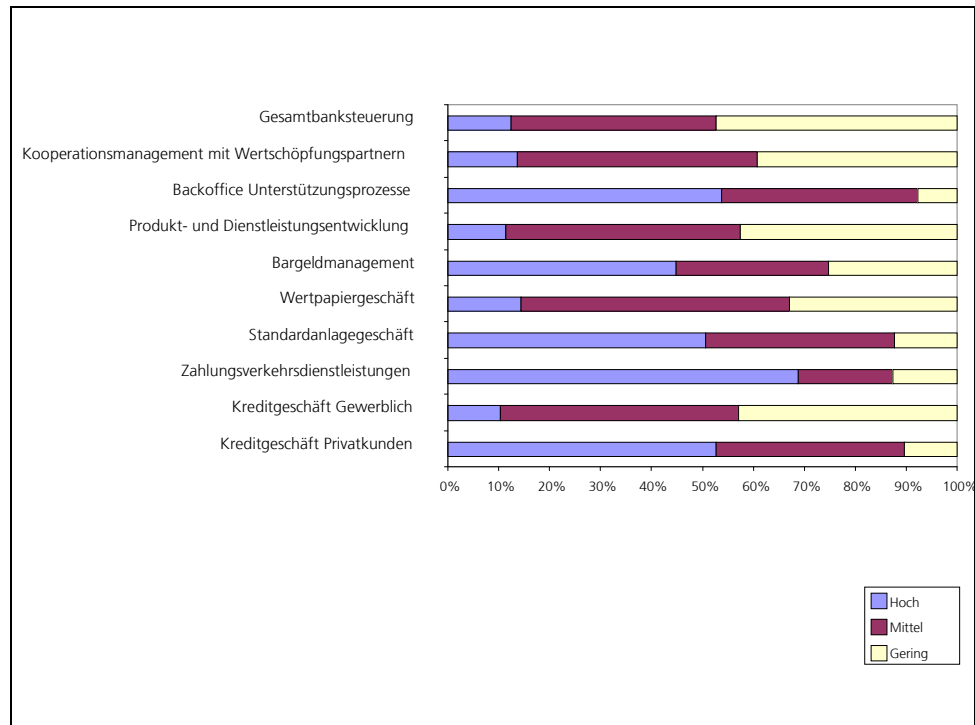


Abbildung 4: Industrialisierungspotenziale aus Sicht von Banken (Quelle: Spath / Engstler / Praeg / Vocke 2008)

Die Ergebnisse zeigen, dass 70 Prozent der Banken den Zahlungsverkehrsdienstleistungen ein hohes Industrialisierungspotenzial beimessen. Für 54 Prozent der Teilnehmer sind in den Backoffice Prozessen der Banken nennenswerte Potenziale vorhanden. Berücksichtigt man zusätzlich die als "mittel" eingestuften Potenziale, so werden derzeit in diesem Bereich die größten Potenziale gesehen.

53 Prozent der Banken sehen im Kreditgeschäft für Privatkundinnen und Privatkunden noch wahrnehmbare Industrialisierungspotenziale. Dagegen wird das gewerbliche Kreditgeschäft als ein Bereich mit tendenziell geringerem Potenzial angesehen. Einerseits kann dies an der spezifischen Situation des gewerblichen Kreditgeschäfts erklärt werden, andererseits besteht ebenso die Möglichkeit, dass Banken in diesem Bereich schon Anstrengungen unternommen haben und daher die Potenziale als gering einstufen.

Das Standardanlagengeschäft ist für ungefähr die Hälfte (51 Prozent) der Banken ein Bereich mit hohen Industrialisierungspotenzialen. Ergänzend dazu bewerten 37 Prozent der Banken das Industrialisierungspotenzial als "mittel". Das Bargeldmanagement wird von 45 Prozent der Studienteilnehmer

merinnen und Studienteilnehmern mit einem hohen Industrialisierungspotenzial und von 30 Prozent mit einem mittleren Potenzial in Verbindung gebracht. (Spath et al. 2008).

Erschließung der Industrialisierungspotenziale

Die Identifizierung von Industrialisierungspotenzialen zeigte, dass es in Banken zahlreiche Bereiche gibt, in denen aufgrund von Maßnahmen zur Industrialisierung wahrnehmbare Effizienzsteigerungen möglich sind. Ein weiterer interessanter Aspekt in diesem Kontext ist die Antwort auf die Frage, mittels welcher Methoden und Instrumente Banken die identifizierten Potenziale erschließen möchten (siehe Abbildung 5).

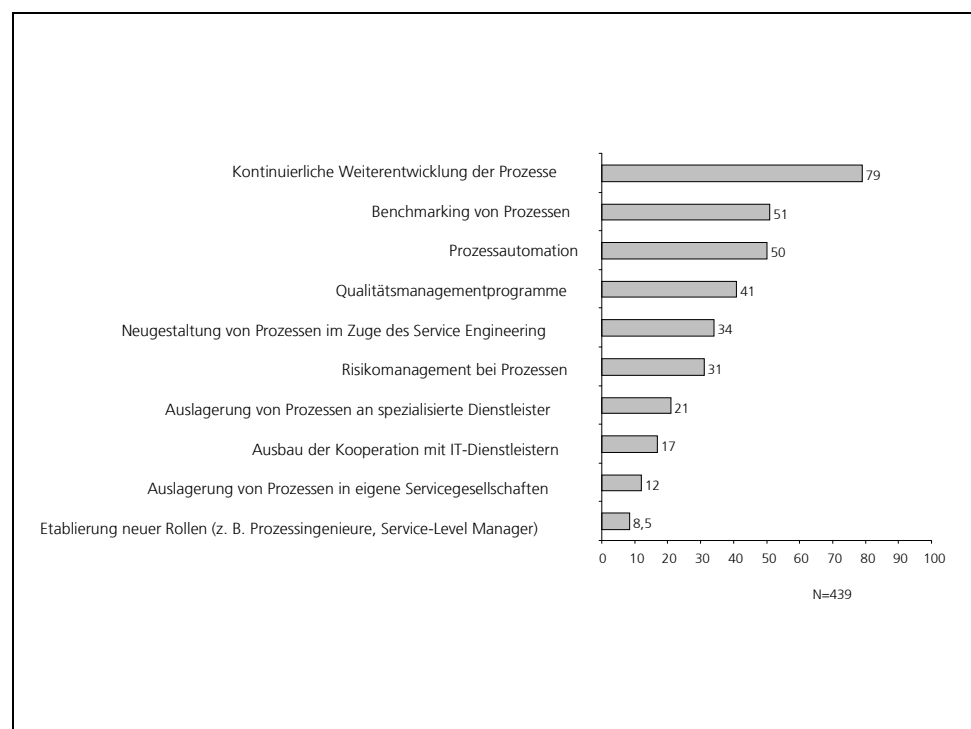


Abbildung 5: Maßnahmen zur Erschließung der Industrialisierungspotenziale bei Banken (Quelle: Spath / Engstler / Praeg / Vocke 2008)

Vor allem die kontinuierliche Weiterentwicklung der Prozesse und des Prozessmanagements steht im Fokus der Aktivitäten. 79 Prozent der Teilnehmerinnen und Teilnehmer sehen darin eine wichtige Maßnahme zur Erschließung von Industrialisierungspotenzialen in Banken. Dabei zeigt die detaillierte Analyse, dass vor allem Genossenschaftsbanken diese Maßnahme überdurchschnittlich stark präferieren. Eine mögliche Erklärung dafür liegt in

der Vorstellung von Referenzprozessen für Genossenschaftsbanken im Rahmen des vom Bundesverband der Volks- und Raiffeisenbanken (BVR) beauftragten Projektes "VR-Process". Dort sind ausgewählte Referenzprozesse für das Bankmanagement dokumentiert und beschrieben. Darüber hinaus werden diese Referenzprozesse in den jeweiligen bankfachlichen Anwendungen der IT-Dienstleister unterstützt, was zusätzlich zu einer Stärkung der Akzeptanz und Nutzung dieser standardisierten Prozesse beitragen wird.

Für 51 Prozent der Teilnehmerinnen und Teilnehmer ist das Benchmarking von Prozessen eine wichtige Maßnahme im Rahmen der Bankenindustrialisierung. Eine detaillierte Analyse bezüglich der Art und des Umfangs des Benchmarkings wurde an dieser Stelle nicht durchgeführt. Allerdings setzt Benchmarking die Implementierung von gleichartigen Prozessen voraus, um sinnvolle und aussagekräftige Ergebnisse zu erhalten. Zwischen den jeweiligen Bankengruppen bestehen für das Benchmarking keine großen Abweichungen bezüglich der Einschätzung der Relevanz.

Die Prozessautomation ist für 50 Prozent der Banken derzeit eine geeignete Maßnahme, um die Industrialisierung umzusetzen. Vor allem in den Geschäftsbanken wird diese Maßnahme priorisiert. Dies ist aufgrund der tendenziell größeren Erfahrung und einer höheren Industrialisierungsreife der Organisationen eine durchaus sinnvolle Einschätzung. In diesen Instituten sind bereits Prozesse und ein Prozessmanagement implementiert, welche es erlauben sich auf die Automation von hoch standardisierten Prozessen zu konzentrieren.

Eine Neugestaltung von Prozessen im Zuge eines Service Engineerings sehen in der aktuellen Untersuchung 34 Prozent der Studienteilnehmerinnen und Studienteilnehmer als geeignete Maßnahme im Rahmen der Industrialisierung (Spath / Engstler / Praeg / Vocke 2008).

Mögliche Auswirkungen der Industrialisierung auf Banken

Wie die vorangegangenen Ausführungen gezeigt haben, ergeben sich aufgrund von Industrialisierungsmaßnahmen vielfältige Auswirkungen auf die Strukturen und Geschäftsmodelle von Banken.

Eine bedeutende Entwicklung ist die weiter zunehmende Prozessorientierung bei Banken. Die bisherigen Fachbereiche und funktional orientierte Strukturen werden sich zukünftig zugunsten einer prozessorientierten Organisationsform verändern. Aufgrund dieser Prozessorientierung werden Banken in die Lage versetzt werden, Teile ihrer Wertschöpfungsaktivitäten auf

Partner auszulagern. Die zunehmende Auflösung der Wertschöpfungskette innerhalb der Bank wird die Folge sein.

Basierend auf dieser Entwicklung führt eine zunehmende Industrialisierung auch zu einer verstärkten Modularisierung von vorhandenen Geschäftsprozessen bzw. Prozessketten innerhalb der Banken. Durch eine konsequente Modularisierung von Prozessketten, wird beispielsweise deren Wiederverwendung und Standardisierung ermöglicht (Praeg 2007). Damit stellt das Prinzip der Modularisierung einen vielversprechenden Ansatz zur Gestaltung von variantenreichen Dienstleistungen unter Einbeziehung mehrerer Wertschöpfungspartner dar. Vor dem Hintergrund der Gestaltung von Prozessketten zwischen Banken und öffentlicher Verwaltung ist dieses Prinzip demnach von großer Bedeutung (Praeg 2008a: 179). Es muss geprüft werden, welche Teile der Wertschöpfungskette von Banken selbst erbracht werden und in welchen Bereichen der Wertschöpfung externe Partner integriert werden.

Des Weiteren wurden im Rahmen des Innovationsforums "Bank & Zukunft" Szenarien zur Gestaltung von zukünftigen Strukturmodellen industrialisierter Banken entwickelt (Praeg 2008b). Mit Hilfe von Expertinnen- und Experteninterviews wurden verschiedene Entwicklungsszenarien bezüglich zukünftiger Strukturen von Banken aufgrund von Industrialisierungsmaßnahmen entwickelt. Als Ergebnis dieser Studien zeigte sich, dass sich in der Mehrzahl der erarbeiteten Modelle die klassischen Organisationsgrenzen auflösen, zugunsten von mehr oder weniger festen bzw. losen Wertschöpfungsverbänden. Diese Resultate untermauern heute und zukünftig die große Bedeutung der Kompetenzen zum Management von organisationsübergreifenden Prozessketten.

Als Folgen hiervon ergeben sich sowohl für Banken als auch für deren Wertschöpfungspartner tiefgreifende und umfassende Veränderungen in der Aufbau- und Ablauforganisation.

Die anstehenden Herausforderungen beziehen sich beispielsweise auf die Konzeption und Umsetzung der Prozessketten. Parallel dazu müssen entsprechend neue Rollenprofile und Aufgaben in den Organisationen geschaffen werden, wie beispielsweise die Rolle eines "Prozessverantwortlichen", welcher für den reibungslosen Betrieb einer solchen Prozesskette verantwortlich ist. Dies erfordert die Gestaltung von organisationsübergreifenden Kompetenzen und Verantwortlichkeiten für die entsprechenden etablierten Rollen. Im Endeffekt wird dadurch auch die Gestaltung und Umsetzung ganz neuer Managementkonzepte sowohl auf Bankenseite als auch bei der öffentlichen Verwaltung notwendig.

Zusammenfassend kann festgehalten werden, dass das Management von organisationsübergreifenden Prozessketten ein zentrales Erfolgskriterium bei der Definition von zukunftsorientierten Bankenstrukturen darstellen wird. Die Gestaltung von organisationsübergreifenden Prozessketten ist eine der zentralen Herausforderungen für die Banken in den kommenden Jahren. Welche wirtschaftlichen und politischen Potenziale und Möglichkeiten dabei bestehen, wird im Rahmen dieser Machbarkeitsstudie aufgezeigt.

2.3 Die E-Government-Perspektive

E-Government 2.0 - Strategische Ziele

Ein strategisches Ziel in einem rohstoffarmen Land wie Deutschland ist die Steigerung des Anteils der Investitionen in Forschung und Entwicklung am Bruttoinlandsprodukt bis 2010 um drei Prozent. Mit sechs Milliarden Euro will die Bundesregierung die Forschung und Entwicklung in den zukunftsträchtigsten Bereichen stärken. Dazu wurden insgesamt 17 Zukunftsfelder identifiziert, die von herausragendem nationalen Interesse sind und wirtschaftliches und wissenschaftliches Potenzial besitzen. Hierzu zählen die Informations- und Kommunikationstechnologien und damit auch das E-Government. Auf der intensiveren Nutzung von IT und Internet beruhen etwa 35 Prozent aller Produktivitätszuwächse der Wirtschaft in Deutschland.

Ebenso steht IT-Governance und deren staatliche Bedeutung mehr und mehr auf der politischen Agenda. "Alle für Deutschland traditionell wichtigen Infrastrukturen haben ihren Platz im Grundgesetz in den Artikeln 83 ff. Ihre Bedeutung, die Verantwortungsbereiche und die sie betreffenden Verfahren sind klar geregelt. Solche eindeutigen Regelungen benötigen wir auch für die IT-Infrastruktur der öffentlichen Verwaltung", so Bundesinnenminister Dr. Wolfgang Schäuble am 17. Juli 2007 auf der Konferenz "Zukunft gestalten – E-Government-Forschung für Deutschland" in Berlin (www.bmi.bund.de/cln_028/nn_122688/sid_C2BEF6417C3D710F37AC23C0956F4D20/nsc_true/Internet/Content/Nachrichten/Reden/2007/07/BM_E_Government_Forschung.html).

Ein weiteres strategisches Ziel in Deutschland ist es, einen TOP3-Rang in internationalen E-Government Vergleichsuntersuchungen zu erreichen.

E-Government 2.0 - Ziele auf Anwender Ebene

Die strategischen Ziele heißen für die Anwenderinnen und Anwender in Politik, Verwaltung, Wirtschaft, Forschung und Gesellschaft ganz konkret: E-Government "Made-in-Germany" muss **sicher, wertschöpfend und benutzungsfreundlich** sein.

E-Government 2.0 - Ziele auf Handlungsebene

Im Handlungsfeld "Prozessketten" selbst sollen folgende operative Ziele erreicht werden (Umsetzungsplan 2007 E-Government 2.0: 30 f.):

- Die Bearbeitung der Verwaltungsverfahren soll deutlich und messbar beschleunigt werden (15–30 Prozent).
- In den bis 2009 realisierten Prozessketten sind die Bearbeitungszeiten oder die Kosten für die Wirtschaft nachweislich um 15 Prozent reduziert. Gleichzeitig sind entsprechende Einsparungen auf Seiten der Verwaltung möglich.
- Im Jahr 2010 werden in den Prozessketten 80 Prozent der Verwaltungsvorgänge vollkommen medienbruchfrei und elektronisch abgewickelt.
- Die Prozessketten sind bis Ende 2010 nach ISO 27001 (IT-Grundschutz) zertifiziert.
- Ab 2012 sollen Transaktionen zwischen Wirtschaft und Verwaltung grundsätzlich nur noch elektronisch abgewickelt werden und damit eine entsprechende Ankündigung gegenüber der Wirtschaft auf dem ersten nationalen IT-Gipfel erfüllt werden.

IT-Herausforderungen: Dienste statt Software – von Diensten zu Prozessketten

Mit der Umsetzung der EU-Dienstleistungsrichtlinie steht die deutsche Verwaltung vor einer ihrer größten Herausforderungen. Durch die EU-Dienstleistungsrichtlinie müssen bzw. sollen nach dem Willen der Bundesregierung die bisherigen Bemühungen zum Aufbau von E-Government Strukturen einen deutlichen Ausbau erfahren. Auch die Verwaltungsmodernisierung, die damit verbundene Konsolidierung der öffentlichen Haushalte und der demografische Wandel erfordern immer mehr die fach- und ebenenübergreifende Zusammenarbeit von Verwaltungen bis hin zu kommunalen- und länderübergreifenden Kooperationen. Voraussetzung für solche organi-

sationsübergreifenden und durchgängig unterstützten IT-Prozessketten ist der Aufbau einer umfassenden IT-Infrastruktur, die eine kooperative und kollaborative Zusammenarbeit zwischen Kommunen, Ländern und Bund, aber auch zwischen Wirtschaft und Verwaltung ermöglicht. Aus isolierten "Anwendungsinseln" müssen vernetzte, föderierte Infrastrukturen³ entstehen.

Die Umsetzung von organisationsübergreifenden Prozessketten stellt nicht nur eine organisatorische, sondern auch eine technische Herausforderung dar. Obwohl die Technik nur Mittel zum Zweck ist, stellt sich die Frage, ob die IT-Infrastrukturen, und hierzu zählen auch die Fachanwendungen, bereits darauf vorbereitet sind. Die meisten IT-Fachverfahren sind geschlossene monolithische Software-Systeme, die zwar die Prozesse eines einzelnen Verwaltungsvorgangs unterstützen, aber kaum mit anderen Systemen kommunizieren und Daten austauschen können. Auch verfügen viele über keine definierten und standardisierten Schnittstellen. Dieses gilt in der Regel auch für andere Komponenten der Infrastrukturen. So gibt es z. B. in Deutschland bisher keine einheitliche Kommunikationsinfrastruktur. Von Interoperabilität zwischen den Systemen kann daher noch nicht gesprochen werden. Neben organisatorischen und technischen Anforderungen muss eine solche Infrastruktur auch die semantische Interoperabilität sicherstellen.

Ein technischer Ansatz zur Lösung dieser Herausforderungen wird im Bereich der "Service-Orientierten-Architekturen" (SOA) gesehen. Bei SOA bieten verschiedene IT-Komponenten anderen Komponenten ihre Dienste an, so dass Anwendungen aus verschiedenen Komponenten und Diensten orchestriert werden können. Damit lassen sich nun auch Prozessketten (Geschäftsprozesse) realisieren, die über die Grenzen einzelner geschlossener Fachinseln und Behörden- und Unternehmensgrenzen hinweggehen. SOA dient daher als Integrationsplattform für die Realisierung kooperativer und kollaborativer IT-Infrastrukturen.

³ zu den Fraunhofer eGovernment Zentrum Empfehlungen im einzelnen siehe Brunzel, M. / Fröschle, N. / Kraft, R. / Nentwig, L. / Nordbrock, G. / Steffens, P. / Tschichholz, M. / Wehner, J. 2007: Aktuelle Trends im E-Government und Vorschläge zum Programm "E-Government 2.0", Studienkurzzusammenfassung Fraunhofer eGovernment Zentrum für BMI, 5 S.

Gleichzeitig ist die Einführung einer SOA aber auch zu neuen Herausforderungen verbunden. Ein wesentlicher Faktor dabei ist die Tatsache, dass Dienste nicht aus administrativen oder technologischen Gesichtspunkten vorgegeben, sondern aus der Analyse der Geschäftsprozesse unter Berücksichtigung der Sicherheits- und Fachanforderungen abgeleitet werden. Auch Fragen des zukünftigen Betreiber- und Geschäftsmodells stellen einen nicht zu vernachlässigenden Faktor dar. All diese Fragen müssen bei der Planung einer service-orientierten Infrastruktur berücksichtigt werden.

Eine Service-Orientierte Architektur lässt sich heute nur schrittweise einführen und ist eng verbunden mit der Migration bestehender IT-Infrastrukturen hin zu einer SOLL- (Ziel-)Architektur. Diese Zielarchitektur muss sich in eine IT-Gesamtarchitektur der Verwaltung (ähnlich einer Unternehmensarchitektur) eingliedern. Um diese Ziele zu erreichen, ist die Einführung eines SOA Projektmanagements und einer SOA Governance unbedingt notwendig.

Trotz der vielen heterogenen IT-Landschaften in der öffentlichen Verwaltung werden bereits in verschiedenen Vorhaben in Deutschland Voraussetzungen für den Aufbau einer einheitlichen Infrastruktur geschaffen. Beispiele aus dem Deutschland-Online Vorhaben des Bundes oder Beispiele aus den Ländern und Kommunen zeigen, dass vereinzelt Bausteine für ein organisationsübergreifendes E-Government geschaffen werden. Zu nennen sind hier insbesondere die Projekte "Deutschland Online Infrastruktur" und "Deutschland Online Standardisierung" (siehe www.deutschland-online.de). Die bisherigen Maßnahmen greifen noch nicht weit genug. Es ist notwendig, die vielen einzelnen E-Government Inseln zu föderierten Systemen zusammenzuführen. Dies bedarf aber der Zusammenarbeit aller Verantwortungsbereiche von der Fachlichkeit über die Technik bis zum Betrieb. Prozessorientiertes E-Government lässt sich nur realisieren, wenn von Anfang an Fachverantwortliche das Thema unter Einbeziehung der technischen und betrieblichen Anforderungen und Rahmenbedingungen vorantreiben.

Ein Erfolgskriterium für die Umsetzung dieser föderierten und interoperablen IT-Infrastrukturen und -Anwendungen ist die Nutzung von Standards. Ein wesentlicher Bereich der Standardisierung ist die Vorgabe einheitlicher IT-Standards und Software-Architekturen des BMI, die ausführlich im SAGA-Dokument beschrieben werden (www.cio.bund.de/cln_102/sid_9130FA044B6A5C2FA9750E368A73D56E/D/E/Standards/SAGA/saga_node.html). Auch die Standards der XÖV-Strategie des Bundes (www.standardisierung.deutschland-online.de) müssen bei der Entwicklung von organisationsübergreifenden Prozessketten berücksichtigt werden.

E-Government und Sicherheit

Für die Sicherheit der E-Government Anwendungen ist es erforderlich, dass

- die Daten bei ihrer Übertragung vor unerwünschtem Mitlesen und Fälschungen geschützt werden,
- bei Bedarf nachvollzogen werden kann, wann eine Übertragung stattgefunden hat sowie wer in welcher Weise daran beteiligt war und
- das organisatorische Umfeld, in dem die Daten verarbeitet und gespeichert werden, hinreichend sicher ist.

Zur Erfüllung dieser Anforderungen tragen Sicherheitsstandards wie etwa die Normenfamilie ISO / IEC 27001 ff. oder der dazu kompatible und als Rahmenwerk für die Informationssicherheit in Bundesbehörden verbindliche BSI-Standard 100-2 (IT-Grundschutz-Vorgehensweise) bei.

Der BSI-Standard 100-2 enthält

- Empfehlungen für den Aufbau, den Betrieb und die Weiterentwicklung eines Managementsystems für Informationssicherheit
- eine systematische Vorgehensweise zur Entwicklung, Umsetzung und Verbesserung von Sicherheitskonzepten mit Hilfe der IT-Grundschutz-Kataloge und ggf. erforderlichen zusätzlichen Sicherheitsuntersuchungen.

Der BSI-Standard 100-2 wird ergänzt durch die IT-Grundschutz-Kataloge, die konkrete Hinweise zu möglichen Gefährdungen und erforderlichen Sicherheitsmaßnahmen geben. Die Klammer zwischen den dort aufgeführten Gefährdungen und Maßnahmen bilden die in die fünf Schichten "Übergreifende Aspekte", "Infrastruktur", "IT-Systeme", "Netze" und "IT-Anwendungen" gruppierten Bausteine (= Kapitel), in denen für typische IT-Komponenten Standardsicherheitsmaßnahmen empfohlen werden. Diese berücksichtigen sowohl die technischen und infrastrukturellen, als auch die organisatorischen und personellen Aspekte der Informationssicherheit. Die Empfehlungen sind auf IT-Infrastrukturen mit mittlerem Schutzbedarf hin ausgerichtet, können aber auch als Basis für hochschutzbedürftige Systeme und Anwendungen dienen.

Der ermittelte Schutzbedarf bestimmt, welche Sicherheitsmaßnahmen umzusetzen sind:

- Bei normalem Schutzbedarf sind die möglichen Auswirkungen von Sicherheitsverletzungen begrenzt und überschaubar und es genügt im allgemeinen die Maßnahmenempfehlungen der IT-Grundschutz-Kataloge umzusetzen.
- Bei hohem Schutzbedarf drohen beträchtliche Schadensauswirkungen und daher sind ggf. höherwertige Schutzmaßnahmen erforderlich.
- Bei sehr hohem Schutzbedarf (katastrophale Schadensauswirkungen) ist der Einsatz höherwertiger Sicherheitsmaßnahmen sehr wahrscheinlich erforderlich.

Finanzkrise, Prozessketten und politische Steuerung

Die Debatte und die politischen Willensbildungs- und Entscheidungsprozesse zur Finanzkrise 2008 werden vorwiegend zum Thema neue Finanzarchitektur und Instrumente zu ihrer globalen Überwachung geführt. In Bezug zur Machbarkeitsstudie ist der Zusammenhang damit deutlich, dass es sich bei einer Vielzahl dieser Objekte der politischen Steuerung⁴ um Prozessketten zwischen Finanzdienstleistern und Verwaltungen handelt, die einen immensen Einfluss auf die Finanzwirtschaft und Realwirtschaft haben.

Neue Spielregeln in der Welt(finanz)wirtschaft reichen jedoch allein nicht aus. Damit Staaten die Möglichkeit haben politische Steuerung auszuüben, bedarf es des Umstands, dass das Thema (auch) ein IT-Thema auf der in-

⁴ M. G. Schmidt unterscheidet politikwissenschaftlich zwischen Steuerbarkeit des zu lenkenden Prozesses und Steuerungsfähigkeit derer, die lenkend tätig sind bzw. sein wollen: "Aussagen über die Steuerbarkeit beziehen sich auf "Antwortprozesse" (H. Bußhoff), die unter bestimmten Anfangsbedingungen und auf der Grundlage bestimmter Eingaben hervorgerufen werden oder im Fall der Nichtsteuerbarkeit unterbleiben. Die Steuerungsfähigkeit eines Akteurs oder lenkenden Systems hingegen "verlangt die Zugriffsmöglichkeiten zu den nötigen Eingabeprozessen am zu steuernden System, die Fähigkeit zur Beobachtung der relevanten Anfangsbedingungen sowie die Kenntnis der regelhaften Zusammenhänge zwischen Eingabeprozessen, relevanten Anfangsbedingungen und Antwortprozessen" (H. Bußhoff)." (Schmidt 1995: 937).

ternationalen Agenda wird. Proaktives globales Risikomanagement ist möglich, die Prozessketten müssen aber in mehrdimensionaler Hinsicht wirtschaftlich, prozessual und organisatorisch, IT-architektonisch, sicherheitstechnisch und juristisch richtig gemanagt sein.

Hierbei können Prozesslandkarten und Prozessbibliotheken einen wichtigen Beitrag leisten. Nicht zuletzt die Blaupause der Arbeitsgruppe um den ehemaligen EZB-Chefvolkswirt Issing für Kanzlerin Merkel zur Vorbereitung des Weltfinanzgipfels zeigen dies deutlich: Neben der Kontrolle von Hedge-Fonds und einem internationalen Kreditregister wird eine "Risiko-Weltkarte" vorgeschlagen, die Banken, Versicherungen, Hedge-Fonds und alle wichtigen Finanzprodukte verzeichnen soll (SPIEGEL ONLINE vom 13.11.2008).

3 Die FDL-Prozesskette in der IST-Situation

3.1 Erhebung der IST-Situation – angewandte Vorgehensweise "PRK-Screening"

Ausgangspunkt der Neugestaltung bzw. Optimierung einer Prozesskette zwischen Wirtschaft und Verwaltung ist das Wissen um den Status Quo einer existierenden Prozesskette.

PRK-Screening⁵

ist eine in der Machbarkeitsstudie entwickelte wissenschaftliche und praktische Methode, um Prozessketten in Bezug auf die wichtigsten Merkmale und deren Merkmalsausprägungen zu "screenen", d. h. zu durchleuchten.

Die Methode lässt sich je nach Einsatzzweck auf unterschiedliche Analyseebenen (z. B. vergleichende Analyse von Prozessketten bzw. Fallstudie etc.) anpassen.

Im folgenden wird die wissenschaftliche Vorgehensweise des im Projekt entwickelten "PRK-Screenings" in der Anwendung aufgezeigt. Nach der Benennung des Erkenntnisziels und der Fragestellung wird der wissenschaftliche Ansatz erklärt und die Methodenauswahl, Operationalisierung und Datenerhebung dokumentiert sowie der Nutzwert verdeutlicht (siehe zum wissenschaftlichen Vorgehen Alemann 1995: 71 ff., Schnell / Hill / Esser 1989: 109 ff.).

⁵ Screening (englisch) für Durchsiebung, Rasterung, Selektion, Durchleuchten; als Fachausdruck aus der Medizin stammend

Erkenntnisziel

Wissenschaftliches Ziel war die Beantwortung der Fragestellung 2 aus dem Kap. 1 "Wie kann die FDL-Prozesskette in der IST-Situation beschrieben und analysiert werden und wie sieht die Prozesskette in Deutschland aus?"

Wissenschaftlicher Ansatz

Als wissenschaftlicher Ansatz, der Forschungsdesign und Untersuchungsgegenstand widerspiegelt, wurden auf der Ebene der Originalität (1) eine Primärerhebung (Expertinnen- und Experteninterviews mit Banken und Bankdienstleistern) ausgewählt, die durch eine Sekundärerhebung (z. B. Checklisten von Deutsche Bundesbank, BaFin, Wirtschaftsprüfern wie z. B. KPMG 2001 etc.) als Qualitätssicherung ergänzt wurde.

Auf der Ebene der Reichweite (2) erfolgte eine vergleichende Analyse der Prozessketten und keine Fallstudien. Die Zeitebene (3) war eine synchrone Analyse, die im Zeitquerschnitt untersucht. Bei der Auswahlebene (4) handelt es sich vom Forschungsansatz her um eine Vollerhebung. Die Fokussierung der Akteure und die Auswahl, welche PRKs untersucht werden, wird weiter unten im Detail ausgeführt. Die Aggregationsebene (5) arbeitet sowohl mit Individualdaten (Expertinnen- und Experteninterviews mit Banken und Bankdienstleister) als auch mit Aggregatdaten aus SKM-Messungen des Statistischen Bundesamtes (Statistisches Bundesamt 2006: Methodenhandbuch und Statistisches Bundesamt 2008: SKM-Datenbank).

Insofern wird von der Akteur- / Systemebene (6) der Blickwinkel der Akteure (Bank) sowie des Systems (öffentliche Verwaltung als System) eingenommen. In Bezug auf die Realitätsebene (7) wurde eine empirische Feldstudie und keine experimentelle Studie durchgeführt.

Nachfolgende Tabelle zeigt den wissenschaftlichen Ansatz mit seinen im Projekt gewählten Analyseebenen im Überblick (nach von Alemann 1995: 82 ff.):

Dimensionen der Analyseebene	Theoretische Analyseebenen	Gewählte Analyseebene / n
(1) Ebene der Originalität	Primärerhebung	X
	Sekundärerhebung	X
(2) Ebene der Reichweite	Vergleichende Analyse	X
	Fallstudie	
(3) Zeitebene	diachrone Analyse (Längsschnitt)	
	synchrone Analyse (Querschnitt)	X
(4) Auswahlebene	Vollerhebung	X
	Auswahl (Stichprobe)	
(5) Aggregationsebene	Individualdaten	X
	Aggregatdaten	X
(6) Akteur- / Systemebene	Akteur	X
	System	X
(7) Realitätsebene	Feldstudie	X
	experimentelle Studie	

Tabelle 1: Wissenschaftlicher Ansatz von PRK-Screening am Beispiel der Untersuchung der FDL-Prozesskette in Deutschland

Methodenauswahl, Operationalisierung und Datenerhebung

Die Methodenauswahl fiel auf Expertinnen- und Experteninterviews bei einer Universalbank und eines Bankdienstleisters. Mit deren Fachabteilungen wurden im Rahmen von gemeinsamen Workshops je PRK Cluster gemeinsam mit der Gruppe der Forscher und entsprechend nachbereitet.

Es handelte sich um explorative Expertinnen- und Experteninterviews. In einem ersten Loop erfolgte ein Pretest des strukturierten Fragebogens und der "PRK-Screening" Materialien in Matrixtabellenform. In einem zweiten Loop wurden Fragebogen und Matrix validiert und optimiert bzw. partiell vereinfacht und bei Bedarf verfeinert. Auf dieser Basis konnte die Datenerhebung erfolgreich durchgeführt werden.

Die Operationalisierung hatte in diesem Forschungsprozess drei konzeptionelle Herausforderungen, die zu lösen waren:

1. Welcher Akteur bzw. welche Akteure aus der Gruppe der Wirtschaft im allgemeinen und der Finanzdienstleister im besonderen sollen als Untersuchungsobjekt der Machbarkeitsstudie fokussiert werden?
2. Welche Prozessketten (und mit wem auf der staatliche Seite vis-a-vis der genannten ersten Gruppe) werden in den Untersuchungsfokus aufgenommen und welche nicht?
3. Auf welche Merkmale und Merkmalsausprägungen werden genau diese ausgewählten Prozessketten "gescreent"?

PRK-Screening: Branchenkompass

Zur Beantwortung der erstgenannten konzeptionellen Frage fokussiert das Autorenteam der Studie auf einen Branchenkompass, der in Anlehnung des **NACE-Branchen Codes** erstellt wurde (siehe Abbildung 6).

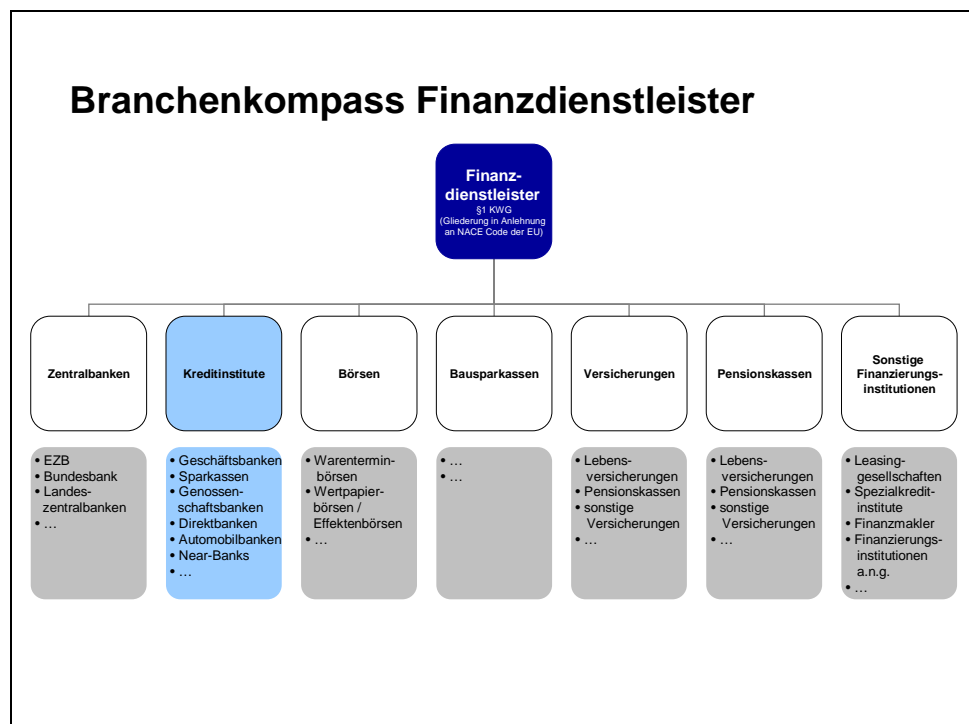


Abbildung 6: Branchenkompass Finanzdienstleister (Quelle: Eigene Darstellung)

Diese Branchenkompass wurde auf Basis des NACE ("Nomenclature statistique des activités économiques dans la Communauté européenne") Codes, sowie der Unterteilung der in §1 des KWG genannten Organisationen

erstellt. Diese statistische Systematik der Wirtschaftszweige in der Europäischen Union ist ein System zur Klassifizierung von Wirtschaftszweigen. Grundlage der Arbeiten im Rahmen der Machbarkeitsstudie war die verfügbare Dokumentation mit dem Stand von April 2008. Dabei wurde vor allem auf den **Abschnitt K (Erbringung von Finanz- und Versicherungsdienstleistungen), Abteilung 64 bis 66** referenziert (Statistisches Bundesamt 2008: 22).

Wie in Abbildung 6 dargestellt, wurde die Unterteilung der Branche der Finanzdienstleister in sieben Kategorien vorgenommen. Diese sind:

- Zentralbanken
- Kreditinstitute
- Börsen
- Bausparkassen
- Versicherungen
- Pensionskassen
- Sonstige Finanzierungsinstitutionen

Aufgrund der Komplexitätsreduktion und besseren Handhabbarkeit der Arbeiten, wurde im Rahmen der Machbarkeitsstudie festgelegt, eine Fokussierung auf die Kreditinstitute zu legen und anhand dieses Beispiels die Arbeiten zu den Prozessketten darzustellen.

Dabei werden im Rahmen der Machbarkeitsstudie die Begriffe "Kreditinstitut" und "Bank" synonym verwendet.

PRK-Screening: Untersuchungsgegenstand

Zur Beantwortung der zweiten konzeptionellen Frage staffelte das Autorenteam der Studie die Prozessketten in drei Klassen einer Pyramide, wie die Abbildung 7 zeigt.

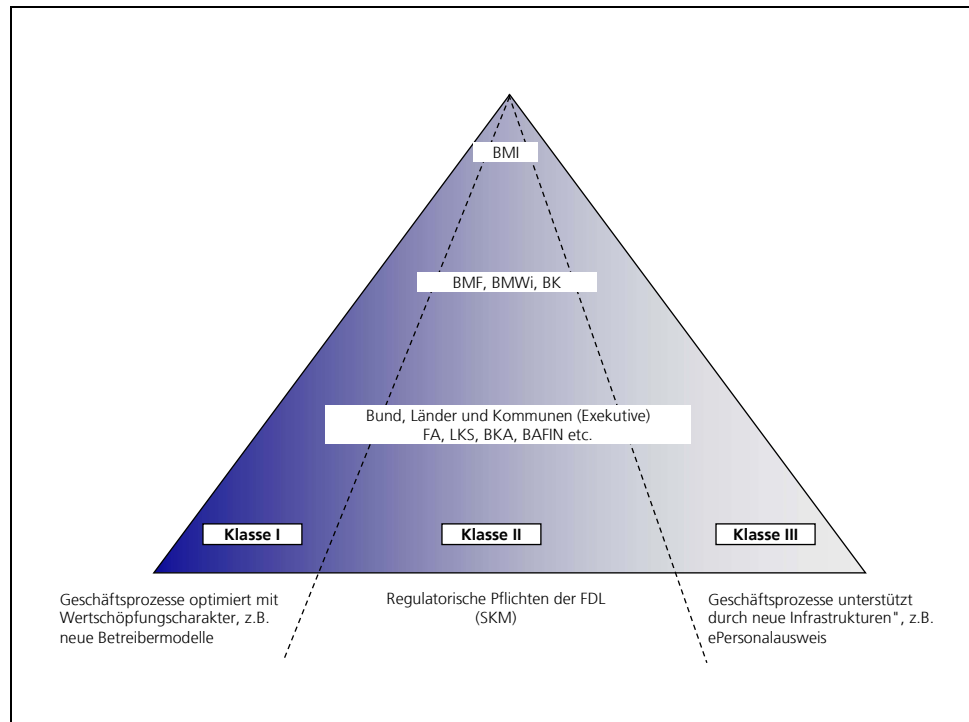


Abbildung 7: Die PRK Pyramide (Quelle: Eigene Darstellung)

Die bei der Klassifizierung zugrunde gelegte Fragen bezogen sich auf die regulatorischen Pflichten sowie auf zukünftige Gestaltungsoptionen und die Nutzung neuer Technologien und Infrastrukturen. Als Ergebnis der Projektarbeiten wurden folgende Klassen von Prozessketten im Projekt definiert:

Klasse I:

Prozessketten, die einen neuen Wertschöpfungscharakter besitzen und deren Realisierung entsprechende neue Betreibermodelle, sowohl von Seite der Banken als auch der öffentlichen Verwaltung, voraussetzen. Diese Prozesskettenklasse bietet für alle beteiligten Akteure sehr große Gestaltungsspielräume.

Klasse II:

Prozessketten, die aufgrund regulatorischer Pflichten von Seite der Banken zu erfüllen sind. Für diese Prozessketten gibt es wenig bis keinen Spielraum, da sie aufgrund gesetzlicher Regelungen etabliert sein müssen. Lediglich die Art und Weise der Erfüllung dieser Pflichten gibt den Beteiligten einen gewissen Gestaltungsspielraum.

Klasse III:

Prozessketten die erst durch den Einsatz und die Nutzung neuer Technologien ermöglicht werden. Technologien ermöglichen erst die Gestaltung dieser Art von Prozesskettenklasse. Auch hier ist ein begrenzter Gestaltungsspielraum für alle Beteiligten gegeben, da die Technologien sowohl von Seite der Banken als auch von Seiten der öffentlichen Verwaltung für den Einsatz und Nutzung freigegeben und bestimmte Voraussetzungen dafür erfüllt sein müssen.

Die Untersuchungen im Rahmen der Machbarkeitsstudie haben gezeigt, dass vorhandene Prozessketten sehr stark anhand der regulatorischen Pflichten erfolgen, welche Finanzdienstleister unterworfen sind. Aus diesem Grunde wurde die Entscheidung getroffen, **alle Prozessketten der Klasse II, der gesetzlichen Meldepflichten, und Klasse III, Unterstützung aufgrund neuer Infrastrukturen, in den Untersuchungsfokus aufzunehmen**. Die Prozessketten der Klasse I werden im Rahmen der Beschreibung neuer Geschäfts- und Betreibermodelle berücksichtigt.

PRK-Screening: Merkmale

Zur Beantwortung der dritten konzeptionellen Frage traf das Autorenteam der Studie eine Auswahl von Merkmalen, deren Merkmalsausprägungen mit Werkzeugen zu untersuchen sind, die in den Anhängen der Studie dokumentiert und zur Selbstanwendung angeboten sind. Diese wurden rückgespiegelt mit Erfahrungen, die die öffentliche Hand in Empfehlungsdokumenten gemacht und zur Anwendung vorgeschlagen hat (BMI 2007b und www.dvdv.de)

Es wurde auf folgende **sechzehn PRK-Screening Merkmale** untersucht:

1. ID (Festlegung)
2. Name der PRK
3. Gesetzliche Anspruchsgrundlage
4. Wertschöpfungscluster (Bankensektor)
5. Involvierte Akteure (Bank)
6. Involvierte Akteure (Verwaltung)
7. Qualitative Relevanz: Notfallrelevanz, Risikobezug (Bank)

8. Quantitative Relevanz: Fristigkeiten (Bank)
9. Quantitative Relevanz: Prozessfallzahl p.a. (Bank)
10. Quantitative Relevanz: Durchlaufzeit (hoch, mittel, gering) (Bank)
11. Quantitative Relevanz: Kosten (hoch, mittel, gering, ggf. quantifizieren) (Bank)
12. Vorhandene Prozessmodellierung (Bank)
13. Beschreibung der PRK Workflows (Bank - Verwaltung)
14. Beschreibung des Rückkanals (Verwaltung - Bank)
15. PRK Generation⁶
16. PRK Kosten⁷

⁶ die mit Fußnote bezeichneten Merkmale sind mit der SKM-Datenbank (siehe Kap. 3.2.3) abgeglichen (Sekundäranalyse, Aggregatdaten); die anderen Merkmale sind mittels der Primäranalyse im Projekt (Bankeninterviews, Individualdaten) erhoben worden

⁷ s. o.

Exkurs Modellierung FMC

Im Rahmen der FMC Diagramme werden folgende Symboliken verwendet:


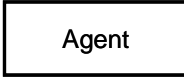




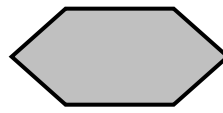

Fundamental Modeling Concepts (FMC) Aufbau- oder Blockdiagramme	
Symbol	Bedeutung
 	<p>Aktive Systemkomponenten (rechteckige Symbole): maschinelle Agenten, menschliche Akteurinnen und Akteure</p> <p>Die Agenten können Softwarekomponenten oder Personen mit einer bestimmten Rolle sein.</p>
 	<p>Passive Systemkomponenten (runde oder ovale Symbole): Speicher, Dokumente, Kanäle</p> <p>Die Speicher sind in der Regel Datenbanken aber auch Dokumente. Die Kanäle, kleiner Kreis, halten selbst keine Daten sondern übertragen diese nur. Sie stellen die Übergabepunkte (Schnittstellen) zwischen den Systemen dar.</p>
 	<p>Gerichtete und ungerichtete Kanten: Datenfluss</p> <p>Eine Kante darf nur zwei Knoten verschiedener Klassen verbinden (Agent, Storage)</p>

Tabelle 2: Legende zu den Architekturdarstellungen (FMC)

Exkurs Modellierung von Prozessen mittels EPK

Im Rahmen der Prozessdarstellung mit Ereignisgesteuerten Prozesskette werden folgende Symboliken verwendet:

Bezeichnung	Symbol	Beschreibung
Ereignis		Ereignisse sind zeitpunktbezogene Zustände. Das Eintreten eines Ereignisses zieht eine bestimmte Folge nach sich.
Funktion		Die Funktion beschreibt die Transformation von einem Eingangszustand (Input) in einen Zielzustand (Output)

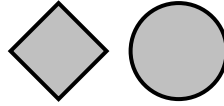


Verzweigungsoperatoren		Verzweigungsoperatoren beschreiben die logische Verbindung zwischen Ereignissen und Funktionen. Diese treten als "exklusive-oder", "oder" sowie "und" Operatoren auf.
Prozess		Ein Prozess ist eine logische Folge von Aktivitäten
Informationsfluss		

Tabelle 3: Legende zur Prozessmodellierung mittels EPK

3.2 Erhebung der IST-Situation – Ergebnisse

Das Forschungsvorhaben mit der Fragestellung "Wie kann die FDL-Prozesskette in der IST-Situation beschrieben und analysiert werden und wie sieht die Prozesskette in Deutschland aus?" führte zu folgenden Ergebnissen.

3.2.1 Ergebnis I: Prozessketten Wertschöpfungscluster

Projektarbeiten sowie die "Studie Bank & Zukunft" zeigen, dass Banken sich in Zukunft prozessorientiert organisieren werden (Spath / Engstler / Praeg / Vocke 2008).

In Anlehnung an das Konzept der Wertkette nach Porter (Porter 2000: 64 ff.) werden Banken in strategisch relevante Tätigkeiten gegliedert. Im Rahmen der Prozessketten ist die Wertkette einer Organisation (z. B. Bank) mit denen der Partner verbunden. Die Wertkette ist dabei eine Ansammlung von Tätigkeiten, durch die eine Leistung oder ein Produkt hergestellt, vertrieben, ausgeliefert und unterstützt wird (Porter 2000: 67). Die Wertkette lässt sich prinzipiell in zwei Typen untergliedern. Die primären Prozesse, die in Abbildung 8 im unteren Teil dargestellt sind, befassen sich mit der direkten Dienstleistung an Kundinnen oder Kunden der Bank. Die unterstützenden Prozesse sorgen dafür, dass die primären Prozesse in der Bank aufrecht

gehalten werden können und bieten daher einen indirekten Beitrag zur Wertschöpfung einer Bank.

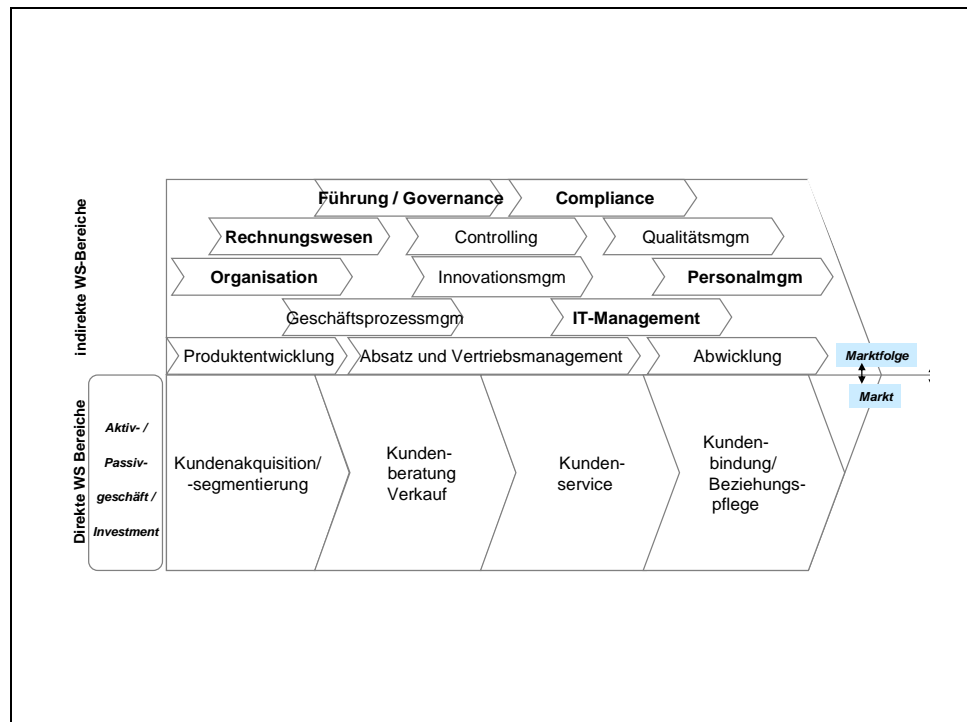


Abbildung 8: Prozessorientierte Sicht auf eine Bankorganisation (Quelle: Eigene Darstellung)

Die Bank als Organisation besteht somit aus einer bestimmten Anzahl miteinander interagierender Prozesse, welche direkt und / oder indirekt zur Wertschöpfung der Bank beitragen.

Um die Anzahl der Prozesse in einer überschaubaren Anzahl halten zu können, wurden im Rahmen der Projektarbeiten sogenannte Wertschöpfungscluster gebildet. Diese Wertschöpfungscluster können anhand von verschiedenen Kriterien typologisiert werden:

- Wertschöpfungsbereiche
- Strategische Bedeutung
- Bearbeitungsobjekt
- Funktion

- Prozessinput /-output
- etc.

Für die Clusterung im Rahmen der Machbarkeitsstudie wurde die Typologie der **Wertschöpfungsbereiche** herangezogen. Die Gründe dafür sind:

- Diese bleiben im Zeitablauf stabil.
- Durch die zunehmende Auslagerung von Organisationsbereichen und Geschäftsprozessen bei Banken wird sich die Organisationsstruktur nachhaltig verändern. Wertschöpfungsbereiche bilden in sich stabile Gebilde.
- Banken werden sich zukünftig anhand dieser Wertschöpfungsbereiche orchestrieren.

Im Rahmen der Projektarbeiten wurden aufgrund von Einschätzungen von Expertinnen und Experten folgende Cluster gebildet:

Direkte Wertschöpfungscluster	Indirekte Wertschöpfungscluster
Kundenakquisition / -segmentierung	Führung
Kundenberatung und Verkauf	Governance
Kundenservice	Compliance
Kundenbindung	IT-Management
	Personal
	Rechnungswesen
	Abwicklung
	Produktentwicklung

Tabelle 4: Wertschöpfungscluster Banksektor

Aufgrund der Entwicklungen im Bankensektor und der zunehmend verteilten Wertschöpfung von Banken, durch Auslagerung von Prozessen und Wertschöpfungscluster, könnte eine Bank an sich zukünftig nur noch als "organisatorische Hülle" fungieren, in deren Hintergrund verschiedene Partner im Rahmen der Wertschöpfung einzelne Teilleistungen für den Marktbereich einer Bank in-time bereitstellen.

Ergebnis I lautet: Es gibt **Wertschöpfungscluster**, d. h. definierte Stellen an denen die Wirtschaft (Sender) ihre Meldungen an die öffentliche Verwaltung (Empfänger) abschickt. Und über die sie Rückmeldungen des Systems wieder empfängt.

Abbildung 9 zeigt die Folgen dieser orchestrierten Leistungserstellung, sowie die damit verbundenen Verpflichtungen der einzelnen Wertschöpfungscluster in Bezug auf die regulatorischen Vorschriften (Meldungen, Anzeigen, etc.) an der Schnittstelle einer Bank und Einrichtungen der öffentlichen Verwaltung.

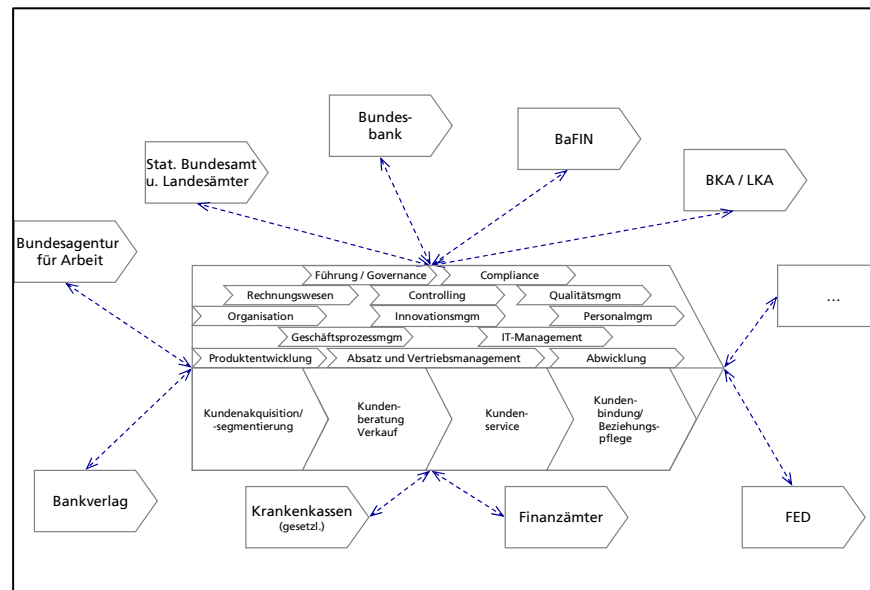


Abbildung 9: Ergebnis – PRK Wertschöpfungskuster (Quelle: Eigene Darstellung)

Es ist jedoch nicht zwingend erforderlich, dass jedes Wertschöpfungskuster mindestens eine Schnittstelle zur öffentlichen Verwaltung besitzt.

3.2.2 Ergebnis II: Prozessketten Generationen

Ergebnis II lautet: es sind bei Prozessketten **Generationen** beobachtbar, im Sinne von Entwicklungsstand, Innovationshöhe und Reifegrad (siehe Abbildung 10).

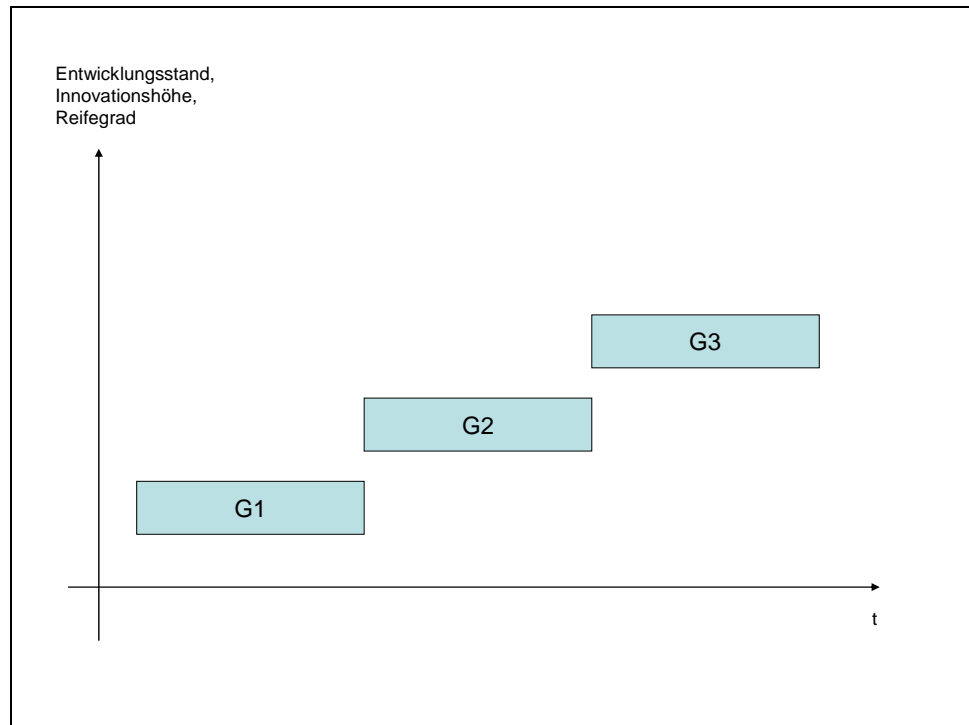


Abbildung 10: Ergebnis – PRK Generationen (Quelle: Eigene Darstellung)

Generation 1 (G1) meint in diesem Bild die papiergebundene Interaktion, die durch reale Transaktionen wie Gelber Post, Kurierdienste etc. unterstützt wird.

Generation 2 (G2) zielt ab auf (IT-)anwendungsorientierte Interaktion, d. h. dass Datenströme in unterschiedlichen Formaten, auf unterschiedlichen Medien, über unterschiedliche Netze bzw. Kanäle etc. im Hin- und Rückkanal zwischen Wirtschaft und öffentlicher Verwaltung laufen.

Generation 3 (G3) ist infrastrukturorientiert. Auf einer (Web-)Plattform mit an den realen Geschäftsprozessen orientierten elektronischen Diensten und digitalen Inhalten können die betroffenen Stakeholder ihre ganzheitlichen Prozesse managen. Die Plattform bietet zugeschnittene Lese- und Schreibrechte für alle Mitglieder der Prozesskette (rollenbasierter 24 / 7 Pull-Service auf Anfrage). Die Plattform ist im Hol- und Bringschuld Management intelligent konfiguriert und gibt Benachrichtigung an dedizierte Adressaten bei Systemzustandsänderungen (orts-, zeit- und situationsbedingter Information-Push).

3.2.3 Ergebnis III: Quantitative und qualitative Ergebnisse

Quantitative Ergebnisse

Es wurden im PRK-Screening **154 Prozessketten** und Verwaltungsverfahren zwischen Banken und Verwaltungen in Deutschland identifiziert.⁸

Alle Prozessketten basieren auf Gesetzen, Verordnungen und Normen. In Bezug auf das Merkmal "**Gesetzliche Anspruchsgrundlage**" lässt sich folgendes Ranking der Häufigkeitsverteilungen der Herkunft aufstellen (n= 217, Mehrfachzuordnungen möglich):

1. **KWG (51,6 Prozent)**
 2. **AnzV (18,4 Prozent)**
 3. **GroMiKV (7,8 Prozent)**
 4. SGB (3,2 Prozent)
 5. BBankG (2,8 Prozent)
 5. SolvV (2,8 Prozent)
- Rest: Sonstige

⁸ PRK aus den Gesetzesbereichen AAG, Abgabenordnung, AnzV, ArbschG, AWG, AWV, BBankG, BStatG, ErbStG, EStDV, FkSolV, GroMiKV, GwG, Insolvenzordnung, KWG, LrV, MaRisk, MuSchG, SGB, BBKG, MonAwV, SolvV, VerdStaG, Zu-MonAwV, InvG; z. B. der Bereich Steuer wurde ausgeschlossen

Bei der Zuordnung der PRK zu den genannten "**Wertschöpfungsclustern (Bankensektor)**" war folgende Häufigkeitsverteilung zu beobachten (n= 154) (siehe Abbildung 11):

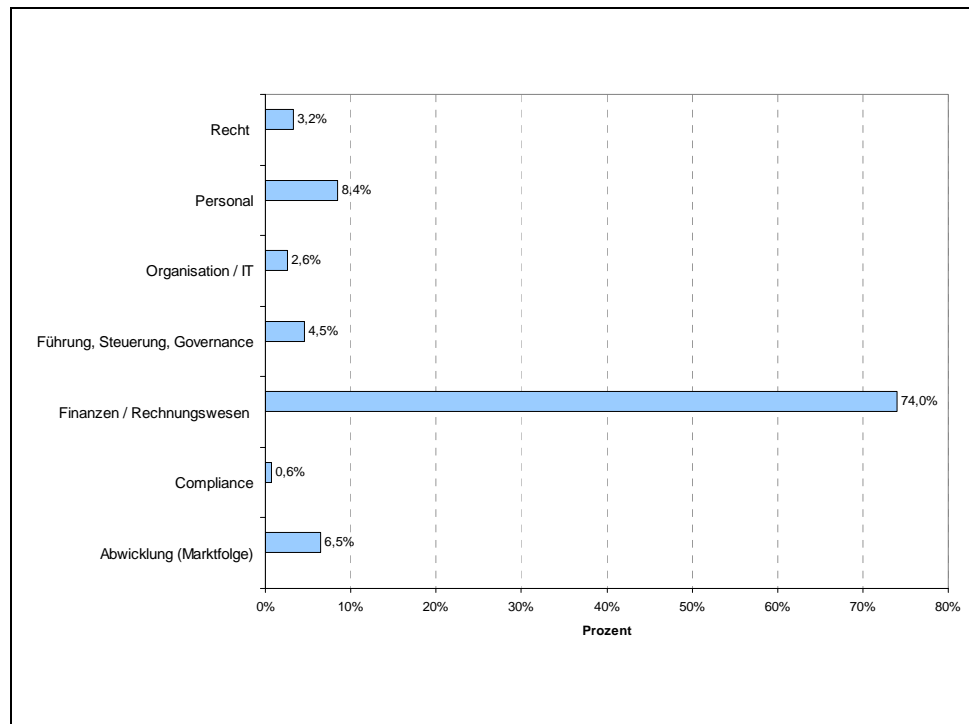


Abbildung 11: Ergebnis – Häufigkeitsverteilung der Wertschöpfungscluster (Bankensektor) in der FDL-PRK (Quelle: Eigene Darstellung)

Der Großteil der PRK wird mit **insgesamt 112 PRK vom Wertschöpfungscluster Finanzen / Rechnungswesen betrieben**, was 74 Prozent aller vorhandenen PRK zwischen Banken und Verwaltung entspricht.

Zum Merkmal "**Involvierte Akteure (Verwaltung)**" ergab sich folgende Verteilung (n= 240, Mehrfachzuordnungen möglich) (siehe Abbildung 12):

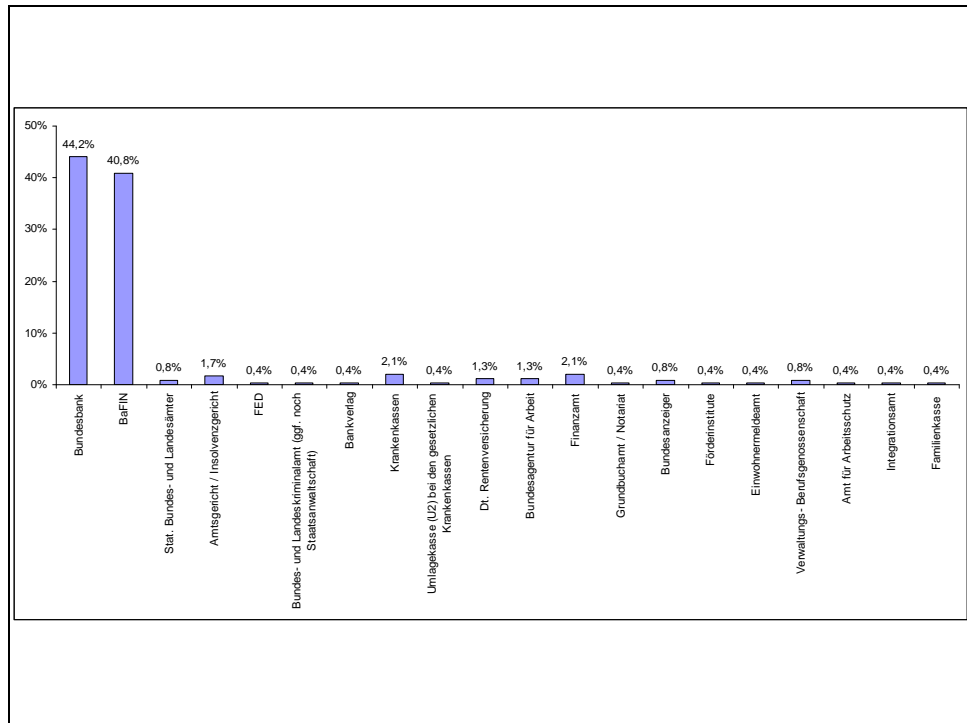


Abbildung 12: Ergebnis – Häufigkeitsverteilung der involvierten Akteure (Verwaltung) in der FDL-PRK (Quelle: Eigene Darstellung)

Die Banken haben eine große Anzahl ihrer Interaktionen mit der **Bundesbank (44,2%)** und der **BaFin (40,8%)**. Andere Verwaltungen sind im Vergleich dazu mit sehr geringen Häufigkeiten vertreten.

Mit Hilfe der Zuordnung vorhandener PRK zu den "**Generationen G1, G2 und G3**" konnten die PRK evaluiert werden. Es wurde hierzu die beste bekannte Merkmalsausprägung aus den Individualdaten Expertinnen- und Experteninterviews des Projekts und den Daten aus der SKM-Datenbank des Statistischen Bundesamtes (Version 1.3.12 Wirtschaft, mit Stand vom 20. Oktober 2008)⁹ herangezogen. Das Merkmal spannt folgende Häufigkeiten bei den empirischen Merkmalsausprägungen auf (n= 154) (siehe Abbildung 13):

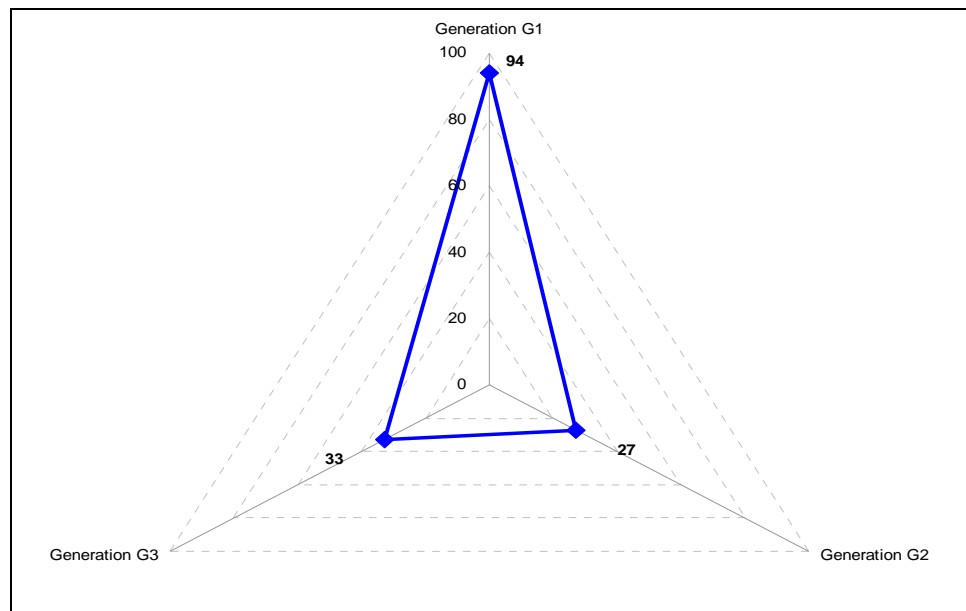


Abbildung 13: Ergebnis – Häufigkeitsverteilung von Generation G3, G2 und G1 in der FDL-PRK (Quelle: Eigene Darstellung)

⁹ Informationspflicht online ja + Unterlagen online ja = G3
 Informationspflicht online ja + Unterlagen online nein = G3
 Informationspflicht online nein + Unterlagen online ja = G2
 Informationspflicht online nein + Unterlagen online nein = G1

Das heißt:

- **94 der 154 PRK** (61%) sind als **G1** einzuschätzen, es gibt sowohl in den Interviews, der SKM-Datenbank als auch in den Gesetzestexten, Verwaltungsvorschriften, Checklisten der Behörden etc. keine Hinweise darauf, dass eine "elektronische Steckdose" zur Verwaltung existiert.
- **27 der PRK** sind der **G2** (17,5%) zuzuordnen.
- Als fortschrittliche **G3** ausgewiesen sind **33 PRK** (21,4%).

Um bestmögliche Werte für das Merkmal "**Kosten**" für die betreffenden 154 PRK der FDL-PRK anzugeben, wurden die untersuchten PRK mit den Informationspflichten (IP) der SKM-Datenbank abgeglichen (Version 1.3.12 Wirtschaft mit Stand vom 20. Oktober 2008). Das ergab folgendes Gesamtbild:

- Von der Grundgesamtheit der 154 PRK konnten 88 IPs zugeordnet werden.¹⁰
- Zu 85 der 88 betreffenden PRK liegen vom Statistischen Bundesamt entsprechend gemessene Kosten vor (für die Wirtschaft in Deutschland in Euro p. a.).
- Die Spannweite der Kosten für eine PRK reicht von ca. 0 Euro bis 292.733.000 Euro
- In der Histogrammverteilung sind **35 PRK mit weniger Belastung für die Wirtschaft verbunden als 50.000 Euro** (41,2%); **12 PRK kosten**

¹⁰ Die Anzahl der nicht zuordenbaren PRK – Informationspflichten liegt vor allem darin begründet, dass für die Daten in der SKM-Datenbank die Stichtagsregelung gilt, d. h. es wurden die Informationspflichten erfasst und gemessen, deren rechtliche Grundlagen am 30.09.2006 mindestens zwei Jahre in Kraft waren. Weiterhin ist z. B. die Bundesbank ermächtigt, von sich aus bestimmte Meldepflichten einzufordern, z. B. durch ein Rundschreiben. Solche Meldepflichten oder Prozesse werden nicht in der SKM-Datenbank erfasst.

Die durchgeführte Analyse bezieht sich zum einen auf das "Kreditwesengesetz in der Fassung der Bekanntmachung vom 09.09.1998 (BGBl. I S. 2276) zuletzt geändert durch Artikel 2 des Gesetzes vom 21.12.2007 (BGBl. I S. 3089" und der Verordnung über Anzeigen und die Vorlage von Unterlagen nach dem Kreditwesengesetz (Anzeigeverordnung- AnzV) vom 19.12.2006 und zum anderen auf die Übersicht der gesetzlichen Anzeige- bzw. Meldepflichten für Institute der Deutschen Bundesbank- Zentralbereich Banken und Fachaufsicht- B40-4 Stand Juli 2008. Daher können gerade aufgrund der Änderung der Paragraphen aus dem KWG der AnzV nicht eindeutig der SKM-Datenbank zugeordnet werden, zumal Meldepflichten dazu gekommen sind aber auch andere wiederum weggefallen sind.

mehr als 1.000.000 Euro (15,3%), zwischen diesen Schwellenwerten firmieren 37 PRK in der Mittelgruppe (43,5%).

Qualitative Ergebnisse

Bezüglich der qualitativen Aspekte bei der Untersuchung der 154 PRK ergaben folgende qualitative Erkenntnisse:

- Eine **Vielzahl identifizierter Prozessketten und Schnittstellen sind konzentriert** auf wenige Akteure in der öffentlichen Verwaltung.
- Es bestehen **keine Meldepflichten innerhalb der Bankenbranche** ("Stichwort: Branchenweite Prozessintegration des Levels-1 auf Systemebene)", sondern zur Bankenaufsicht und anderen öffentlichen Verwaltungen.
- Viele Prozessketten sind **Unikate**; es gibt in der Schnittstellenbetrachtung zwischen Wirtschaft und Verwaltung kaum generische Muster, die für eine Professionalisierung und Rationalisierung auf beiden Seiten auf Antrieb erkennbar sind.
- **Steckdosen zur Verwaltung** - es ist den Mitarbeiterinnen und Mitarbeitern im Bankensektor **oft nicht bekannt**, ob es sie gibt und wo ihre Existenz kommuniziert wird (Hol- und Bringschuld für beide Partner).
- Es gibt grundsätzlich **wenig Rückkanalmeldungen von der Verwaltung** an die Banken, und wenn dann nur ad-hoc im Krisenfall (geschäftliche Logik vs. Logik des Verwaltungshandelns).

3.2.4 Ergebnis IV: Prozesslandkarte und Prozessbibliothek

Die Ergebnisse in Kap. 3.2.3 stellen zweierlei dar – die Datenbank an sich bietet den Kern einer **Prozessbibliothek**, wie sie über alle PRK in Deutschland zwischen Wirtschaft, Verwaltung und Bürgerinnen und Bürgern aufzubauen ist.

Doch mit einer Datenbank allein sind keine Menschen zu erreichen, mitzunehmen und zu überzeugen – auf dem Weg hin zu Verwaltungsmodernisierung und Bürokratieabbau in Wirtschaft und Verwaltung.

Es bedarf dreierlei:

- PRK müssen visualisiert werden ("**Prozesslandkarte**").
- PRK müssen such- und findbar, **interaktiv** aufrufbar und in der nächsten Ausbaustufe dynamisch mit Realdaten vernetzt sein (z. B. Daten der SKM-Messung werden als Webservices eingebettet etc.).
- Die Prozesslandkarte hat dann eine Zukunft, wenn sie nicht proprietär sondern auf eine **Webbrowser-basierten Open-Source-Lösung** basiert.

Vor dem Hintergrund dieser Herausforderungen hat Fraunhofer IAO die Daten der Studie über ein Framework aufbereitet.

Dabei zeigt Abbildung 14 das Schema einer Prozesslandkarte, welche auf Basis der Ergebnisse erstellt wurde.

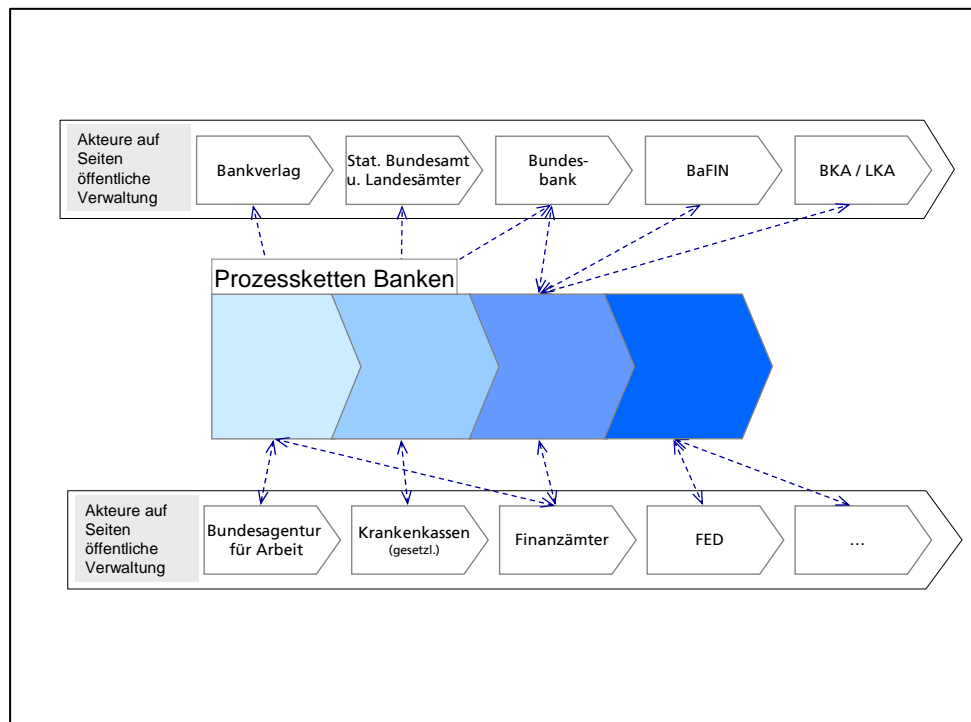


Abbildung 14: Prozesslandkarte für die identifizierten PRK zwischen Verwaltung und FDL (Quelle: Eigene Darstellung)

Drei exemplarische Bilder sollen als Screenshots die Arbeit mit der Prozesskette verdeutlichen.

Das erste Bild verdeutlicht die Systematik der Darstellung im Prozesskettenbrowser für die FDL-PRK in Deutschland (siehe Abbildung 15).

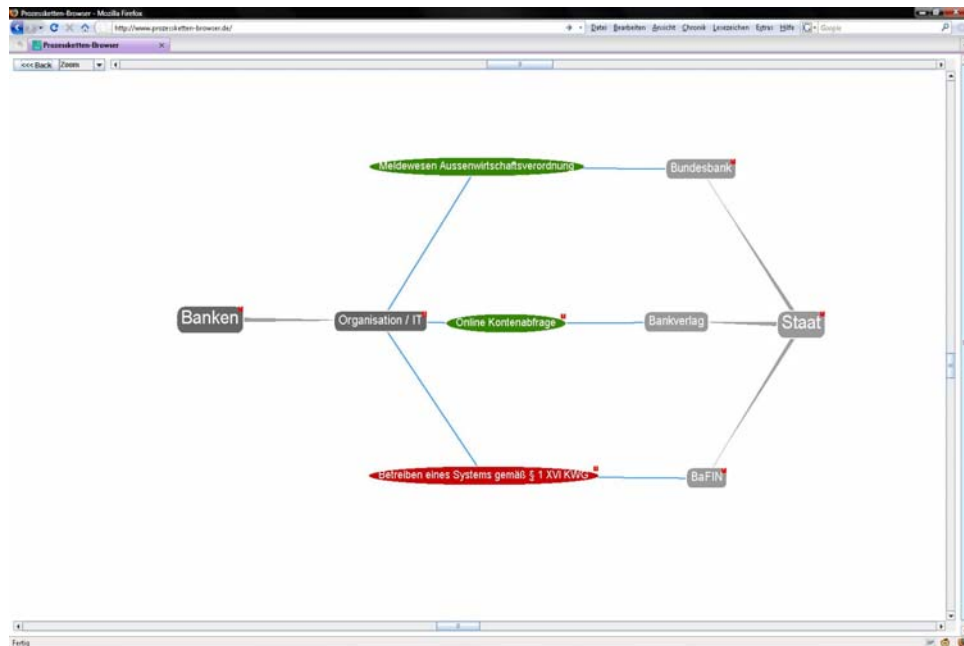


Abbildung 15: Systematische Visualisierung von PRK mittels Prozesskettenbrowser (Quelle: Eigene Darstellung)

Das zweite Bild zeigt als Beispiel die PRK "Geldwäscheverdachts-Anzeige" zur Fallstudie in Kap. 8 (siehe Abbildung 16).

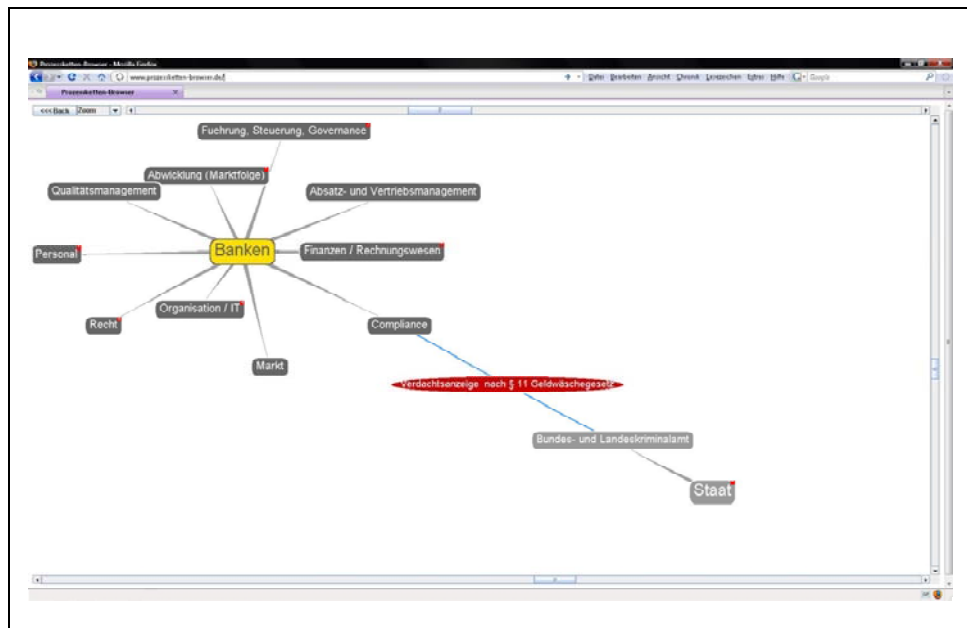


Abbildung 16: Ergebnis – Die PRK "Geldwäscheverdachts-Anzeige" im Prozesskettenbrowser (Quelle: Eigene Darstellung)

Das dritte Bild zeigt die FDL-PRK in Deutschland in ihrer Gesamtheit (siehe Abbildung 17).

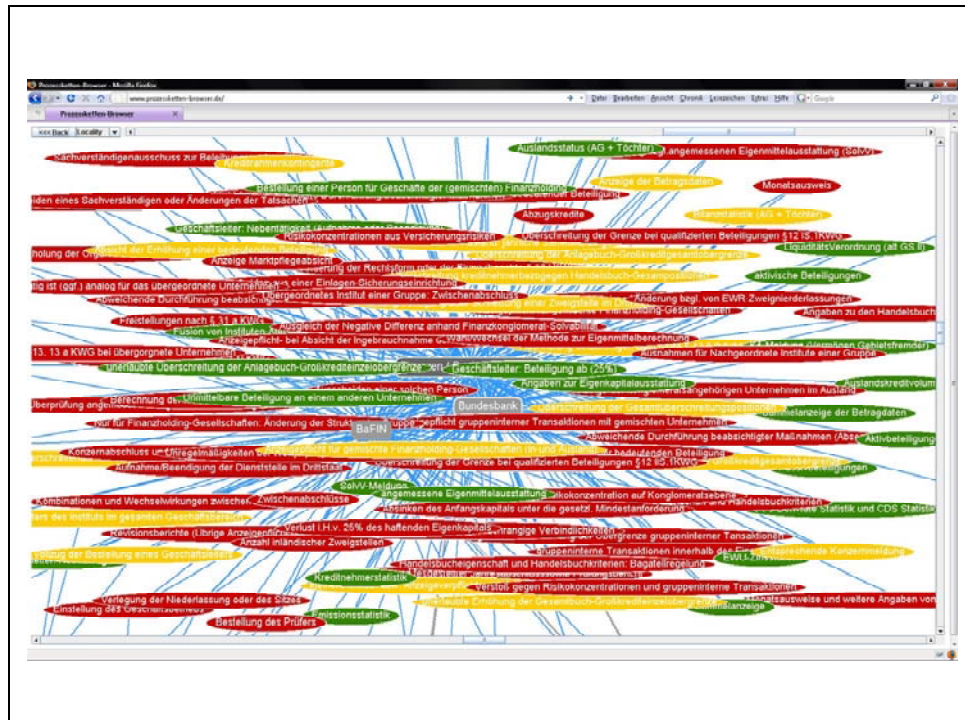


Abbildung 17: Ergebnis – Die Prozesslandkarte FDL-PRK in Deutschland im Prozesskettenbrowser (Quelle: Eigene Darstellung)

Die Farben signalisieren in Ampellogik "rot" für PRK der Generation 1, "gelb" für G2 und "grün" für die fortschrittlichsten PRK der G3. Einzelne PRK bzw. Akteure lassen sich im Webbrowser dynamisch anordnen, aufklappen, filtern zoomen u. ä. Über "Mouse-Over" lässt sich Prozessbibliothek-Wissen interaktiv aufrufen (Prozessmodellierungsschaubilder, XML-Schemata, AGB, DVDV-Verzeichnisse, Deutschland-Online Dienste, andere Webservices etc.).

Die erhobenen Daten befinden sich im **Anhang I - Prozessbibliothek "FDL-Prozesskette in Deutschland" – Ergebnistabelle des PRK-Screenings**.

3.2.5 Ergebnis V: Best Practices Bundesbank-Extranet und Kontenstammdatenbereitstellung

Um die Ziele und Anforderungen für eine IT-Architektur zur Bildung von organisationsübergreifenden Prozessketten zu definieren, wurde zunächst eine generalisierte IST-Analyse von bestehenden Prozessketten zwischen FDL und Verwaltung durchgeführt. Diese IST-Analyse diente dem Zweck, bereits eingesetzte IT-Komponenten und -Technologien zu identifizieren und sie mit den Zielen und Anforderungen an eine SOLL-Architektur, die dem aktuellen State-of-the Art entsprechen soll (u. a. Berücksichtigung des SAGA-Standards) abzugleichen.

Bei diesem PRK-Screening fielen besonders zwei Best Practices auf: das Bundesbank Extranet und die PRK Kontenstammabfrage.

Status Quo

Aus der IST-Analyse konnten folgende Gruppen von Prozessen zwischen FDL und Bundesbehörden (hauptsächlich Bundesbank und BaFin) abgeleitet werden:

- Gesetzlich vorgeschriebene Standardberichte (unterschiedlicher Wichtigkeit und Berichtszeiträume)
- Berichte auf Anfrage
- Gesetzlich vorgeschriebene Datenbereitstellung

Hinzu kommen Berichte an internationale Organisationen (z. B. aus EU und USA).

Je nach Anwendung und Bereich gibt es Unterschiede in der elektronischen Vernetzung (siehe Abbildung 18).

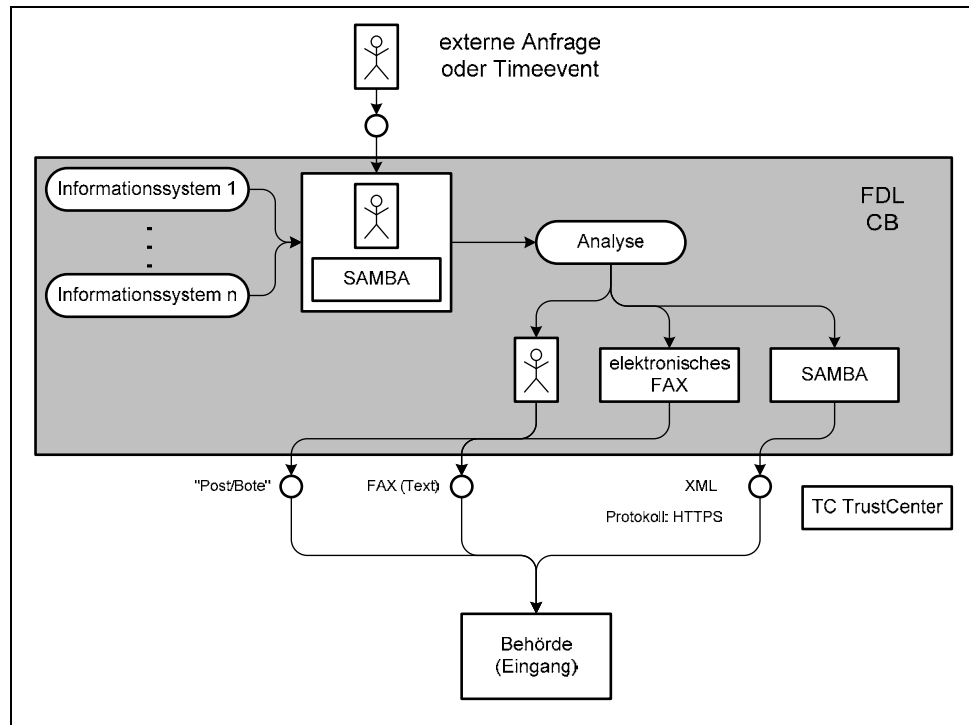


Abbildung 18: Allgemeine IST IT-Architektur zwischen FDL und Verwaltung (FMC) (Quelle: Eigene Darstellung)

In der Regel werden auf Anfrage (Brief, Telefonanruf) oder durch gesetzliche Vorgaben Analysen angestoßen und von Mitarbeiterinnen und Mitarbeitern in Organisationen und / oder IT-Anwendungen, z. B. die Anwendung Standard Anwendung Meldewesen Banken (SAMBA) (www.logicacmq.com) ausgeführt. Das Ergebnis der Analyse wird dann per Post, Fax (eventuell elektronisch) oder durch eine Anwendung (z. B. SAMBA) an die Behörde geschickt.

Best Practice Bundesbank Extranet

Eine Behörde ist die Deutsche Bundesbank (BB) und eine empfangende bzw. sendende IT-Infrastruktur ist das Extranet der BB (Deutsche Bundesbank 2008).

Hierbei handelt es sich um eine Webanwendung, die sich sowohl interaktiv von entfernten externen Nutzerinnen oder Nutzern als auch aus eigenen Fachanwendungen der FDL nutzen lässt (siehe Abbildung 19).

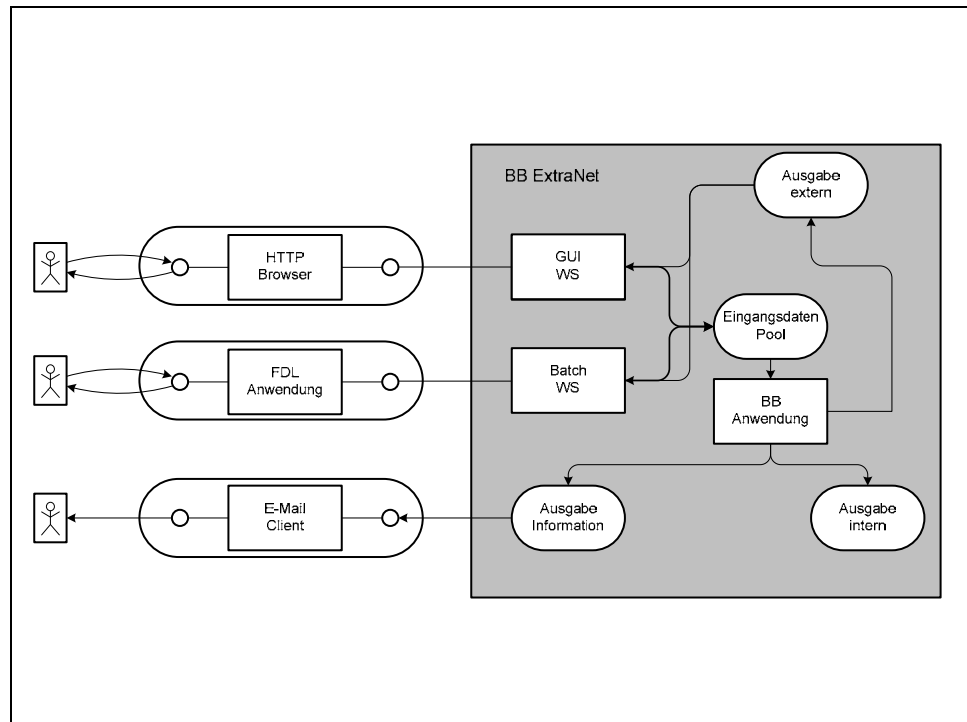


Abbildung 19: Best Practice Architektur Bundesbank ExtraNet (FMC) (Quelle: Eigene Darstellung)

Daten für einige Fachanwendungen der BB können in ein Web-Frontend eingegeben werden oder über eigene Anwendungen nach einem bestimmten Protokoll übermittelt werden, deren Eingang quittiert wird. Die Daten-Dateien stehen dann in einem Eingabedatenpool zur weiteren Verarbeitung bereit. Ist die Eingabe ein Antrag oder eine Anfrage, die eine Antwort von einer Fachanwendung erfordert, so wird diese Antwort im Ausgabebereich bereitgestellt und die Kundinnen und Kunden werden per E-Mail darüber informiert.

Es handelt sich also um eine asynchrone ereignisgesteuerte Prozesssteuerung. Inhalte und Formate bestimmt die Fachanwendung. Die Übertragung erfolgt verschlüsselt per HTTPS bzw. SSL wofür vorher Zertifikate (von TC-TrustCenter ausgestellt) ausgetauscht werden. Die Authentifizierung erfolgt über den Namen der Benutzerin oder des Benutzers und das Passwort.

Für einen Bericht, dem Meldeprozess nach Basel II, ist die Process Support Map in Abbildung 20 dargestellt.

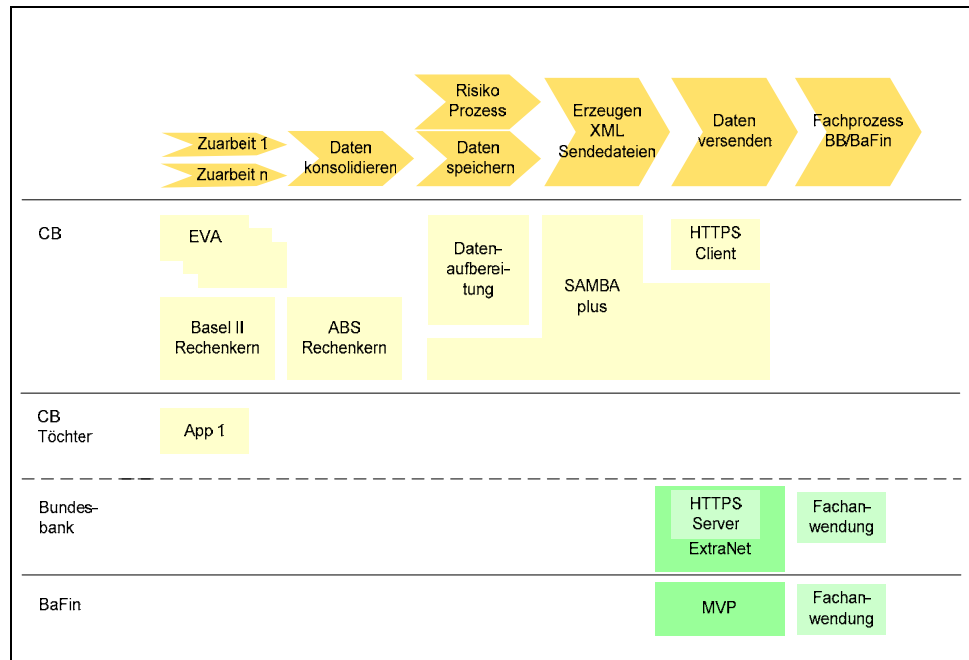


Abbildung 20: Best Practice PRK Meldeprozess Basel II (Process Support Map) (Quelle: Eigene Darstellung)

Best Practice PRK Kontenstammdatenbereitstellung

Es gibt eine gesetzlich vorgeschriebene Datenbereitstellung (Kontenstammdaten), die exemplarisch über die Bank-Verlag GmbH (Köln) realisiert wird (siehe Abbildung 21). Andere Institutsgruppen stellen dies entweder in Eigenregie bzw. über andere Serviceprovider zur Verfügung.

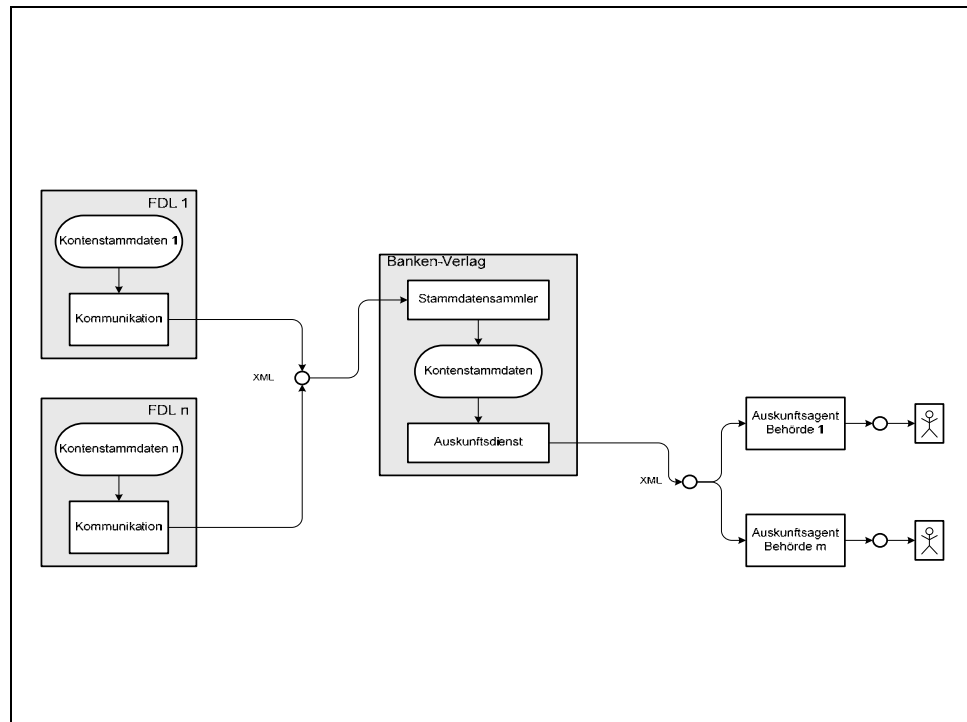


Abbildung 21: Best Practice Architektur Abruf Konteninformationen bei Bank-Verlag (FMC) (Quelle: Eigene Darstellung)

Hierbei handelt es sich um einen Self-Service, der von den Banken der BaFin zur Verfügung gestellt wird. Realisiert wird der Service dadurch, dass der Bankverlag den privaten Banken den Service zum Einstellen der Daten (Lesen, Bearbeiten) bereitstellt. Die BaFin hat ein privates Recherchetool, das auf den Bankverlag zugreift.

Die relevanten Informationen von Kundinnen und Kunden inkl. der Kontoreferenzdaten werden am Beispiel der privaten Banken z. B. von einem Dritten, dem Bank Verlag gesammelt, zusammengefasst und den Behörden über eine einzige Schnittstelle bereitgestellt.

Die zugehörige Process Support Map ist in Abbildung 22 zu sehen.

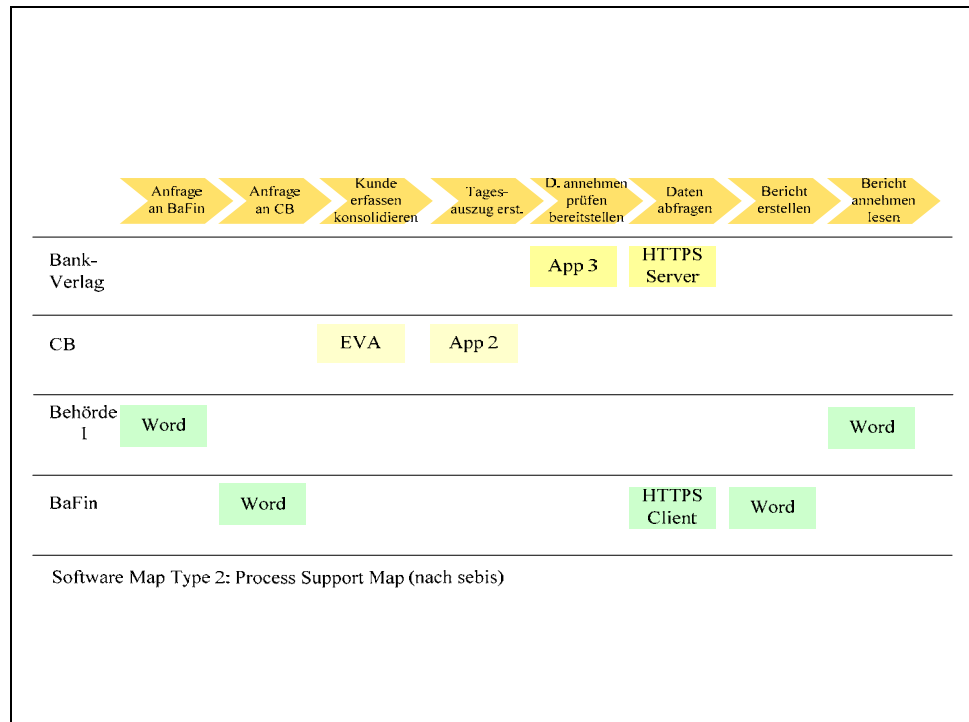


Abbildung 22: Best Practice PRK Abruf Konteninformationen (Process Support Map) (Quelle: Eigene Darstellung)

Beispielhafte Datenschnittstelle des Bundesbank Extranets (XML-Schemata)

Für den Datenaustausch mit der BB sind zweierlei Schemata definiert.

Das Basisschema BbkXmwBasis.xsd mit den folgenden komplexen Typen (in deutsch):

- adresse
- basisFeld
- basisLieferung
- basisMeldung
- terminMeldung

Und je Fachverfahren (Meldung) ein oder zwei weitere Schemata (Formular ähnlich) für:

- SolvV, LiqV, Monatsausweise
- Beteiligungsanzeigen
- Groß- und Millionenkredite
- Meldung zum Auslandskreditvolumen
- Bankenstatistik (Bilanzstatistik, Auslandsstatus der Banken (MFIs), Kreditnehmerstatistik)
- Depotstatistik
- EWU-Zinsstatistik
- Emissionsstatistik für festverzinsliche Wertpapiere
- Statistik über Investmentfonds
- Statistik über Investmentfonds

Resümee IST-Analyse zur IT-Architektur

Bereits jetzt werden für die Abarbeitung von Prozessketten zwischen FDL und Verwaltung IT-Komponenten eingesetzt. In der Regel handelt es sich um Level-3 Prozesse, die noch nicht durchgängig medienbruchfrei abgewickelt werden. Ein Großteil der ausgetauschten und übermittelten Dokumente werden noch als Papierdokumente zwischen den Beteiligten ausgetauscht.

Die Angebote der Bundesbank und der BaFin für den Austausch von Daten müssen als positiv hervorgehoben werden. Beide Behörden bieten bereits jetzt über ein Extranet / Portal Dienste für die Meldung von Daten der Banken und öffentlich definierte Datenschnittstellen XML-Schemata an und sind daher eine hervorragende Voraussetzung für die Weiterentwicklung der IT-Infrastruktur für Level-1 Prozessketten, die die im folgenden definierten Ziele erfüllen soll.

4 Ziele und Anforderungen für Prozessketten Level-1

4.1 Von Prozessketten Level-3 zu Level-1 (Systemebene)

Das **BMI** definiert **Prozessketten** nach "Level-3", "Level-2" und "Level-1" (BMI 2007: 3f.).

Level-3 (L-3) bedeutet, dass es "punktuelle Informationsverpflichtung und Verfahren mit einer Behörde gibt. Auf einer Wertschöpfungsstufe innerhalb eines Unternehmens erforderlicher punktueller Datenaustausch mit einer Behörde".

Level-2 (L-2) fokussiert auf eine "unternehmensweite Prozessintegration: Über mehrere Wertschöpfungsstufen eines Unternehmens laufende Prozesskette mit vielfältigen punktuellen Informationspflichten und Verfahren mit Behörden".

Level-1 (L-1) bedeutet "branchenweite Prozessintegration: Über mehrere Wertschöpfungsstufen einer Branche laufende Prozesskette mit vielfältigen punktuellen Informationspflichten und Verfahren mit Behörden".

Folgendes Schaubild zeigt dies im Überblick (siehe Abbildung 23).

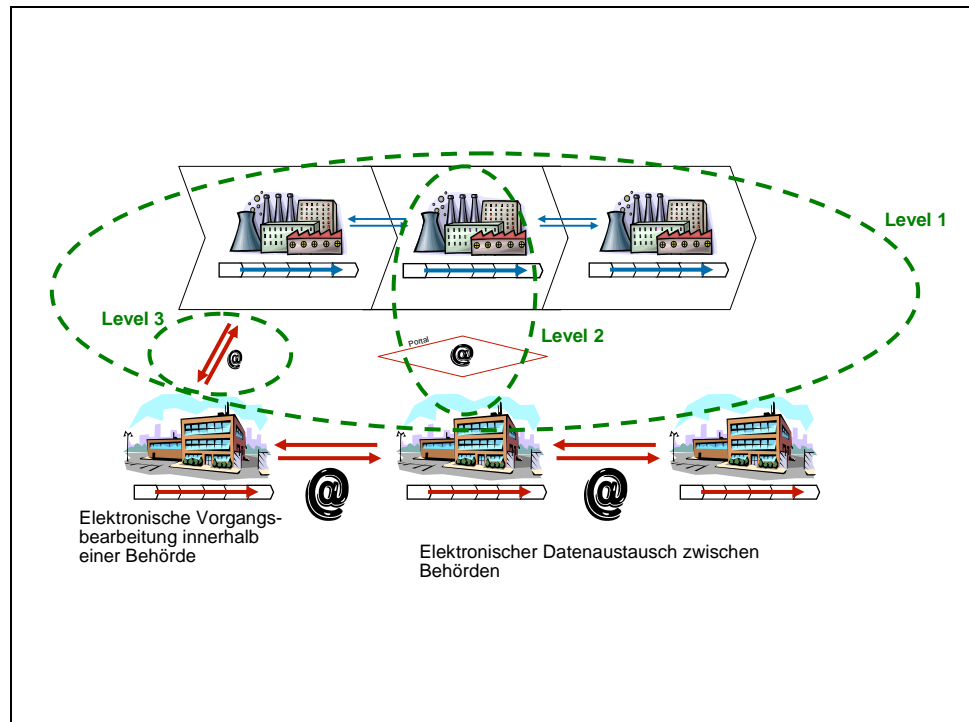


Abbildung 23: PRK Levels nach BMI (Quelle: BMI 2007: 4)

In einem Workshop der Wissenschaftlerinnen und Wissenschaftler aus den Prozessketten-Projekte Los 1 "Umwelt", Los 2 "Finanzdienstleistungen" und Los 3 "Informations- und Meldepflichten für Arbeitgeber" am 07.10.2008 im BMI, Berlin konnte auf Vorschlag der TU München folgende pragmatische **Operationalisierung für Prozessketten und ihren Level-Status** erarbeitet werden:

- Als **Level-3** kann bezeichnet werden, wenn ein Akteur auf Seite der Wirtschaft mit einem Prozessketten-Verfahren mit einem Akteur auf Seite der öffentlichen Verwaltung verbunden ist ("**1 : 1 : 1**").
- Als **Level-2** kann bezeichnet werden, wenn ein oder mehrere Akteure auf Seite der Wirtschaft mit einem oder mehreren Prozessketten-Verfahren mit einem oder mehreren Akteuren auf Seite der öffentlichen Verwaltung verbunden sind; dabei ist aber mindestens eine der genannten Anzahl von Akteuren oder Verfahren gleich 1, d. h. es kann noch nicht von einer branchenweiten oder branchenübergreifenden Prozesskette gesprochen werden ("**(2-x) : (2-x) : (2-x)**").

- Als **Level-1** kann bezeichnet werden, wenn mehrere Akteure auf Seite der Wirtschaft mit mehreren Prozessketten-Verfahren mit mehreren Akteuren auf Seite der öffentlichen Verwaltung verbunden sind; es kann von einer branchenweiten oder branchenübergreifenden Prozesskette gesprochen werden (" $(2+x) : (2+x) : (2+x)$ ").

Abbildung 24 zeigt die Operationalisierung von Level-3, Level-2 und Level-1 aufeinander aufbauend in schematischer Darstellung.

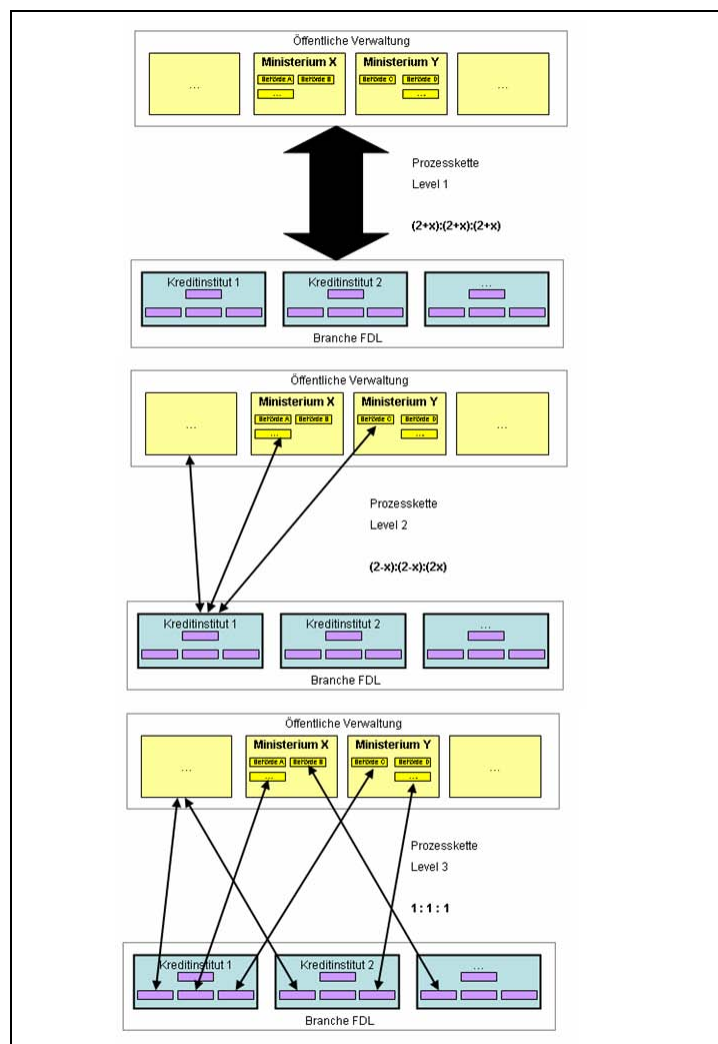


Abbildung 24: PRK Level Anhebung auf Systemebene (Quelle: Eigene Darstellung)

Übergreifendes Ziel ist es, eine **Levelanhebung von Prozessketten** von "Level-3" auf "Level-2" und auf "Level-1" zu erreichen, um die Realisierung von politischen Zielen (siehe Kap. 2.3) als auch zunehmende Skaleneffekte, abnehmende Grenzkosten und die Ausschöpfung von Win-Win-Situationen für Wirtschaft und Verwaltung zu ermöglichen.

Es sei an dieser Stelle darauf hingewiesen, dass Level-2 oder gar Level-1 Prozessketten-Angebote notwendige und nicht hinreichende Bedingung dafür sind, dass die Wirtschaft solche auch nachfragt und aktiv und nachhaltig nutzt.

Es ist also erforderlich, dass es eine **"Steckdose" zwischen öffentlicher Wirtschaft und Verwaltung** gibt, die besondere Eigenschaften hat, wie nachfolgendes Kapitel herleitet.

4.2 Entwicklung in Generationen – von der fehlenden Steckdose zwischen Wirtschaft und Verwaltung über viele unterschiedliche Steckdosen zu der einen Steckdose (Prozesskettenebene)

4.2.1 Das Bild der Steckdose: ...

Das **Bild der elektrischen Steckdose** begleitete das Autorenteam von Anbeginn des Projektes; selbsterklärend konnte es die nicht einfache Problematik von PRK zwischen Politik, Verwaltungen und Banken kommunizieren.

Es halfen dabei die bekannten Eigenschaften einer Steckdose (und der Infrastruktur dahinter), die analog auf Ziele und Anforderungen für PRK Level-1 in unterschiedlichen Dimensionen übertragen werden können.

Jede Steckdose hat eine räumliche Existenz und (idealerweise) einen leicht findbaren Zugang für den Stromstecker.

Jede Steckdose bietet in **wirtschaftlicher Dimension** eine Leistung an. Der Provider tarifiert gegenüber der Nutzerin oder dem Nutzer einen Preis für sein Gut und die Nutzerin oder der Nutzer kann (im liberalisierten Strommarkt) den Provider gemäß Preis und Leistung auswählen.

Jede Steckdose ist an Architekturen eingepasst. Es gibt in **infrastruktureller Dimension** unterschiedliche Arten von Steckdosen und Infrastrukturen (Gebäudeinstallationen, Spannungsnetze; Verteiler-, Aufputz-, Unterputz-, tragbare Verlängerungskabel-, Mehrfachsteckdosen; Buchsen, Stecker, Kupp-

lungen etc.), die aber alle dieselben grundsätzlichen Standards einhalten müssen.

Jede Steckdose hat in der **Dimension Sicherheit** viel zu leisten. Es bedarf Außen-, Neutral-, Schutzleiter etc., um Zertifizierungen, Empfehlungen und Normen einzuhalten (z. B. CE-Kennzeichnung, GS Geprüfte Sicherheit, nach dem Geräte- und Produktsicherheitsgesetz etc.).

Jede Steckdose und ihre Leistungen haben auch eine **rechtliche Dimension**, der Provider bietet sein Angebot zu unterschiedlichen vertraglichen und rechtsverbindlichen Konditionen an (AGB, SLA, Datenschutz etc.).

Jede Steckdose bietet Innovationspotenziale, an die zu Beginn ihrer Erfindung bzw. in der ersten Zeit ihres Einsatzes nicht gedacht wurde (z. B. Telefonie, Datendienste etc.).

Vor diesem Hintergrund kann das in Kap. 3.2 ausgeführte Ergebnis, dass es messbare PRK der Generation G1, G2 und G3 gibt, einfach graphisch dargestellt werden.

Es gibt PRK zwischen Wirtschaft und Verwaltung, die **keine (elektronische) Steckdose** haben (siehe Abbildung 25).

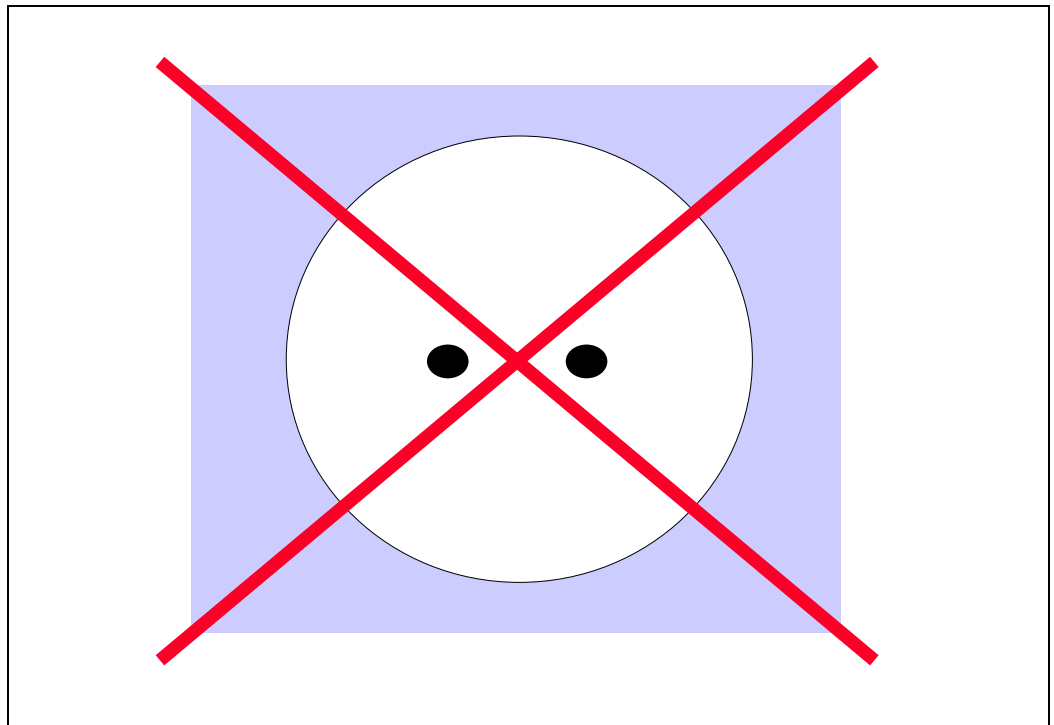


Abbildung 25: PRK der Generation G1 (Quelle: Eigene Darstellung)

Ein Beispiel für eine solche Prozesskette ist die Meldung für Verdachtsanzeigen bei Geldwäschestraftatbeständen. Bei einer Anzeige werden zur Zeit von den Banken Papierformulare ausgefüllt und diese nebst Anlagen (z. B. über getätigte Transaktionen) an das Bundeskriminalamt gefaxt. An einer elektronischen Steckdose beim BKA wird zur Zeit gearbeitet (siehe Kap. 8).

Weitere Beispiele hierfür sind die PRK "Errichtung grenzüberschreitenden Dienststellenverkehrs" (ID88) und die PRK "Überschreitung der Anlagebuch-Großkreditgesamtobergrenze" (ID64).

Es gibt des weiteren PRK zwischen Wirtschaft und Verwaltung, die auf **heterogenen und zum Großteil inkompatiblen Steckdosen** basieren (siehe Abbildung 26).

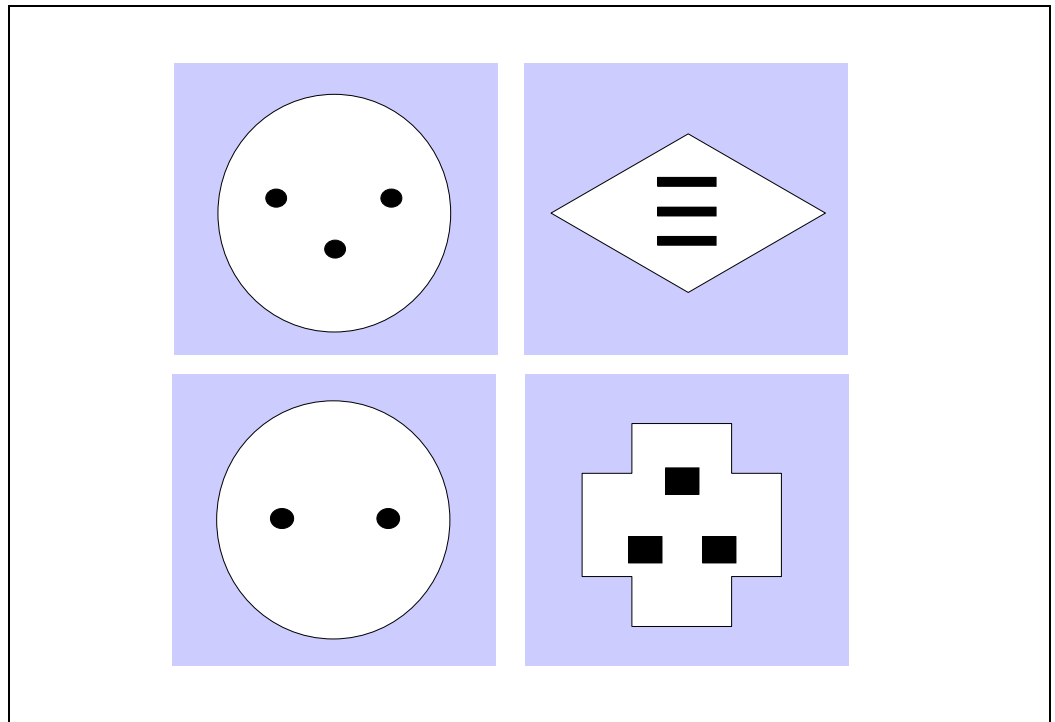


Abbildung 26: PRK der Generation G2 (Quelle: Eigene Darstellung)

Ein Beispiel sind die Portale der BaFin, Bundesbank oder des Bank-Verlags. Alle Portale bieten Dienste und Datenschema für den elektronischen Austausch von Informationen an. Die Dienste der einzelnen Portale sind untereinander aber noch nicht abgestimmt und basieren nicht auf einer gemeinsamen Infrastruktur und es werden auch noch keine Datenschema im Sinne XÖV wiederverwendet.

Weitere Beispiele hierfür sind die PRK "Arbeitgeberkündigung prüfen und durchführen" (ID12) und die PRK "Elektronische Übermittlung von Jahresabschlussdaten (Bilanzen)" (ID129).

Und es gibt PRK zwischen Wirtschaft und Verwaltung, **die Ziele und Anforderungen für PRK Level-1 erfüllen** und die zukünftige Entwicklung sicherstellen (siehe Abbildung 27).

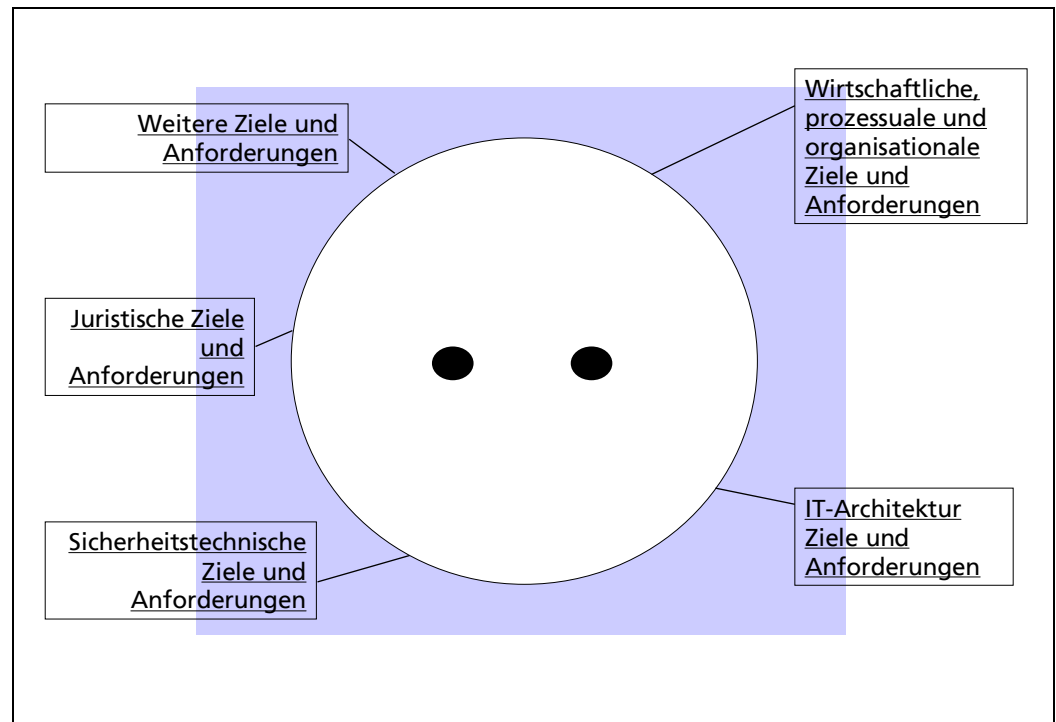


Abbildung 27: PRK der Generation G3 (Quelle: Eigene Darstellung)

Beispiele hierfür sind z. B. die PRK "Monatsausweise und weitere Angaben von Instituten an Deutsche Bundesbank" (ID119) und die PRK "Millionenkredite" (ID74).

Doch was sind die konkreten Ziele und Anforderungen für PRK Level-1, die nicht der Generation G1, nicht der Generation G2, sondern der Generation G3 entsprechen?

Für eine sinnvolle Planung, Steuerung und Kontrolle von Prozessketten ist die Definition und organisationsübergreifende Abstimmung von Zielen unerlässlich. Grundsätzlich stellen Ziele anzustrebende SOLL-Größen dar, welche eine handlungsleitende Funktion für Organisationen und Personen darstellen (Gabler 2000). Ziele dienen zur Präzisierung von Zukunftskonzeptionen von Prozessen und gleichzeitig als handlungsleitender Gestaltungsauf-

trag für die Prozessverantwortlichen sowie Mitarbeiter und Mitarbeiterinnen (Kunz 2003).

- Top-down Zielplanung:
Ableitung von Prozesskettenzielen aus den Organisationszielen und -strategien
- Bottom-up Zielplanung:
Ableitung der Prozesskettenziele erfolgt aus:
 - Problemanalysen, welche Auskünfte über Verbesserungspotenziale geben
 - Prozess-Benchmarkings, die Auskunft über Leistungen der eigenen Prozesskette im Vergleich mit Wettbewerbern oder "Best Practices" gibt
 - Zeitvergleiche, welche Auskünfte über die Leistungsentwicklung in der Vergangenheit geben
 - Kombination von Informationsquellen: Problemanalysen, Benchmarking und Zeitvergleiche.

Im Rahmen des Managements von Prozessketten stellt die Erarbeitung und Definition von Zielen einen wichtigen Bestandteil des Managementzyklus dar. Dabei gibt es zwei grundsätzliche Vorgehensweisen zur Festlegung von Zielen für Prozessketten (Schmelzer / Sesselmann 2003): Im folgenden hat das Autorenteam der Studie im Sinne eines geschlossenen Panels von Expertinnen und Experten Ziele und Anforderungen zusammengestellt und aufbereitet, die zum einen auf den Arbeiten und Erkenntnissen der Studie selbst, zum anderen auf einer Vielzahl von Erfahrungen aus Projekten, gutachterlicher Tätigkeit sowie Forschung und Lehre im Themenkreis E-Government und Finanzdienstleister beruhen.

4.2.2 wirtschaftlich, prozessual und organisatorisch, ...

Ziele

Für die Neugestaltung und Optimierung von Prozessketten sind die folgenden Ziele und Anforderungen ökonomischer Art geboten:

Prozesskosten minimieren [W1]

Hierbei handelt es sich um eine der klassischen Aufgabe der Ökonomie: Wie optimiere ich eine Zielgröße unter der Nebenbedingung knapper Güter und Produktionsfaktoren (Arbeit, Kapital und Boden, Humankapital)?

Die quantitative (monetäre) Betrachtung der Wirtschaftlichkeit ist zu unterscheiden in zwei Betrachtungsweisen:

- Beurteilung im Sinne einer Rentabilitäts- oder Amortisationsrechnung und
- Prozessorientierte Betrachtung.

Z. B. WiBe21 betreibt ersteres mit seinem kombinierten Ansatz aus Investitionskostenrechnung und Nutzwertanalyse, es werden vor allem Projekte betrachtet. Methoden, die eine Prozesskostenrechnung betreiben, sind z. B. das Standardkosten-Modell und der eGOV-Rechner (siehe 5.2 und Anhang II).

"Das SKM ist eine international anerkannte Methode zur Messung von bürokratischen Belastungen durch gesetzlich veranlasste Informationspflichten. Das sind alle Daten, die für Behörden oder Dritte zu beschaffen, verfügbar zu halten oder zu übermitteln sind... Der Zeitaufwand wird ermittelt, indem Betroffene befragt werden, wie lange sie für die Ausführung einzelner Arbeitsschritte benötigen, z. B. für das Beschaffen der notwendigen Formulare, das Durchführen von Berechnungen, das Aufsetzen von Schreiben. Diese Arbeitsschritte werden auch "Standardaktivitäten" genannt und geben dem Modell seinen Namen. Zur Errechnung des finanziellen Aufwands werden Gebühren und andere Kosten, z. B. für Porto und Versandmaterial, für Beratungsleistungen, oder für notwendige Anschaffungen erfragt und aufgenommen... Bei den Unternehmen wurden die Kosten des für die Erfüllung der Pflichten eingesetzten Personals und für weitere Anschaffungen in Euro ermittelt. Die so erfassten Zeiten und Kosten werden mit der Anzahl der Betroffenen in einem Jahr multipliziert. Dadurch wird der bürokratische Aufwand, den eine Informationspflicht in Deutschland verursacht, objektiv aufgezeigt. Die Ergebnisse machen die Größenordnung und Verteilung der bürokratischen Belastungen für die Öffentlichkeit deutlich."

www.destatis.de/jetspeed/portal/cms/Sites/destatis/Internet/DE/Content/Projekte/SKM/Methode,templateld=renderPrint.psmI

Der eGOV-Rechner vergleicht einen IST- mit einem SOLL-Prozess und misst den Transformationseffekt pro Prozess in Euro (www.egov-rechner.org).

Bürokratie abbauen [W2]

Die Bundesregierung erstattet dem Deutschen Bundestag gemäß § 7 des Gesetzes zur Einrichtung eines Nationalen Normenkontrollrates (NKR-Gesetz) jährlich einen Bericht über die Erfahrungen mit der angewandten Methodik zur standardisierten Bürokratiekostenmessung (s. o.), den Stand des Bürokratiekostenabbaus in den einzelnen Ministerien und die aktuelle Prognose, ob die von der Bundesregierung festgelegten Ziele innerhalb des angegebenen Zeitraums erreicht werden.

Der Nationale Normenkontrollrat (NKR) nimmt hiermit gemäß § 4 Abs. 3 NKR-Gesetz zu dem jährlichen Bericht der Bundesregierung Stellung zu der Frage, "inwieweit das von der Bundesregierung gesetzte Ziel erreicht worden ist" (www.normenkontrollrat.bund.de/nn_252070/Webs/NKR/Content/DE/Artikel/2008-12-10-presseerklaerung-nkr-nimmt-stellung-zum-bericht-der-bundesregierung.html).

Verwaltung modernisieren [W3]

Sowohl Banken als auch Verwaltungen stellt sich die Herausforderung, effizient und effektiv zu wirtschaften. Hierzu sind nicht zuletzt Innovationen der Katalysator.

Auf Seiten der öffentlichen Verwaltung ist durch E-Government ein Kulturwandel von der (ausschließlichen) Organisationsorientierung hin zur Prozessorientierung beobachtbar.¹¹ Prozesskettenorientierung wird die nächste große Innovations-Herausforderung.

Auch die Bankenseite "engineert" Innovationen systematisch wie nachfolgende Graphik zeigt (siehe Abbildung 28).

¹¹ einen Abriss gibt z. B. Kussmaul 2006: 117 ff.

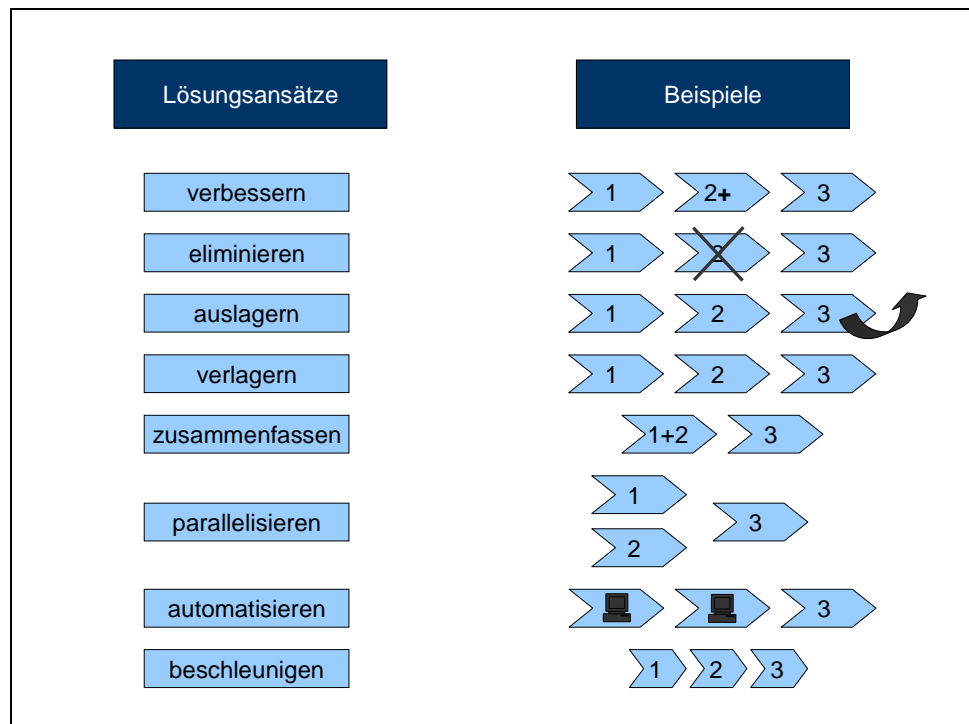


Abbildung 28: Prozessoptimierung durch Innovation (Quelle: Morrman / Hillesheimer / Metzler / Zahn 2006)

Innovation lässt sich z. T. systematisch programmieren über den Einsatz von TRIZ-Innovationstechniken wie Segmentierung, Extraktion, Lokale Optimierung, Asymmetrie, Kombination, Gegengewichte, Inversion, Dynamisierung, Geschwindigkeit, Rückkopplung, Selbstwartung, Kopieren, Virtualisieren, Einwegkomponenten, Verwerfen etc. erfolgen (siehe heise c't 23 / 2001: 96 ff. oder Krcmar 2003: 104 ff.).

Fallzahlen maximieren [W4]

Um vorhandene "Economies of Scale" (Skaleneffekte) nutzen zu können, ist eine möglichst hohen Fallzahl bezüglich der Nutzung der Prozessketten wünschenswert. Die Fallzahlen sind dabei die Anzahl der Nutzung der betreffenden Prozesskette in einem definierten Zeitraum. Verbunden mit der Erhöhung der Fallzahlen ist eine Reduzierung der Durchlaufzeit der Prozesskette notwendig, falls die Rahmenbedingungen konstant bleiben.

In Bezug auf die Prozessketten als elektronische Steckdose zwischen Wirtschaft und Verwaltung heißt dass, dass das Angebot (wenn es keine gesetz-

lichen Zwang mit "online verpflichtend" gibt) nicht gleich der Nachfrage sein muss.

Eine neue umgesetzte und angebotene Level-1 kann schwach, mittel oder stark genutzt werden und im Strukturwandel neue "Kunden" anziehen oder bestehende Fallzahlen des nicht-elektronischen Verfahrens substituieren.

Von der Zielsetzung her können Fallzahlen vor allem durch die Maßnahmen der gesetzlichen Auflage (s. o.) oder durch differierende Service Levels bzw. sogar Preisdifferenzierung (verursacherkostengerechte Gebühren) angereizt und maximiert werden.

Qualität, Reifegrad und Exzellenz von Prozessketten erhöhen [W5]

Die Qualität von Prozessketten kann anhand von quantitativ messbaren Indikatoren, sowie von qualitativen Indikatoren bestimmt werden.

Quantitative Indikatoren können dabei mittelbar oder unmittelbar gemessen werden (z. B. die Quote der Einhaltung vereinbarter Service Levels, die Anzahl fehlerfreier Durchläufe der Prozesskette etc.). Dagegen lassen sich qualitative Indikatoren nur mittelbar erheben (z. B. die wahrgenommene Servicequalität anhand von Kundenbefragungen etc.). Die Qualität spielt insbesondere an der direkten Kundenschnittstelle der Prozesskette eine sehr große Rolle.

Existenz eines Geschäfts- / Betreibermodells [W6]

Tragfähige und nachhaltige Betreibermodelle sind vor allem für Prozessketten der Klasse I und III von besonders großer Bedeutung (siehe Kap. 3.1).

Entscheidend ist, wer finanziell, wirtschaftlich, technologisch, rechtlich etc. verantwortlich zeichnet für den Betrieb des Geschäftsmodells der PRK.

In der älteren E-Government Debatte wurden diese Modelle oft als Public-Private-Partnerships (PPP), in der neueren Debatte als Shared Service Center (SSC) thematisiert.

4.2.3 IT-architektonisch, ...

Ziele

Für die Zukunftssicherheit der IT-Architekturen und IT-Infrastrukturen für Level-1 Prozessketten sind folgende Ziele anzustreben:

- **Realisierung eines hohen Grades an IT-Unterstützung [IT 1]**

Ein hoher Grad an IT-Unterstützung verspricht für viele Prozesse eine Verbesserung der Effektivität und damit auch eine schnellere Abwicklung und eine Kostenreduktion.

- **Orientierung der technischen Dienste an den Geschäftsprozessen [IT 2]**

Nur wenn die unterstützenden Dienste im Kontext der Geschäftsprozesse, ihren Schritten und auf deren Abstraktionsebene konzipiert sind, besteht die Möglichkeit die Prozesse und die IT-Anwendungen evolutionär zu verändern. Wenn die obersten IT-Komponenten und Dienste nur technisch nach implementatorischen Gesichtspunkten zugeschnitten sind, werden in der Regel Prozessänderungen tiefere technische Änderungen erfordern.

- **Kompatibilität der IT-Anwendungen optimieren [IT 3]**

Das Zusammenspiel nicht kompatibler Anwendungen setzt immer zusätzliche Transformatoren voraus. Wo diese fehlen, ist keine Zusammenarbeit möglich. Jede Inkompatibilität reduziert das Verständnis der Vorgänge und der Bedeutung der auszutauschenden Daten zwischen den Partnern und kann zu Missverständnissen führen. Jede zusätzliche Transformation reduziert die zu erzielende Effektivität.

- **Kompatibilität zum SAGA-Standard (Bundesverwaltung) ausbauen [IT 4]**

Dieser Standard gilt zwar nur für die Bundesverwaltung, er bietet aber auch allen anderen Parteien, besonders wenn sie mit der Bundesverwaltung zusammenarbeiten wollen, eine gute Vorlage für die zu entwickelnde IT-Infrastruktur.

- **Nutzung offener Standards ausweiten [IT 5]**

Eine grundlegende Forderung auch in SAGA ist die Forderung der Verwendung offener Standards und von Lösungen, für die die Gewährung von Li-

zenzen sicher ist, um Abhängigkeiten und Gefahren proprietärer Lösungen zu vermeiden.

Allgemeine fachliche und gesetzliche Anforderungen an IT-Anwendungen, die für alle Anwendungen der FDL oder der Verwaltung gelten, wie unter anderem die Revisionssicherheit im Backend behalten selbstverständlich neben den Zielen ihre Gültigkeit, dienen aber nicht primär der Beurteilung der Zukunftssicherheit der Architektur. Dies gilt auch für die die Gewährleistung der Barrierefreiheit der Benutzungsschnittstellen. Seit dem 31. Dezember 2005 ist die Barrierefreie Informationstechnik-Verordnung (BITV) für alle Webangebote des Bundes verbindlich. Dieses auf der Grundlage der WAI-Richtlinien (Web Accessibility Initiative) des World Wide Web Consortiums entwickelte Regelwerk formuliert Anforderungen und Bedingungen, die in der Entwicklung von E-Government-Anwendungen von Beginn an berücksichtigt werden sollten. Dazu zählen einfache Bedienung, Konsistenz in Layout und Navigation, Übersichtlichkeit, Gliederung der Inhalte nach möglichen Nutzerfragen, Erwartungskonformität und Verständlichkeit der Inhalte.

Allgemeine zukünftige IT-Architektur für Prozessketten

Doch wie stellt sich der Weg zu Level-1 Prozessketten im Hinblick auf Architekturen in der Praxis dar? Die IST-Situation ist durch den Übergang von der Generation 1 zur Generation 2 gekennzeichnet, dass immer mehr Behörden untereinander bzw. mit externen Parteien eine elektronische Vernetzung (Kommunikation, Nutzung von Services) eingehen. Dabei werden zur Zeit die verschiedensten Nutzerverwaltungen und Sicherheitskonzepte verwendet, die eine komfortable Erweiterung und Anhebung auf Level-1 behindern. Darum wird im folgendem ein Architekturmuster für alle Fallbeispiele und für alle Übergabepunkte (d. h. Schnittstellen zwischen den Partnern) skizziert, das diese Hindernisse reduziert.

Es wäre sinnvoll, für die Konstruktion von Prozessketten Level-1 und das Erreichen der herausgearbeiteten Ziele, eine standardisiert einheitliche Infrastruktur zu schaffen, die flexibel erweiterbar ist, die föderalen Strukturen der politischen und Verwaltungslandschaft widerspiegelt und in Richtung der Sicherheitsanforderungen skalierbar ist. Alle Partner (FDL und Behörden) müssen die Verantwortung über ihre IT behalten und diese unabhängig entwickeln können. Es sollte auch keine weitere zentrale Institution geschaffen werden. Eine ähnliche Aufgabe wurde zum Beispiel mit der elektronischen Fallakte (eFA) gelöst (www.fallakte.de). Anforderungen, Standards und Lösungsansätze für eine europäische Infrastruktur finden sich in der "European Interoperability Framework" (EIF) (IDABC 2004) und den zugehörigen "Architecture Guidelines". Analog wird im Umfeld der Realisierung der EU Dienstleistungsrichtlinie (Deutschland-Online 2008) im Projekt SAFE

(Deutschland-Online 2007) und (Deutschland-Online 2008a) der Vorschlag gemacht ausgehend von der bereits bestehenden Infrastruktur des Elektronischen Gerichts- und Verwaltungspostfachs (EGVP) (www.egvp.de) durch Flexibilisierung und Erweiterung die geforderte Infrastruktur zu schaffen.

Die Architektur ist in der Abbildung 29 zu sehen.

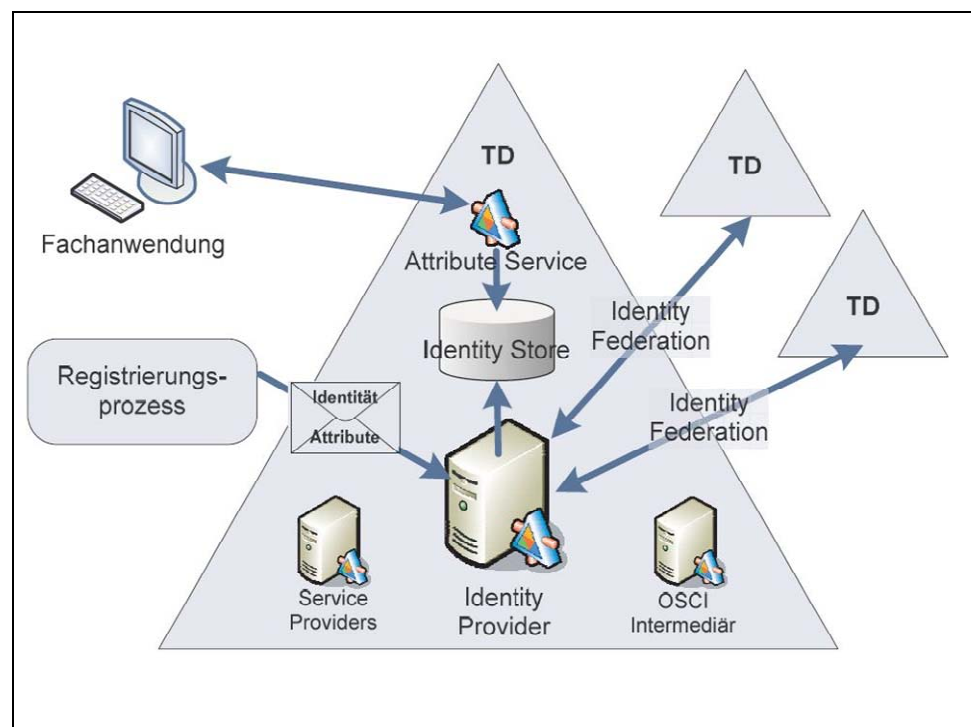


Abbildung 29: Allgemeine Architektur von Trust-Domains (Quelle: SAFE 2007: 18)

Jede oder fast jede größere Institution bildet eine Trust Domain. In jedem Trust Domain muss vorhanden sein ein Identity Provider mit einem Attribut Service und einer Registrierungskomponente und kann vorhanden sein ein Service Provider oder ein OSCI Intermediär (Online Services Computer Interface (OSCI) (www.osci.de)). Die Fachanwendungen und besonders alle neu geschaffenen Webservices nutzen den Attribut Service zur Authentifizierung / Autorisierung.

Die wichtigsten Überlegungen sind:

- Durch Schaffung mehrerer Trust-Domains (TD) nach gleichem Standard die Verwaltung und Implementierung der Infrastruktur zu dezentralisieren

und trotzdem Interoperation zuzulassen. Den Kern bildet das Föderierte Identity-Management und ein zentraler Meta-Attribut-Service.

- Durch den Verzicht auf die Notwendigkeit des OSCI Intermediär leichtgewichtiger und schnell zu realisierende Services zu schaffen.
- Durch unterschiedliche Level des Registrierungsprozesses und der Anforderungen der Services eine breite Palette von Sicherheitsabstufungen zu ermöglichen.

Das Föderierte Identity-Management wird dadurch gebildet, dass die IDP der verschiedenen TD einander vertrauen. Eine autorisierte Identität eines TD bekommt vom IDP eines vertrauten zweiten TD die notwendige Autorisierung für die Nutzung eines Service des zweiten TD (siehe Abbildung 30).

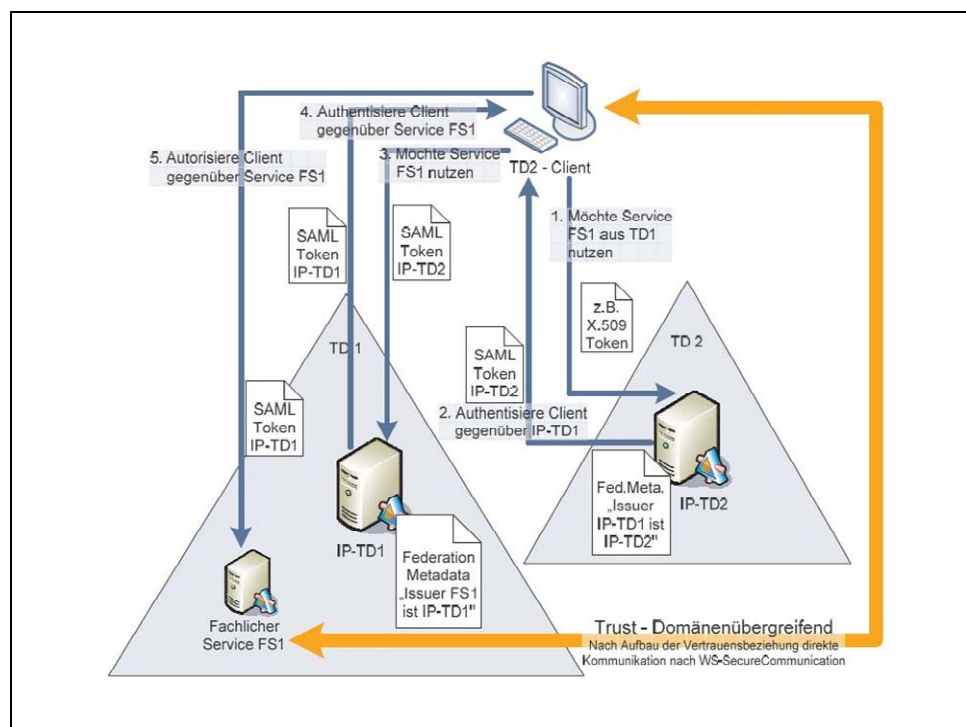


Abbildung 30: Tokenvermittlung im System SAFE (Quelle: SAFE 2007: 30)

Die Architektur benutzt für die Realisierung der Sicherheitsanforderungen u. a. die Standards: WS-Trust, WS-Federation, WS-Policy, WS-SecurityPolicy; SAML-Assertions, SPML 2.0, SPMLv2 XSD Profile, XPath.

Die Architektur der Standards ist in Abbildung 31 dargestellt.

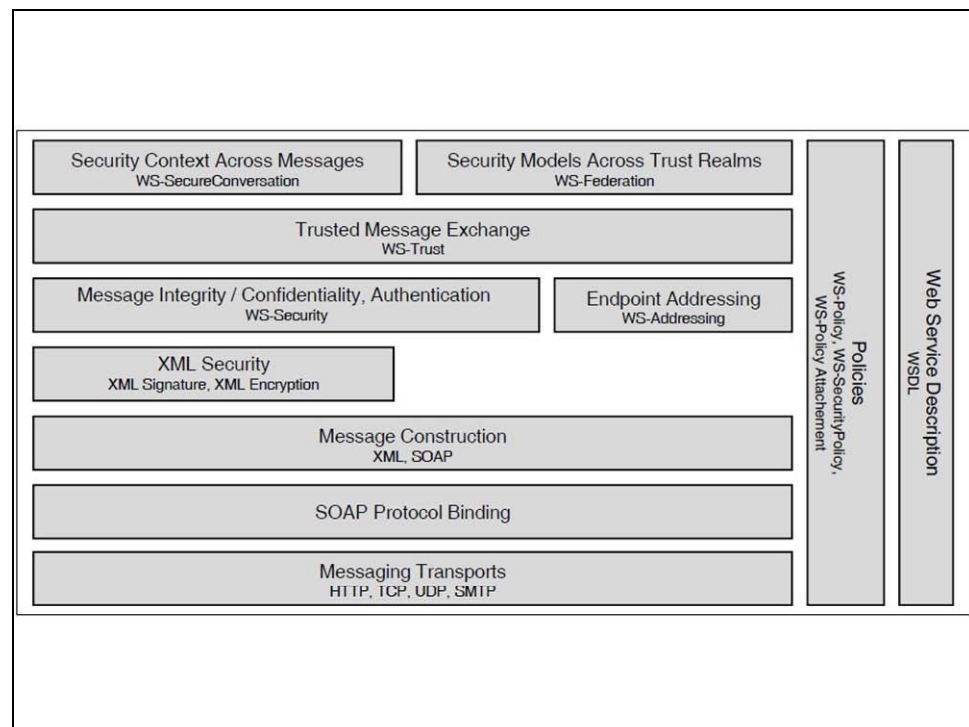


Abbildung 31: Architektur der Standards für sichere Webservices (Quelle: Kulisch 2007)

Diese Architektur hat den Vorteil, dass sich eine Bürgerin oder ein Bürger ohne große IT-Infrastruktur z. B. bei einem Bürgeramt für einen nahen IDP registrieren lassen kann und dann einfache Dienste über Web Portale nutzen kann, z. B. ein modifizierter Kanal 1 der eVA.

Große FDL haben bereits solche Komponenten wie Identity Provider (IDP) und Attribute Service (AS) in Betrieb. Nur kann es sein, dass sie nicht die geforderten Schnittstellen bereitstellen. Wenn neue Services eingeführt werden sollen, wie z. B. eVA, so müssen generell Anpassungsarbeiten vorgenommen werden, eine Standardisierung würde langfristig den Aufwand reduzieren. In der Regel wird es ausreichen eine dem Standard entsprechende Fassade vor die bestehenden Anwendungen zu setzen und das bestehende System weitgehend unberührt zu lassen.

Nachdem einmal die föderierte Infrastruktur geschaffen ist und die Vertrauensverhältnisse zwischen den Parteien eingerichtet sind, verwaltete jede Partei zum einen ihre eigenen Nutzerinnen und Nutzer, zum anderen Servi-

ces, Attribute und Security Policies. D. h. sie werden dort verwaltet wo die Informationen anfallen und können somit immer aktuell und vollständig sein.

Ein Erfolgskriterium für die Umsetzung dieser föderierten und interoperablen IT-Infrastrukturen und -Anwendungen, wie bereits in Kap. 2.3 ausgeführt, ist die Nutzung von Standards. Die Nutzung des SAGA-Standards stellt daher eine wesentliche Anforderung für die Umsetzung der IT-Architekturen von Prozessketten dar. Dieses gilt ebenso für die XÖV-Strategie des Bundes und ähnlichen Initiativen der Finanzwirtschaft. So erhält der SAGA-Standard auch Empfehlungen für den Aufbau Service-Orientierter-Architekturen. Dieses Vorgehen garantiert, dass die Komplexität von Level-1 Prozessketten aus Sicht der Anforderungen an eine sichere IT-Infrastruktur bewältigt werden kann.

Oberstes Ziel aus Architektur-Sicht ist daher zukünftig die Orchestrierung von Level-1 Prozessketten aus Diensten, die von den an der Prozesskette beteiligten Banken und Behörden als Webservices mit standardisierten Schnittstellen und Datenschemata – wie aus der Steckdose – bereitgestellt werden.

4.2.4 sicherheitstechnisch und...

Ziele

FDL-Prozessketten nutzen in der Regel das Internet als Transportmedium und müssen daher gegen die spezifischen und bekannten Sicherheitsprobleme dieses Kommunikationsnetzes wie Hacking, Spoofing oder Verfügbarkeitsangriffe geschützt werden. Dies erfordert einen kontinuierlichen und effektiven Informationssicherheitsprozess.

Dazu bietet die IT-Grundschutz-Vorgehensweise (BSI-Standard 100-2) zusammen mit den IT-Grundschutzkatalogen eine Basis für die Methodik zur Gewährleistung von Informationssicherheit (www.bsi.de/gshb/deutsch/baust/01004.htm) (siehe Abbildung 32).

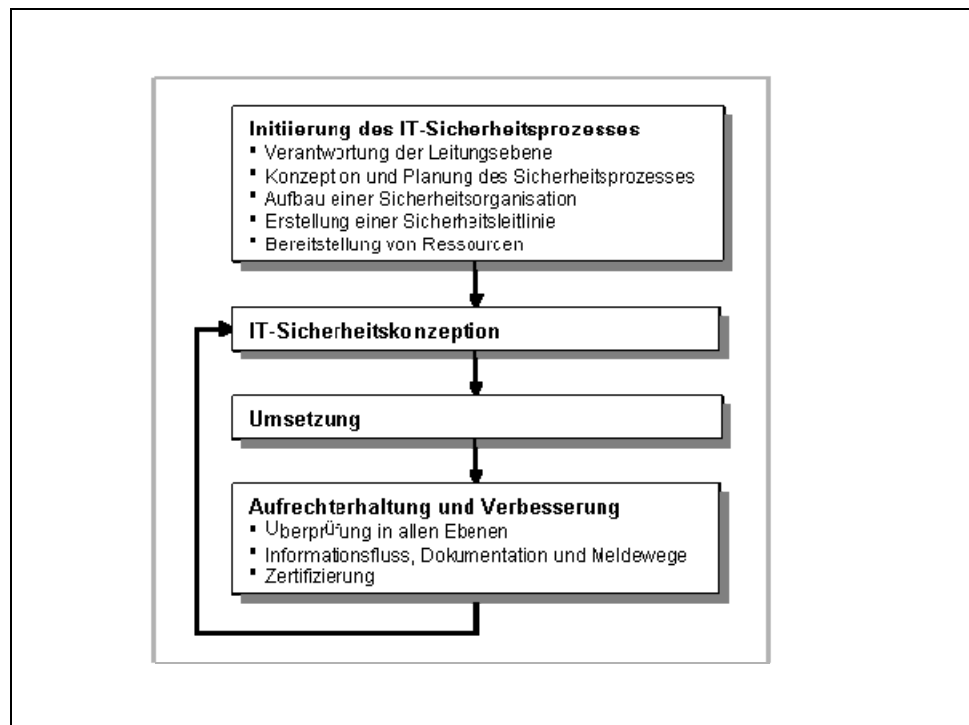


Abbildung 32: Phasen des IT-Sicherheitsprozesses (Quelle: BSI 2008b)

Die Abbildung zum IT-Sicherheitsprozess beschreibt die einzelnen zugehörigen Schritte und den Zyklus zur Aufrechterhaltung sowie Verbesserung der Informationssicherheit.

Die in fünf Schichten strukturierten IT-Grundschutz-Bausteine bilden die technische Grundlage des IT-Sicherheitsprozesses. Sie behandeln typische und für Informationssicherheit wesentliche organisatorische Aspekte, infrastrukturelle Gegebenheiten, Anwendungen oder technische Systeme und enthalten Verweise auf die in Sicherheitskonzepten zu berücksichtigenden Gefährdungen und die anzuwendenden Schutzmaßnahmen.

Die referenzierten Gefährdungen und Maßnahmen sind wiederum in eigenen Katalogen, den Gefährdungs- und Maßnahmenkatalogen, detailliert beschrieben (siehe Abbildung 33).

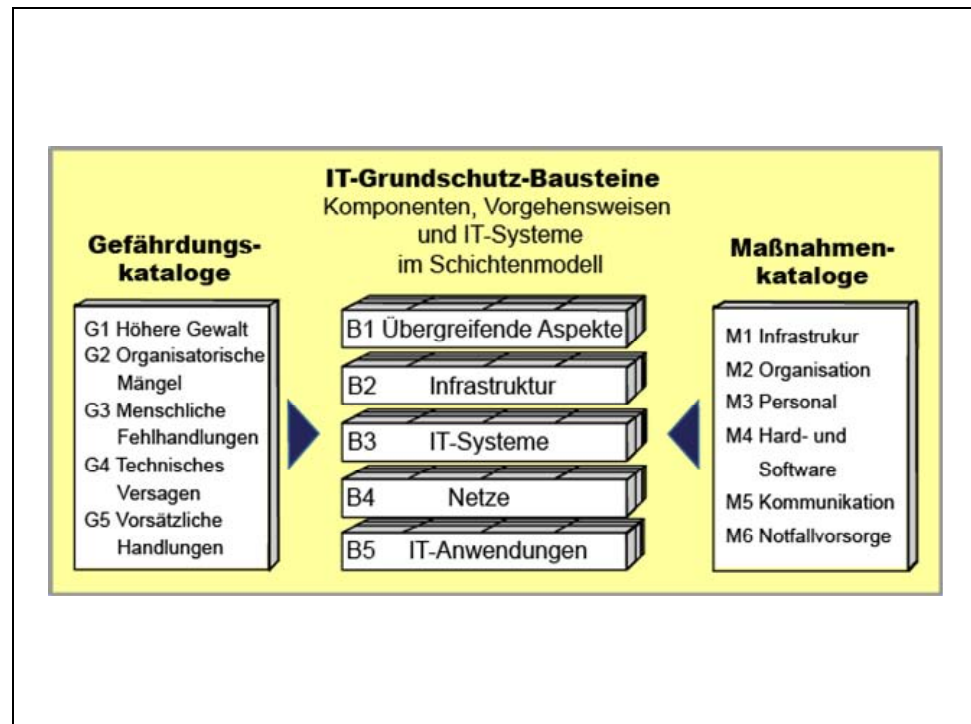


Abbildung 33: Die IT-Grundschutz-Kataloge mit dem Schichtenmodell (Quelle: BSI 2008b)

Für die Gestaltung von Level-1 Prozessketten zwischen Wirtschaft und Verwaltung gibt es unabdingbare Zielsetzungen – gemäß der Anwendung von BSI-Standard 100-2, gemäß der Umsetzung von IT-Grundschutz-Maßnahmen und gemäß erforderlicher zusätzlicher Sicherheitsvorkehrungen:

- **Die Vertraulichkeit der gespeicherten und übertragenen Informationen ist zu gewährleisten und die relevanten datenschutzrechtlichen Rahmenbedingungen müssen eingehalten werden. [S 1]**
- **Die Integrität der verarbeiteten, übertragenen und gespeicherten Informationen muss gewahrt bleiben und Fälschungen müssen leicht nachgewiesen werden können. [S 2]**
- **Die Verfügbarkeit der Informationen, Anwendungen und Systeme ist zu maximieren. [S 3]**

- **Authentizität, Nachweisbarkeit und Nicht-Abstreitbarkeit von Handlungen und Akteuren soweit erforderlich mittels elektronischer Signaturen werden unterstützt. [S 4]**
- **Ein hoher Grad an Vertrauenswürdigkeit in die Prozesskette wird realisiert (durch IT-Grundschutz-Zertifizierung). [S 5]**
- **Der Aufwand für Informationssicherheit ist zu adressieren und muss dem unterschiedlichen Schutzbedarf der Teilprozesse einer Kette gerecht werden. [S 6]**

4.2.5 juristisch

Ziele

Aus juristischer Perspektive schlagen wir folgende Zielsetzungen für rechtssichere Prozessketten vor.

Datenschutz [R 1]

Die vorhandenen Normen reichen zur Absicherung eines effektiven Datenschutzes aus. Es ist darauf hinzuwirken, dass alle Beteiligten datenschutzrechtliche Bestimmungen einhalten. Das Verbot jeglicher Vorratshaltung von personenbezogenen Daten ist zu beachten. Die Beteiligten haben personenbezogene Daten zu löschen, die nicht mehr zur "Zweckbestimmung eines Vertragsverhältnisses oder vertragsähnlichen Vertrauensverhältnisses" (§ 28 Abs. 3 Nr. 4 BDSG) notwendig sind.

Die qualifizierte elektronische Signatur ist das A und O jedes datenschutzrechtlich korrekten Informationsaustausches.

Elektronische Signatur [R 2]

Die elektronische Signatur des Antragstellenden, des Übermittelnden bzw. des Abrufenden kann eingesetzt werden. Dringend erforderlich ist neben dem bereits beschlossenen elektronischen Personalausweis die bundesweite Einführung einer qualifizierten elektronischen Signatur des Datenübermittelnden bzw. -Abrufenden. Beides ist für die Rechtssicherheit absolut notwendig.

Verschärfung des BDSG [R 3]

Prozessketten und ihre rechtssichere Umsetzung ist in Bezug auf etwaige Verschärfung des BDSG (Strafe statt Ordnungswidrigkeit) zu antizipieren. Die Strafdrohung statt Ordnungswidrigkeit bewirkt bei der Verwenderin oder dem Verwender personenbezogener Daten eine höhere Sorgfalt.

EU-Recht-Konformität [R 4]

Im Rahmen der Themenkomplexe ist die EU-Recht Konformität sicherzustellen. Erstrebenswert ist europaweite Harmonisierung des elektronischen Personalausweises; sie dient ebenfalls der Rechtssicherheit.

EU-Harmonisierung [R 5]

Dies gilt auch für die Notwendigkeit der Harmonisierung bei Verträgen innerhalb der EU, z. B. Richtlinie 2008 / 48 / EG des Europäischen Parlaments und des Rates vom 23. April 2008 über Verbraucherkreditverträge und zur Aufhebung der Richtlinie 87 / 102 / EWG des Rates.

Die Umsetzung des Gesetzentwurfes der Bundesregierung "Entwurf eines Gesetzes zur Umsetzung der Verbraucherkreditrichtlinie, des zivilrechtlichen Teils der Zahlungsdiensterichtlinie sowie zur Neuordnung der Vorschriften über das Widerrufs- und Rückgaberecht" vom 05.11.2008 ist im Hinblick auf die neue Fassung des § 492 BGB unbedingt erforderlich. Mit Inkrafttreten des Gesetzentwurfes wird der Vertragsschluss auf elektronischem Weg möglich, da der aktuell gültige § 492 BGB Absatz 1 Satz 2 "Der Abschluss des Vertrags in elektronischer Form ist ausgeschlossen." gestrichen wird. Somit wird der Vertragsschluss durch elektronische Signatur möglich.

Recht der Informationellen Selbstbestimmung [R 6]

Prozessketten und ihre rechtssichere Umsetzung ist in Bezug auf die Verankerung von IT im Grundgesetz zu antizipieren.

Das Recht der Informationellen Selbstbestimmung ist (neben dem Leben) eines der höchst einzustufenden Güter. Es wurde vom Bundesverfassungsgericht (15.12.1983, Az. 1 BvR 209/83) als Grundrecht anerkannt.

Ob und wann der ePA kommt, hat im Querschnitt tiefgreifende Implikationen auf fast alle der genannten Ziele, was an dieser Stelle zu diskutieren ist.

Elektronischer Personalausweis (ePA)

Die am 1. September 2006 in Kraft getretene Föderalisierungsreform hat die Gesetzgebungskompetenz für das Ausweiswesen gem. Art. 73 Abs. 1 GG auf den Bund übertragen. Das Bundeskabinett hat dazu am 23. Juli 2008 dem Entwurf des Gesetzes über Personalausweise (**Entw-ePA**) und dem elektronischen Identitätsnachweis sowie der Änderung weiterer Vorschriften (sind hier nicht besonders aufgeführt) zugestimmt. Tangiert war auch die konkurrierende Gesetzgebung aus dem Recht der Wirtschaft (Art. 74 Abs. 1 Nr. 11 GG). Diese nimmt der Bund zur Wahrung einer einheitlichen Infrastruktur beim elektronischen Identitätsnachweis gegenüber der Wirtschaft (Handel, Banken, Versicherungen) in Anspruch. Als rechtliche Vorschriften genannt sind das **BDSG** idF. v. 14.01.2003, zuletzt geändert 22.08.2006 und das **StGB** idF. v. 13.11.1998, zuletzt geändert 31.10.2008.

Der ePA soll zum 1. November 2010 eingeführt werden.

Aufbau des ePA

Mit ePA ist der elektronische PersonalAusweis gemeint. Er ist eine scheckkartengroße Plastikkarte (wie z. B. Führerschein, Krankenkassenausweis, EC-Karte, etc.) mit einem integrierten Chip, auf den Daten gespeichert werden können. Lichtbild und die persönlichen Daten sind aufgedruckt und gleichfalls auf dem Chip gespeichert. Zudem können auf Wunsch Fingerabdrücke bzw. auch eine digitale Signatur (Identitätssicherung wie bei persönlich vollzogener Unterschrift) gespeichert werden.

Ausweispflichtig sind Deutsche nach Art. 116 Abs. 1 GG und Personen, die sich überwiegend in Deutschland aufhalten, nicht aber Kinder unter 16 Jahren (siehe § 1 Abs. 1 Entw-ePA, jedoch ab dem 10. Lebensjahr auf Antrag möglich). Neu eingeführt ist die Zuständigkeit von Personalausweisbehörden im Ausland (§ 7 Abs. 2 Entw-ePA) bei den Auslandsvertretungen. Der ePA ist insoweit moderner als der Reisepass, der ja immer noch in Papierformat besteht, entweder nur visuell lesbar ist, bzw. einer anderen Lesevorrichtung bedarf. Der ePA ist als Passersatz innerhalb der EU und der EWR-Mitgliedsstaaten zugelassen (Richtlinie 2004/38/EG v. 29.04.2004). Er gilt also im Schengenraum (EU-Staaten mit Ausnahmen Großbritannien, Irland, Zypern, zuzüglich Island und Norwegen).

Eines der obersten (Fern-)Ziele muss die Entlastung der Bürgerinnen und Bürger sein ("Ein Bürger, ein Ausweis"). Abzuleitende Bestrebungen sind begrüßenswert: die Entlastung der Bürgerinnen und Bürger durch Bürgerportale, die Entlastung der Wirtschaft vor unnötigen bürokratischen Pflichten,

der Wegfall konkret anzusprechender Behörde bzw. Dienststellen etc. (siehe 3. IT Gipfel, Darmstadt, 20.11.2008).

Pilotprojekte (z. B. Technische Universität Darmstadt) zum praktischen Einsatz der Ausweiskarten sind aufgenommen.

Vorteile und Gefahren

Die Vorteile des ePA sind insbesondere:

- Sichere Personenidentifikation
- Verlässliches E-Government, Bürgerportal, automatische Zuordnung der Verwaltungsvorgänge
- Sicheres E-Business
- Verbesserter Jugendschutz
- Vorgangsbeschleunigung durch elektronisches Lesen der Identität, keine Übertragungsfehler
- Einfaches und sicheres Austauschen elektronischer Nachrichten zwischen Verwaltung und Dritten
- Schaffung eines Datensafes, z. B. zur Hinterlegung elektronischer Dokumente

Weiter soll ab 2010 die De-Mail-Nutzung Anwendung finden. De-Mails sind elektronische Nachrichten zwischen Internetnutzern auf hohem Niveau. Die Online-Kommunikation soll so vertraulich und verbindlich werden wie die Papierpost und dabei so einfach sein wie eine E-Mail. Die höchste Sicherheitsstufe erfordert dabei die Daten des ePA. In Friedrichshafen soll die Pilotstudie laufen.

Die Einführung des ePA verursacht einmalige und laufende Kosten. In der Vorbemerkung zum Entw-ePA des BMI vom 28.07.2008 werden die Investitionskosten für Entwicklung und Integration der erforderlichen Fachanwendungen in den Jahren 2009 bis 2011 auf 1,71 Mio. Euro sowie die laufenden Kosten für den Betrieb ab 2010 auf 240.000 Euro geschätzt. Für Aufbau und Betrieb der Server und Netze werden im Zeitraum 2009 bis 2011 ca. 4,02 Mio. Euro veranschlagt, ab 2012 laufende Kosten vom ca. 795.000 Euro je Jahr. Ein zusätzlicher Personalbedarf wird auf ca. 35,5 Stellen geschätzt. Diesen Kosten stehen noch festzulegende Gebühreneinnahmen gegenüber.

Die Kosten bei den Auslandsvertretungen sind derzeit nicht bezifferbar. Bei der Zollverwaltung werden Kosten von ca. 2,02 Mio. Euro für die Erstaussstattung mit Lesegeräten angenommen.

Den Kosten müssen die Vorteile gegenüber gestellt werden. Allein für die Wirtschaft wird durch möglichen Bürokratieabbau eine Entlastung von 123,29 Mio. Euro genannt (z. B. durch ein IT-Verfahren unter Verwendung des ePA bei der Geldwäsche). Die Einsparung bei der elektronischen Kreditvergabe könnte sich in gleichem Bereich (wenn nicht sogar höher) bewegen.

ePA: Schlüssel in die IT

Der ePA macht die Verwaltungsvorgänge in Ländern und Gemeinden, aber auch beim Bund transparenter, effektiver und auch kostengünstiger. Mit dem ePA ergeben sich neue Synergien in Richtung "schlanker Verwaltung".

Der ePA bringt im Privatbereich und im Verhältnis zum Staat, also innerhalb der Beteiligten zueinander viele Vorteile und Kostensparpotenziale. Im E-Business schafft der Staat einen Vorteil, der bei richtiger Integration viele Mio. Euro bei Privaten (z. B. Banken etc.) freisetzt. Daneben wird die "barrierefreie Informationstechnik" behinderten Menschen helfen, mittels geeigneter Programmoberflächen in der IT-Technik ihre Behinderung auszugleichen; § 2 BITV, Verordnung des BMI v. 27.04.2002, BGBl I S. 1467).

Der ePA ist zukunftsweisend.

4.3 "PRK-Scoping"

4.3.1 Generische Vorgehensweise "PRK-Scoping"

Nachfolgende Graphik bringt den **operationalisierten Level-Ansatz** des BMI aus Kap. 4.1 und den **Generationen-Ansatz mit der Steckdosen-Metapher** aus Kap. 4.2 zusammen und bildet ihn als 9-Felder-Portfolio ab (siehe Abbildung 34).

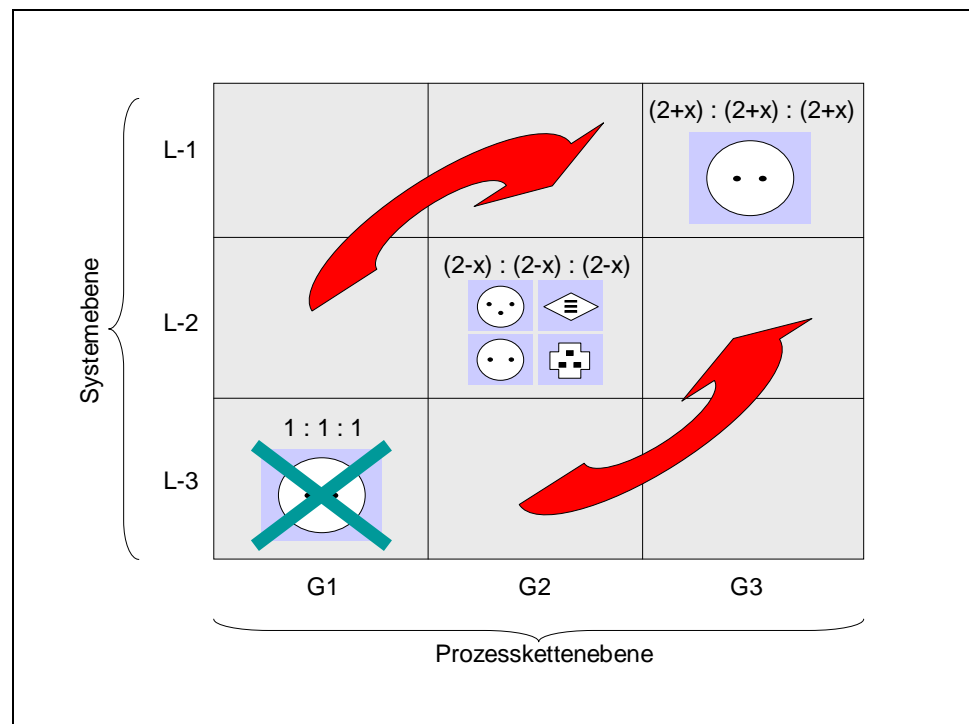


Abbildung 34: PRK Levels und Generationen (Quelle: Eigene Darstellung)

Der Level-Ansatz kann als **systemischer Ansatz** bezeichnet werden, die Levels lassen sich nicht direkt beobachten sondern entstehen in dem Zusammenspiel der Akteure und der Prozessketten. Allgemeines Ziel ist stets die Levelanhebung.

Der Generationen-Ansatz ist ein **Ansatz**, der **auf Prozesskettenebene** arbeitet. Dort lässt sich direkt beobachten, ob eine PRK das Attribut Generation G1, G2 und / oder G3 inne hat und folglich dergestalt verfügbar ist und von Wirtschaft und Verwaltung genutzt werden kann. Spezifisches Ziel ist

stets die Neugestaltung und Optimierung nach zu wählenden Zielen und Anforderungen (siehe Kap. 4.2.2 bis 4.2.5).

So wie es **keinen generischen Bauplan** für den Bau eines Hauses geben kann, gibt es keinen generischen Bauplan für eine PRK zwischen Wirtschaft und Verwaltung. Es gibt aber **anerkannte Ziele, Indikatoren und Werkzeuge**, um strategische Baupläne und operative Handlungsempfehlungen abzuleiten. Dies versucht die PRK-Scoping Matrix und die damit verbundene Vorgehensweise zu unterstützen.

PRK-Scoping¹²

ist eine in der Machbarkeitsstudie entwickelte wissenschaftliche und praktische Methode, um zu erreichende Ziele von Prozessketten zu planen – wirtschaftlich / prozessual / organisatorisch, IT-architektonisch, sicherheitstechnisch und juristisch.

Die PRK-Scoping Matrix bietet einen zusammenfassenden Überblick der Ziele und Anforderungen des Autorenteam aus Kap. 4.1 und Kap. 4.2 (siehe Tabelle 5). Diese können je nach Fall und Herausforderung vom Leser selektiert, angepasst, erweitert und eingesetzt werden. Die PRK-Scoping Matrix ist eine Materialie, die dem Leser konstruktiv und reflexiv dienen soll (Prinzip Self-Customisation und Selbstanwendung).

Zur Anwendung:

- **Spalte "Checkboxen"** – es gibt Muss- () und Kann- () Ziele. z. B. die Checkboxen für das Ziel "Levelanhebung" sind gemäß der Zielsetzung der Studie vorgegeben, gesetzliche Ziele gleichfalls; andere Zeilen können wie oben beschrieben optional selektiert werden.
- **Spalte "Ziele"** – die Ziele für PRK Level-1 (Systemebene) bzw. Generation 3 (Prozesskettenebene), die das Autorenteam vorschlägt (Kap. 4.2)

¹² Scope (englisch) heißt sinngemäß Abgrenzung, Anwendungsbereich, Aufgabenbereich, Bandbreite, Handlungsspielraum; als Fachausdruck "Scoping" im IT-Anforderungsmanagement vorkommend

- **Spalte "Indikatoren"** – für die Steuerung und das Controlling von Prozessketten ist eine Operationalisierung von Zielen in Form geeigneter Indikatoren notwendig. Diese Indikatoren sollen dazu dienen, die Effektivität und Effizienz der Prozessketten aufzuzeigen und die Auswirkungen von Leistungsveränderungen auf die Zielgrößen sichtbar zu machen. Dabei ist die Anzahl von Indikatoren auf ein Mindestmaß zu reduzieren. Für Leistungsvergleiche ist es darüber hinaus sinnvoll und notwendig, möglichst einheitliche Indikatoren für die Prozesskette festzulegen (Schmelzer / Sesselmann 2003).
- **Spalte: "Werkzeuge"** – die angegebenen Werkzeuge werden vom Autorenteam zur Anwendung vorgeschlagen (siehe Kap. 5.2 und Anhang II); es gibt, je nach Zielsetzung, natürlich viele weitere Methoden: WiBe, EFQM, BSC, TRIZ etc.; für manche Fragestellungen sind neue Methoden zu kombinieren oder zu erfinden.

4.3.2 PRK-Scoping Matrix: Ziele, Indikatoren und Werkzeuge

Check-boxen	Ziel	Indikatoren	Werkzeuge
"Levelanhebung"			
<input type="checkbox"/>	Level-3	1 : 1 : 1	Vorgehensweise "PRK-Screening", Vorgehensweise "PRK-Scoping", strategischer PRK-Bauplan und operative Handlungsempfehlungen
<input type="checkbox"/>	Level-2	(2-x) : (2-x) : (2-x)	
<input checked="" type="checkbox"/>	Level-1	(2+x) : (2+x) : (2+x)	

Check-boxen	Ziel	Indikatoren	Werkzeuge
"Wirtschaftliche Effizienz und Effektivität der PRK"			
<input type="checkbox"/>	[W1] Prozesskosten minimieren	SKM-Kosten, Trafoeffekt eGOV-Rechner	Modul A "SKM", "eGOV-Rechner" und Industrialisierungs-Quick-Check für Banken ("IQC") mit Submodul E "Betreibermodell und Changemanagement"
<input type="checkbox"/>	[W2] Bürokratie abbauen	Anzahl der existenten Pflicht-Prozessketten, Anzahl der Prozessschritte, Anzahl der Medienbrüche und Durchlaufzeiten	
<input type="checkbox"/>	[W3] Verwaltung modernisieren	Grad der Innovation (State-of-the-Art, Stand von Forschung und Technik), Best Practices	
<input type="checkbox"/>	[W4] Fallzahlen maximieren	absolute und relative Fallzahlen	
<input type="checkbox"/>	[W5] Qualität, Reifegrad und Exzellenz der PRK erhöhen	multidimensionaler Index mit Qualitätsfaktoren (Kundenzufriedenheit etc.)	
<input type="checkbox"/>	[W6] Existenz eines Geschäfts- / Betreibermodells	Grad der Institutionalisierung, Angebot und Nachfrage (Nutzung)	
<input type="checkbox"/>	[Wx] Weitere Zielsetzung		

Check-boxen	Ziel	Indikatoren	Werkzeuge
"Zukunftssicherheit von IT-Architektur und IT-Governance für die PRK"			
<input type="checkbox"/>	[IT1] Realisierung eines hohen Grad an IT-Unterstützung	Automatisierungsgrad, Anzahl der IT-unterstützten Prozesse / Prozessschritte, gemessene Zeiten und Kosten (einschließlich der Aufwendungen für die IT)	Modul B "IT-Architektur und IT-Governance für Prozessketten"
<input type="checkbox"/>	[IT2] Orientierung der technische Dienste an den Geschäftsprozessen	Anzahl der Dienste, die keine Unterstützung eines Geschäftsprozess anbieten, bzw. deren Funktionalität nicht mit dem Bedarf der zugeordneten Prozessschritte übereinstimmt.	
<input type="checkbox"/>	[IT3] Kompatibilität der IT-Anwendungen optimieren	Anzahl der Medienbrüche, Anzahl der nur technisch bedingten Transformationen (zwischen Protokollen und Datenschemata)	
<input type="checkbox"/>	[IT4] Kompatibilität zum SAGA-Standard (Bundesverwaltung) ausbauen	Anzahl der nicht SAGA-konformen Objekte (Architekturmuster, Protokolle, Schemata usw.).	
<input type="checkbox"/>	[IT5] Nutzung offener Standards ausweiten	Anzahl verwandter nicht offener Konzepte	
<input type="checkbox"/>	[ITx] Weitere Zielsetzung		

Check-boxen	Ziel	Indikatoren	Werkzeuge
"Sicherheit der PRK"			
<input checked="" type="checkbox"/>	[S1] Vertraulichkeit der gespeicherten und übertragenen Informationen optimieren (Umsetzung von IT-Grundschutz für alle Beteiligten – Basisschutz, Einhaltung datenschutzrechtlicher Bestimmungen)	Anzahl Sicherheitsverstöße, Missbrauch personenbezogener Daten, Nichtautorisierte Zugriffe auf Informationsbestände Festgestellte Mängel bei Audits, Güte der Verschlüsselung	Modul C "IT-Sicherheitsmechanismen und Regelwerke für Prozessketten"
<input checked="" type="checkbox"/>	[S2] Integrität von Informationen verbessern (leichte Nachweisbarkeit von Fälschungen)	Anzahl Sicherheitsverstöße, Inkonsistente Datenbestände, Güte der elektronischen Signatur	
<input checked="" type="checkbox"/>	[S3] Verfügbarkeit der Informationen und IT-Anwendungen und – Systeme maximieren (SLAs gemäß Verfügbarkeitsanforderungen)	Anzahl Sicherheitsverstöße, Häufigkeit von Systemausfällen, Prozessausfälle,	
<input checked="" type="checkbox"/>	[S4] Authentizität, Nachweisbarkeit, Nicht-Abstreitbarkeit optimieren (Einsatz elektronischer Signaturen: Möglichkeit zur Überprüfung wer welche Aktionen zu welcher Zeit durchgeführt hat)	Güte der elektronischen Signatur, Zeitstempel	
<input checked="" type="checkbox"/>	[S5] Hoher Grad an Vertrauenswürdigkeit in die Prozesskette realisieren (IT-Grundschutzzertifizierung der Prozesskette)	Anzahl Sicherheitsverstöße, Inkonsistente Datenbestände, Anzahl der Betrugsfälle	
<input checked="" type="checkbox"/>	[S6] Angemessener Aufwand für Informationssicherheit adressieren (Den differenzierten Schutzbedarfen der Prozesskette entsprechende Anwendung der IT-Grundschutz-Vorgehensweise)	Usability, Kosten	
<input type="checkbox"/>	[Sx] Weitere Zielsetzung		

Check-boxen	Ziel	Indikatoren	Werkzeuge
"Rechtssicherheit der PRK"			
<input checked="" type="checkbox"/>	[R1] Datenschutz: Die gesetzlichen datenschutzrechtlichen Bestimmungen werden eingehalten. Verbot jeglicher Vorratshaltung von personenbezogenen Daten.	Missbrauch personenbezogener Daten	Modul D "Die rechtssichere Prozesskette"
<input checked="" type="checkbox"/>	[R2] Die elektronische Signatur des Antragstellers, des Übermittelnden bzw. Abrufenden kann eingesetzt werden	Rechtsverbindlichkeit / Rechtssicherheit	
<input checked="" type="checkbox"/>	[R3] PRK und ihre rechtssichere Umsetzung ist in Bezug auf etwaige Verschärfung des BDSG (Strafe statt Ordnungswidrigkeit) zu antizipieren	Stellung von BDSG bei Gesetzgeber und Rechtsprechung	
<input checked="" type="checkbox"/>	[R4] EU-Recht Konformität sicherstellen. Europaweite Harmonisierung des Passwesens	z. B. Umsetzung der Richtlinie zur EU-Dienstleistungsrichtlinie / freier Verkehr von Waren und Dienstleistungen; z. B. EU-Recht konforme AGB	
<input checked="" type="checkbox"/>	[R5] Notwendigkeit der Harmonisierung bei Verträgen innerhalb der EU, z. B. Richtlinie 2008 / 48 / EG des Europäischen Parlaments und des Rates vom 23. April 2008 über Verbraucherkreditverträge und zur Aufhebung der Richtlinie 87 / 102 / EWG des Rates	§ 492 BGB des Gesetzentwurfes der Bundesregierung "... Umsetzung der Verbraucherkreditrichtlinie, ..." vom 05.11.2008 ermöglicht den Abschluss von Verbraucherkreditverträgen in elektronischer Form.	
<input checked="" type="checkbox"/>	[R6] PRK und ihre rechtssichere Umsetzung ist in Bezug auf die Verankerung von IT im Grundgesetz zu antizipieren (z. B. Recht auf informationelle Selbstbestimmung)	Stellung IT im Grundgesetz	
<input type="checkbox"/>	[Rx] Weitere Zielsetzung		

Tabelle 5: PRK-Scoping Matrix: Ziele, Indikatoren und Werkzeuge

5 Der Bauplan für Prozessketten Level-1

5.1 Vorgehensmodell im Überblick: PRK-Screening, PRK-Scoping, PRK-Bauplan

Bevor in Kap. 5.2 eine Kurzanleitung zu den im Anhang der Studie befindlichen Werkzeugen gegeben wird, soll an dieser Stelle nochmals der Rückblick auf das ausgangs im Kap. 1 vorgestellte Gesamtvorgehensmodell der Machbarkeitsstudie erfolgen (siehe Abbildung 35).

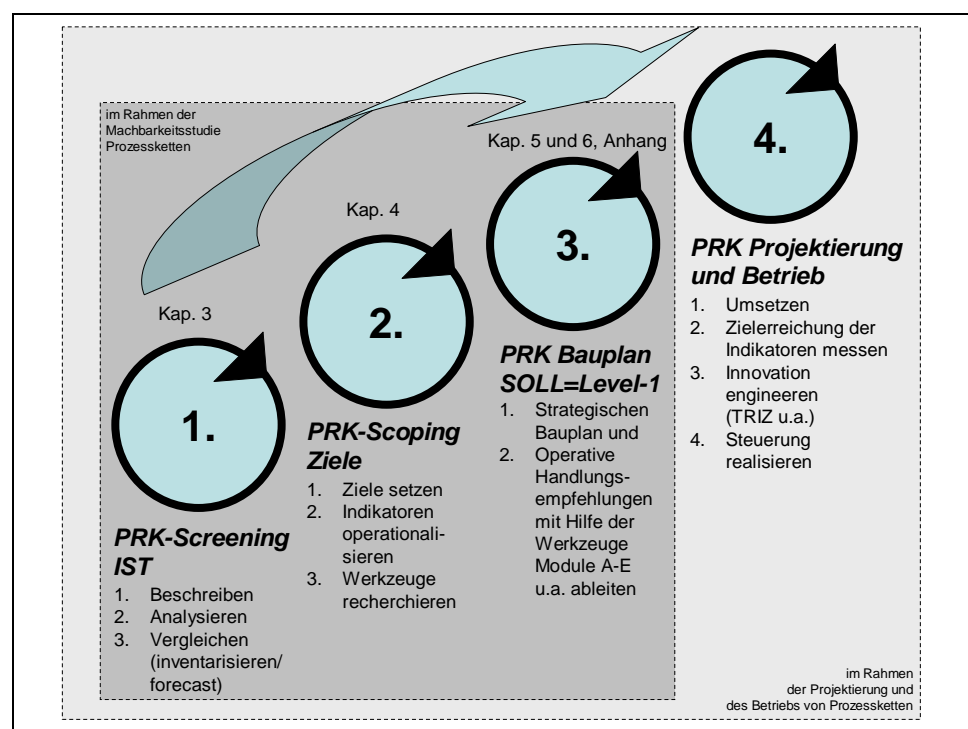


Abbildung 35: Gesamtvorgehensmodell in Wirkkreisen (Quelle: Eigene Darstellung)

Im Kap. 3 wurde die Methode "PRK-Screening" hergeleitet und auf die PRK FDL in Deutschland angewandt. Kap. 4 entwickelte die Methode "PRK-Scoping" und beschrieb sie im Detail für den generischen Einsatz. Im Kap. 5, in dem sich der Leser jetzt befindet, erfolgt der Brückenschlag zu den

Werkzeugen, um sich (selbst) strategische Baupläne und operative Handlungsempfehlungen für PRK Level-1 abzuleiten.

PRK-Bauplan

ist eine in der Machbarkeitsstudie entwickelte wissenschaftliche und praktische Methode, um eine Skizze für die Umsetzung von Prozessketten zwischen Wirtschaft und Verwaltung zu erstellen.

Dazu werden auf Basis der Ergebnisse des Einsatzes von PRK-Screening und PRK-Scoping und mittels Anwendung der Module A-D u. a. (siehe Kap. 5.2 und Anhang II) strategische und operative Handlungsempfehlungen abgeleitet.

Folgende Teilschritte werden bei Erstellung des Bauplans für Prozessketten berücksichtigt:

- Beteiligte Akteure an der Prozesskette identifizieren
- Beziehungen zwischen den Akteuren identifizieren und beschreiben
- Kompetenzen innerhalb der gesamten Prozesskette festlegen
- Schnittstellen zwischen einzelnen Prozessen identifizieren und beschreiben
- Prozesskette über alle Partner integrieren
- Module selektieren und anwenden
- Handlungsfelder identifizieren und beschreiben
- Optimierungen planen, umsetzen und kontrollieren

5.2 Module zur Ableitung von Handlungsempfehlungen (Selbstanleitung)

5.2.1 Die Module im Überblick

Im Anhang II sind die nachfolgenden Module A-E für die Selbstanwenderin und den Selbstanwender hinterlegt, in Kap. 5.2 erfolgt eine kurze Anleitung zur Selbsthilfe bzw. Selbstbedienung (siehe Abbildung 36).

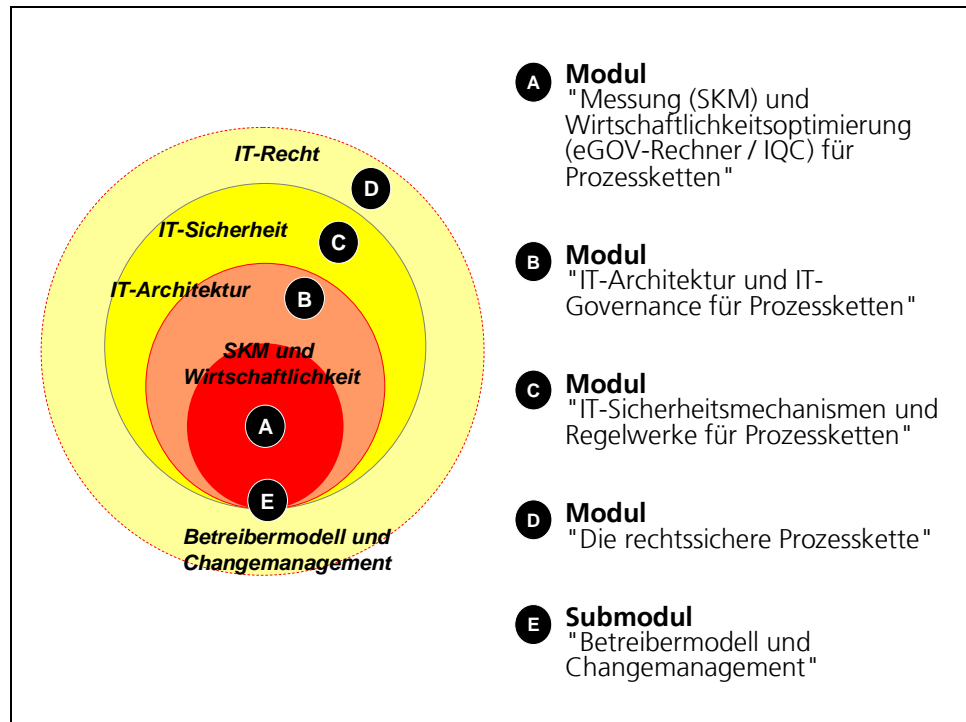


Abbildung 36: Werkzeug-Module des Anhangs im Überblick (Quelle: Eigene Darstellung)

5.2.2 Modul A "eGOV-Rechner"

Qui bono? Quid bonum? – Wem und was nützt eGovernment?

Zur Beantwortung dieser Frage, die die Entscheidungsträgerinnen und Entscheidungsträger in Verwaltung, Politik und Wirtschaft stellen, wurde als Werkzeug der Fraunhofer eGOV-Rechner entwickelt und 2007 veröffentlicht (www.egov-rechner.org).

Entscheidende Zielgröße, die mit dem eGOV-Rechner ausgerechnet wird, ist der **Transformationseffekt pro Prozess in Euro:**

Gesamtkosten IST Prozess
abzgl. Gesamtkosten SOLL Prozess
 = Transformationseffekt

Auf die Thematik der Studie übertragen, kann der eGOV-Rechner und seine Module eine Prozesskette Level-3 bzw. der Generation 1 quantitativ mit der

entsprechenden Prozesskette Level-1 bzw. der Generation 3 (siehe Kap. 4) vergleichen.

Im entsprechenden Anhang ist als vorbereitete Materialie zur Anschauung ein Excel-Datenblatt für eine einfache Prozesskette als IST (z. B. Bank – Bundesbank) und ein Excel-Datenblatt für eine komplexere Prozesskette als SOLL (Bank – Bundesbank Extranet – Bundesbank) hinterlegt. Das komplette digitale Werkzeug lässt sich in Form eines Startpakets mit Guideline, Beispielen, Exceltools etc. unter www.egov-rechner.org herunterladen und für einen zu untersuchenden Prozess bzw. eine zu untersuchende Prozesskette anpassen.

Vorgehen

Der **eGOV-Rechner Prozess-Designer** ist ein Basismodul und seine Vorarbeiten sind Voraussetzung für den zielführenden Einsatz des nächsten Moduls Prozess-Kalkulator (siehe hier und im folgenden Fröschle / Gözl 2007: 13 ff. und Fröschle / Gözl / Klocke 2007).

Es ist ein Prozessbild für den klassischen Prozess und ein Prozessbild für den digitalen Geschäftsprozess zu erstellen.

Der eGOV-Rechner schlägt als Methode in einem Template ein simples Rahmenwerk vor. Ein Prozess wird dazu in seine Einzelprozessschritte zerlegt. Die **Einzelprozessschritte werden** anschließend

1. **in der Dimension "Zeit"** (Informations-, Verabredungs- und Transaktionsphase) **abgetragen** und
2. **in der Dimension "Akteure"** (z. B. Bürger, Bürgerbüro, Fachamt, Rechenzentrum etc.) **zugeordnet**.

Die Modellierung solcher Ablaufvisualisierungen kann mit verschiedenen Programmen durchgeführt werden, z. B. Powerpoint, VISIO, ADONIS, ARIS etc. oder einfach auf einer Flipchart an der Wand.

Auf der Basis des Rahmenwerks des Process-Designers ist eine handhabbare E-Government Matrix mit Zellen entstanden. Im **eGOV-Rechner Prozess-Kalkulator** können nun **transparent die Daten eingegeben und Ergebnisse berechnet werden**, wer wie lange welche Einzelprozesse betreibt und welche Kosten anfallen.

Die Teilprozesse des Gesamtprozesses sind mit Kosten und Nutzen besetzt, welche im Untersuchungsinteresse stehen. Finanzströme, interne Verrech-

nungen und Opportunitätskosten werden quantitativ gemessen und einzel- und gesamtwirtschaftlich kalkuliert (Fallzahlen, Kommunikationskanalkosten, Warte-, Liege- und Rüstzeitenkosten, gemeinsame Bearbeitungskosten, Einzelbearbeitungskosten, IT-Kosten, Sachkosten, Abgaben / Gebühren etc.).

Die Datenerhebung erfolgt mithilfe von Interviews, Studium von Jahresberichten und Statistiken, Datenbankabfragen, Stoppuhrmessungen, Webserver-Logfile-Auswertungen etc.

Der eGOV-Rechner integriert Kosten grundsätzlich im Sinne von Ausgaben, Einnahmen und Aufwänden (Opportunitätskosten).

Der eGOV-Rechner arbeitet mit einer Prozesskostenrechnung auf Basis einer prozessorientierten Kostenträgerrechnung mit Durchschnittsprozesskostenbetrachtung.

Einsatzzweck

Das Werkzeug eGOV-Rechner kann eingesetzt werden, um Prozesse bzw. Prozessketten zu planen, zu kalkulieren und zu evaluieren:

- Der eGOV-Rechner arbeitet **prozess(ketten)orientiert, nicht projektorientiert** wie z. B. WiBe21 mit seinen Modulen Investitionskostenrechnung und Nutzwertanalyse (WiBe 2008).
- Er ist **generisch für Prozesse und Prozessketten** jeglicher Art **verwendbar** und zielt nicht zuerst ausschließlich auf Informationspflichten (Statistisches Bundesamt 2006).
- Er ist vom **Ansatz her organisationsübergreifend** und kann x-beliebige Akteure aus Wirtschaft und Verwaltung in die Erweiterte Wirtschaftlichkeitsrechnung aufnehmen.
- Er arbeitet nach der **Vergleichenden Methode**, sprich es wird dabei der IST Prozess quantitativ und qualitativ mit dem existierenden oder geplanten SOLL Prozess als Fixpunkt verglichen.
- Er integriert **Opportunitätskosten** und setzt entgangenen Aufwand (bzw. realisierten Nutzen), der z. B. bei einer Prozesskette Level-1 im Gegensatz zu einer Prozesskette Level-3 nicht anfällt, an. Es werden also nicht allein öffentliche Haushaltszahlen, monetäre Ein- und Auszahlungen etc. betrachtet.

Lizenz

Der eGOV-Rechner ist lizenziert unter der "Creative Commons. Namensnennung – Weitergabe unter gleichen Bedingungen 2.0 Deutschland"-Lizenz (<http://creativecommons.org/licenses/by-sa/2.0/de>). Die Anwenderin und der Anwender kann den eGOV-Rechner ganz auf seine eigenen Bedürfnisse anpassen, etwa auch die Formeln und die Makros verändern, sowie zu gleichen Bedingungen und unter Nennung der Autorenschaft weitergeben. Über eine Rückmeldung freut sich das Autorenteam.

5.2.3 Modul A "Industrialisierungs-Quick-Check für Banken (IQC)"

Mit dem Industrialisierungs-Quick-Check (IQC) stellt das Fraunhofer IAO einen erprobten Ansatz bereit, mit dessen Hilfe Banken in die Lage versetzt werden, eine systematische Analyse bezüglich ihres Industrialisierungs-Reifegrades durchzuführen. Als Ergebnis erhalten Banken eine detaillierte Analyse der vorhandenen Industrialisierungslücken, sowie eine Methoden- und Instrumentenauswahl zur Schließung der identifizierten Lücken.

Der IQC zielt auf die prozessorientierte und funktionsübergreifende Steigerung der Produktivität innerhalb der Bank und in der Kooperation mit externen Partnern ab. Dabei orientiert er sich an der Strategie und den Zielen des Institutes, sowie an dessen spezifischer Marktsituation.

Die Zielgruppe des IQC sind vor allem Führungskräfte von Banken, insbesondere Prozessverantwortliche sowie Entscheidungsträgerinnen und Entscheidungsträgern aus den Bereichen Organisation, Prozesse und IT.

Konkret soll der IQC die Banken bei der Erreichung folgender Zielsetzungen unterstützen:

- Identifikation und Konzentration auf Prozessketten mit dem größten Potenzial hinsichtlich Wertschöpfung (**Effizienzsteigerung**)
- Fokussierung auf die wesentlichen Felder zur Verbesserung der Wettbewerbsfähigkeit (**Wettbewerbsfokus**)
- Ausrichtung der gesamten Bank auf die Bankenstrategie und Koordination der notwendigen Tätigkeiten (**Strategische Ausrichtung**)
- Durchgängige Konzentration auf die erforderlichen Ergebnisse (**Ergebnissicherung**)

- Systematische Auswahl der geeigneten Methoden und Werkzeuge hinsichtlich dem Wertbeitrag der Industrialisierung (**Wertorientierung**)

Aus diesen genannten Zielsetzungen des IQC lassen sich folgende Ziele bezogen auf die Mitarbeiterinnen und Mitarbeitern ableiten:

- Besseres Rollen- und Aufgabenverständnis (**Klarheit**)
- Wissen, was von Ihnen erwartet wird und wie ihre Arbeit mit der Arbeit anderer und den übergeordneten Zielen zusammenhängt (**Transparenz**)
- Kenntnis des Verantwortungsspielraums und der Kompetenzen (**Empowerment**)
- Möglichkeiten zur gezielten Weiterentwicklung ihrer Fähigkeiten (**Entwicklung**)

Des weiteren wird im Rahmen des IQC eine klare Konzeption zur Produktivitätssteigerung bei Banken beschrieben und ein Ordnungsrahmen für verschiedene Gestaltungsprinzipien, Vorgehen, Methoden und Werkzeuge bereitgestellt.

Der Industrialisierungs-Quick-Check deckt die folgenden vier Bereiche für das Bankmanagement ab:



Abbildung 37: Struktur des IQC (Quelle: Praeg 2008c)

- **Industrialisierungs-Trends und Marktentwicklung:**
Aktuelle und nachhaltige Markttrends und Entwicklungen bilden den Wettbewerbsrahmen für die Banken. Diese Entwicklungen determinieren die Strategien und die daraus abgeleiteten Maßnahmen zur Erhaltung der Wettbewerbsfähigkeit. Diese Trends können im IQC aufgenommen und aus der spezifischen Situation der Bank bewertet werden.
- **Situation und Strategie:**
Aufgrund der gegebenen marktlichen Bedingungen müssen sich die Banken an ihrer strategischen Ausrichtung orientieren. Daher wird in diesem Bereich auf die strategische Ausrichtung fokussiert, um ein kritisches Hinterfragen der eigenen Situation bezüglich der gewünschten strategischen Ausrichtung anzuregen.
- **Reifegradmodell:**
Dieser Bereich zielt auf die vorhandenen internen Abläufe in der Bank ab. Vorhandene Geschäftsprozesse werden auf ihren Reifegrad hinsichtlich der Industrialisierungs-Prozessreife analysiert und von Nutzerinnen und Nutzern bewertet.
- **Methoden und Maßnahmen-Set:**
Basierend auf den Prozess- Bewertungsergebnissen werden vorhandene GAP's (Differenzen zwischen den IST- und SOLL- Prozessreife) identifiziert und quantifiziert. Auf Basis dieser Bewertung werden priorisierte Handlungsempfehlungen für die Nutzerinnen und die Nutzer bereitgestellt. Aufgrund der identifizierten GAP's in den Geschäftsprozessen werden Maßnahmen zum Einsatz geeigneter Methoden und Instrumente bereitgestellt, mit deren Hilfe das innerbetriebliche Methodenmanagement unterstützt werden soll.

Vorgehen

Für den konkreten Einsatz des IQC in der Bank lassen sich die folgenden sechs Vorgehensschritte beschreiben.

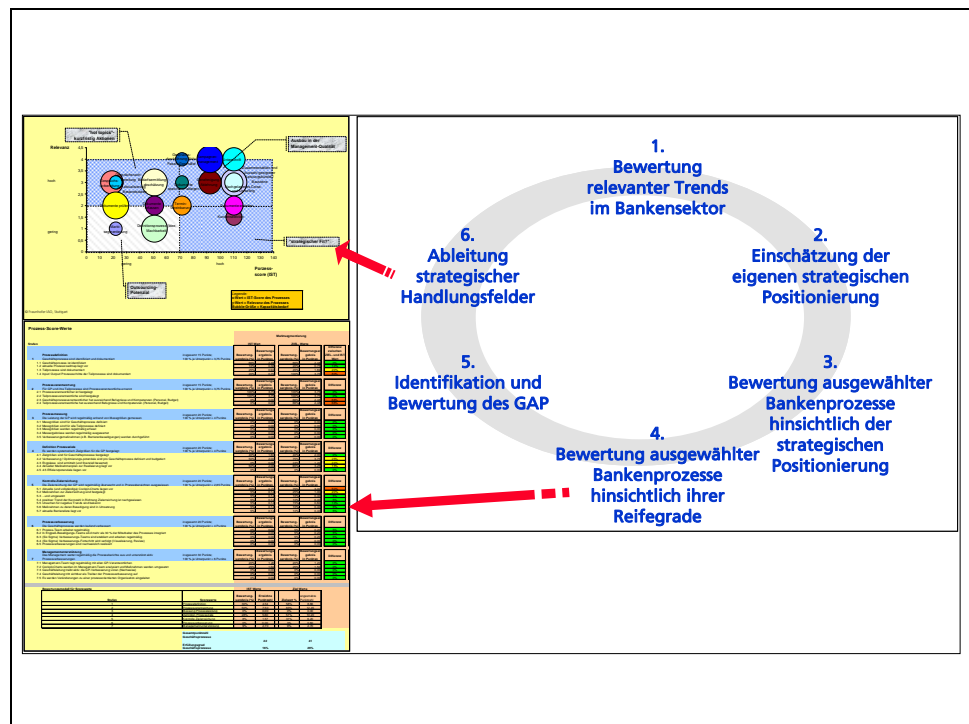


Abbildung 38: Vorgehensschritte zur Nutzung des IQC (Quelle: Eigene Darstellung)

1. Bewertung relevanter Trends im Bankensektor:

Im ersten Schritt bei der Anwendung des Quick-Checks werden die für die Nutzerinnen und Nutzer wichtigen Erfolgsfaktoren und relevanten Marktentwicklungen und Trends aufgenommen. Die dazu notwendigen Informationen können aus aktuellen Marktstudien des Fraunhofer IAO oder der Research-Abteilung der Bank bereitgestellt werden. Im Anschluss daran findet die Einschätzung bezüglich der Relevanz des jeweiligen Trendfaktors sowie eine Gewichtung durch die Anwenderin oder dem Anwender statt.

2. Einschätzung der eigenen strategischen Position

Im zweiten Schritt erfolgt die Einschätzung und Überprüfung der strategischen Positionierung der Bank. Dabei wird von den Nutzerinnen und Nutzern eine Bewertung der verschiedenen vorgegebenen Statements durchgeführt. Dabei können die einzelnen Faktoren gesondert gewichtet und damit die individuelle Situation der Bank berücksichtigt werden. Das Ergebnis beschreibt die nutzerbezogene Einschätzung der strategischen Ausrichtung der Bank.

3. Bewertung der Bankenprozesse in Bezug auf die strategische Positionierung:

In diesem Teil des Quick-Checks werden die zu untersuchenden Geschäftsprozesse bzw. deren Teilprozesse erfasst. Dabei können derzeit maximal 30 Teilprozesse gleichzeitig in der Analyse berücksichtigt werden. Jeder Teilprozess wird einer zweistufigen Bewertung unterzogen. Dabei müssen Nutzerinnen und Nutzer jeweils die Relevanz sowie die intern beanspruchte Kapazität für jeden Teilprozess beurteilen.

4. Bewertung der Bankenprozesse hinsichtlich ihrer Industrialisierungs-Reife

Im vierten Schritt erfolgt die detaillierte Analyse jedes zuvor erfassten Teilprozesses. Dabei wird jeder Teilprozess anhand eines mehrstufigen Verfahrens evaluiert. Dabei bewerten Nutzerinnen und Nutzer den aktuellen Erfüllungsgrad (IST-Wert) eines jeden Reifegradfaktors mittels eines Prozent-Wertes. Die Einschätzung des Erfüllungsgrades wird von den Anwenderinnen und Anwendern vorgenommen.

Im Anschluss daran soll der zukünftig angestrebte Zustand des betreffenden Prozesses ermittelt werden. Dazu benennen Nutzerinnen und Nutzer die anzustrebenden Zielwerte für jeden Reifegrad-Indikator. Aufgrund dieser Bewertung, die für jeden Teilprozess durchzuführen ist, werden Prozess-Score-Werte ermittelt, die sowohl den aktuellen als auch den zukünftig angestrebten Industrialisierungs-Reifegrad darstellen. Darüber hinaus wird für jeden Reifegradfaktor die Differenz zwischen SOLL- und IST-Wert berechnet. Die Differenz wird mittels einer bedingten Formatierung farblich unterstützt.

5. Identifikation der GAP's

Sowohl die Identifikation der vorhandenen GAP's zwischen SOLL- und IST Werten als auch die Gewichtung der einzelnen GAP's mittels der zuvor festgelegten Relevanzfaktoren erfolgt automatisch und verlangt keine unmittelbare Nutzerinteraktion.

6. Ableitung strategischer Handlungsfelder

Aufgrund der zuvor vorgenommenen Bewertungen werden die einzelnen Teilprozesse in einem Prozess-Portfolio dargestellt. Entsprechend der Lage im Portfolio und der Bedeutung des jeweiligen Prozesses können von Nutzerinnen und Nutzern des IQC, entsprechende strategische Handlungsfelder und Maßnahmen definiert werden.

5.2.4 Submodul E "Betreibermodell und Change Management"

Das Submodul "Betreibermodell und Change Management" soll Organisationen (private als auch öffentliche) bei der Planung und Umsetzung sowohl von Veränderungsprozessen als auch bei der Gestaltung neuer, innovativer Betreibermodelle unterstützen.

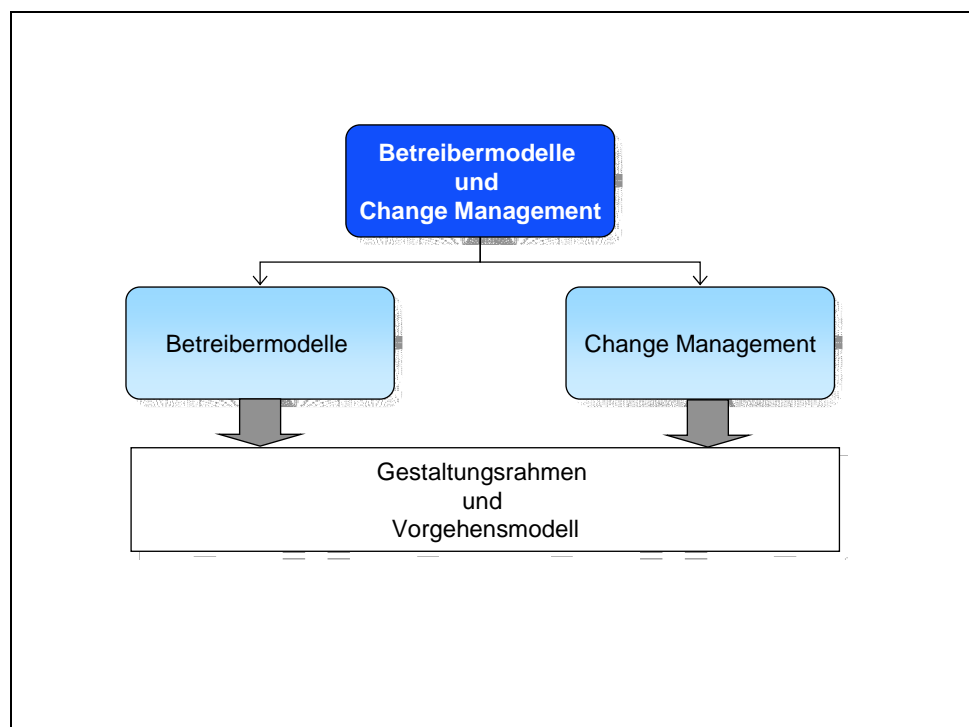


Abbildung 39: Überblick und Struktur des Moduls Betreibermodelle und Change Management (Quelle: Eigene Darstellung)

Dazu werden im folgenden Werkzeuge zur Unterstützung bei der Ausgestaltung als auch Vorgehensmodelle dargestellt. Die Vorgehensmodelle sind bewusst allgemein gehalten, da diese sowohl von wirtschaftsorientierten Unternehmen (Banken) als auch öffentlichen Einrichtungen genutzt werden sollen. Diese Zielgruppen agieren unter unterschiedlichen organisatorischen und rechtlichen Voraussetzungen und Rahmenbedingungen.

Betreibermodelle

Ein Betreibermodell ist ein Geschäftskonzept für die Bereitstellung von Gütern und Dienstleistungen, bei dem diese nicht mehr an Kundinnen und Kunden verkauft, sondern gegen ein leistungsabhängiges Entgelt zur Nut-

zung angeboten werden (Pracht 2008). Betreibermodelle können somit für die Bereitstellung von physischen Produkten und / oder immateriellen Dienstleistungen gestaltet und etabliert werden.

Darüber hinaus erstrecken sich Betreibermodelle nicht nur auf Produkte und Dienstleistungen. Mit der zunehmenden Geschäftsprozessorientierung bei Unternehmen im allgemeinen, sowie Banken und Einrichtungen der öffentlichen Verwaltung im Speziellen, fokussieren Betreibermodelle auf Geschäftsprozesse oder Prozessketten. Diese können komplett oder in Teilen von einem Anbieter für Kundinnen und Kunden bereitgestellt werden.

Charakteristisch für Betreibermodelle ist, dass die zur Leistungserbringung notwendigen Infrastrukturen vom Anbieter bereitgestellt, gewartet und meist auch betrieben werden. Damit übernehmen Anbieter die Verantwortung für die reibungslose Bereitstellung und Funktionsweise ihrer Leistungen und sind darüber hinaus bemüht, die Effizienz der damit verbundenen Prozesse bzw. Prozessketten zu optimieren (Pracht 2008).

Das Betreibermodell beschreibt dabei die Organisation und den Ablauf, wie die adressierten Produkte und Dienstleistungen an Kundinnen und Kunden bereitgestellt werden. Anstatt eines einmaligen Kaufpreises entrichten Kundinnen und Kunden ausschließlich ein leistungsbezogenes Nutzungsentgelt. Das spezifische Preismodell kann je nach Art des Betreibermodells gestaltet werden. Dieses kann ein Spektrum abdecken, welches einen festen monatlichen Betrag bei unbeschränkter Nutzungshäufigkeit bis zur einzelfallbezogenen Bezahlung abdecken.

Dabei bieten Betreibermodelle sowohl für Anbieter als auch Nachfrager der referenzierten Produkte und Dienstleistungen zahlreiche Vorteile (Pracht 2008).

Anbieterseite	Nachfragerseite
Kundenbindungs- und Akquisitionspotenzial	Risikoreduktion
Innovationspotenzial	Kapitalkostensenkung / Finanzierungsvorteile
Erlössteigerungspotenzial (Ausweitung der Wertschöpfung)	Flexibilitätssteigerung
Differenzierungspotenzial	Qualitätssteigerung
	Zugriff auf externe Kapazitäten

Tabelle 6: Betreibermodelle: Anbieter- vs. Nachfragerseite

Für die erfolgreiche Bereitstellung von Betreibermodellen müssen gut ausgebauten Dienstleistungsorganisationen zu Verfügung stehen. Die Herausforderung besteht oftmals im Aufbau notwendiger Kompetenzen in den Bereichen Preis- und Risikomanagement, Finanzierung und Kommunikation.

Die Vielzahl von Betreibermodellen können anhand der in der nachfolgenden Tabelle beschriebenen Ausprägungsformen klassifiziert, beschrieben und gestaltet werden.

Kriterium	Merkmalsausprägungen			
Leistungsfokus	Produkt		Produkt und Dienstleistung	Dienstleistung
Organisationsform	Eigene privatwirtschaftliche Organisation bzw. Organisationseinheit	Gemeinschaftsunternehmen privatwirtschaftlich (z. B. Shared Service Center)	Gemeinschaftsunternehmen öffentlich (z. B. PPP, Shared Service Center)	Öffentliche Einrichtung
Koordinationsform	Hierarchisch		Gemischte Koordinationsform	Marktmechanismus
Kundenfokus	Einzelkunde		Kundengruppe (branchenspezifisch)	Kundengruppe (branchenübergreifend)
Gegenstand	Funktionen		Geschäftsprozess	Prozesskette
Leistungsverrechnung	Umlageverfahren		Direkt	Produkt- / Leistungsorientiert
Preismodell	Fixbetrag pro Zeiteinheit (Flatrate) (z. B. Euro pro Monat)		Fixer Grundbetrag plus nutzungsabhängiger Aufschlag	Rein nutzungsabhängiges Entgelt (pay-per-use)
Absatzmarkt	Kein Zugang		Beschränkter Zugang	Freier Zugang
Kontrahierungsform	Kontrahierungszwang		Kontrahierungsangebot	Wettbewerb
Center-Konzept	Costcenter	Servicecenter	Investmentcenter	Profitcenter
Mitarbeiterinnen und Mitarbeiter	Mitarbeiterkompetenzen evaluieren und weiter entwickeln			
Recht	Rechtliche Rahmenbedingungen berücksichtigen			

Tabelle 7: Gestaltungsfelder von Betreibermodellen (Quelle: Eigene Darstellung, in Anlehnung an Schulz et al. 2008: 69)

Die Tabelle zeigt, wie vielschichtig und komplex die Gestaltung von Betreibermodellen in der Praxis ist. Anhand der dargestellten Gestaltungsbereiche

werden sowohl Banken, Dienstleister als auch Einrichtungen der öffentlichen Verwaltung in die Lage versetzt, die für ein spezifisches Produkt oder eine Dienstleistung im Rahmen der Gestaltung von Level-1 Prozessketten benötigte Leistung, praktikable und nachhaltig tragfähige Betreibermodelle gestalten zu können. Die Klassifizierung sowie die dargestellten Kriterien sollen bei der Ausgestaltung konkreter Betreibermodelle unterstützen. Die Beachtung aller Kriterien ist dabei zu empfehlen, jedoch keine zwingende Voraussetzung.

Zur Gestaltung und Umsetzungsplanung eines Betreibermodells wird folgendes Vorgehensmodell vorgeschlagen.

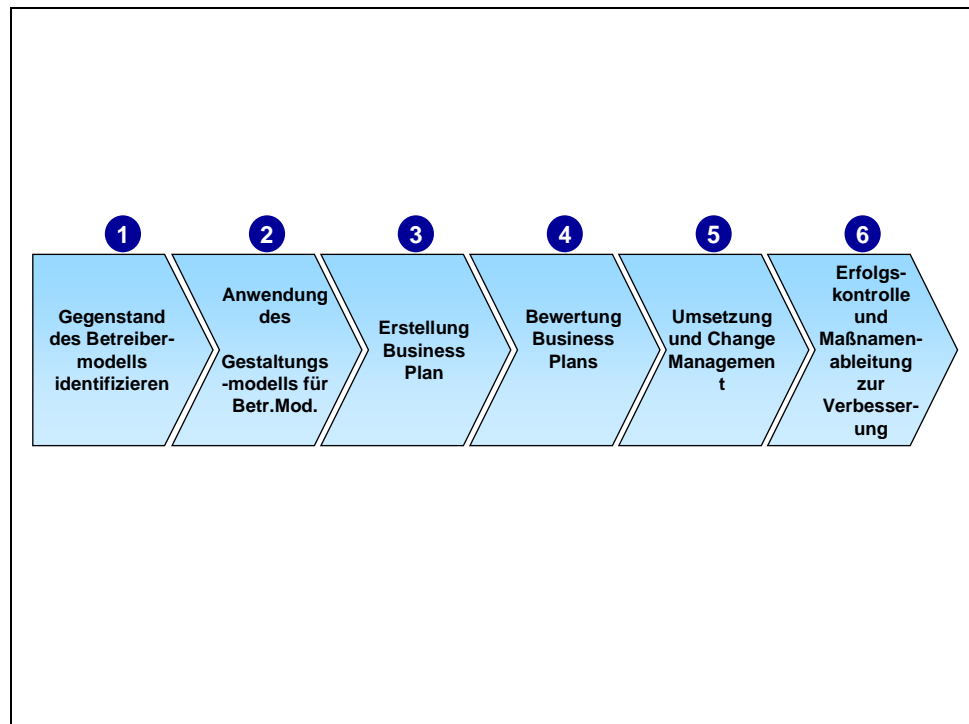


Abbildung 40: Vorgehensmodell zur Gestaltung von Betreibermodellen

Abhängig von der Gestaltung des Betreibermodells muss gegebenenfalls eine Transformation bestehender Organisationen von einem dienstleistenden Produzenten in einen produzierenden Dienstleister erfolgen.

Change Management

Das Change Management zielt auf eine systematische und zielorientierte Veränderung von Organisationen ab. Generell beschreibt Change Management einen Prozess der kontinuierlichen Planung und Realisierung von Veränderungen in Organisationen. Dabei zielt es auf planmäßige mittel- bis langfristig wirksame Veränderungen von Verhaltensmustern und Fähigkeiten ab, um zielgerichtet Prozesse, Prozessketten und Kommunikationsstrukturen zu optimieren (Doppler / Lauterburg 2002).

Dabei ist die Beschreibung geeigneter Veränderungsprozesse ein wichtiger Bestandteil des Change Managements. Im Kontext der organisatorischen Veränderung müssen jedoch auch zahlreiche angrenzende Aspekte des Managements mit berücksichtigt werden, die für ein erfolgreiches organisatorisches Change Management hinreichend und notwendig sind. In diesem Kontext werden Veränderungen erster und zweiter Ordnung adressiert. Veränderungen erster Ordnung sind Verbesserungen bestehender Strukturen, ohne zurunde liegende Werte und Verhaltensweisen zu hinterfragen. Veränderungen zweiter Ordnung betreffen dagegen strategische, technologische, strukturelle und personelle Dimensionen einer Organisation (Kostka / Münch 2002).

Change Management beschreibt einen Prozess kontinuierlicher Planung und Realisierung von Veränderungen, bei denen der Mensch im Mittelpunkt aller Aktivitäten zu berücksichtigen ist. Es gilt verschiedene Stufen der organisatorischen Veränderung gesteuert zu durchlaufen. Diese Stufen der Veränderung sind in der folgenden Abbildung modellhaft darstellt.

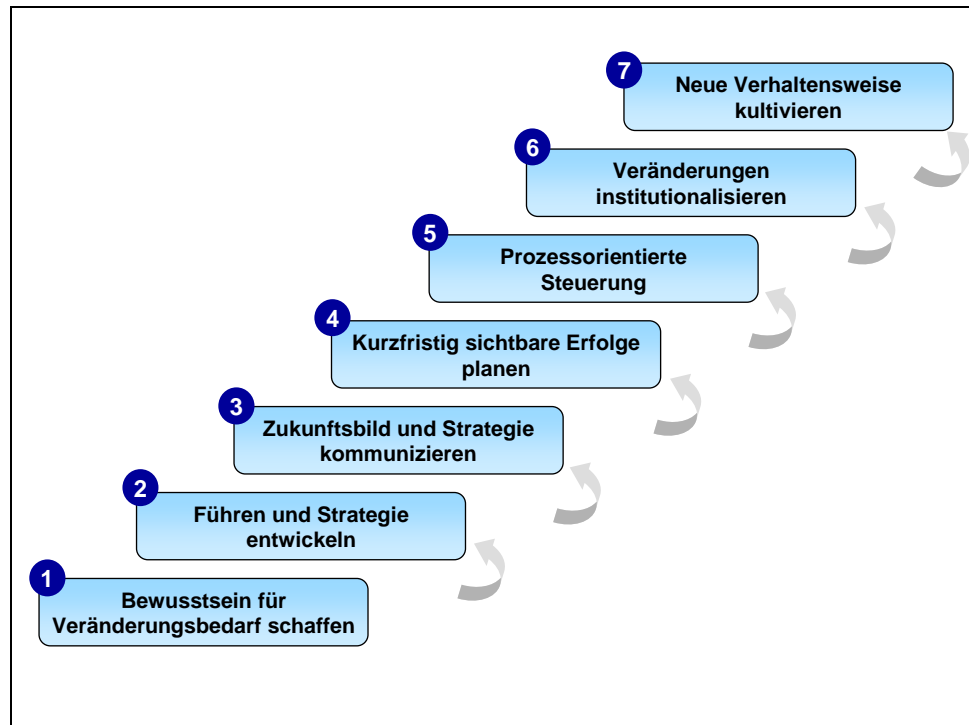


Abbildung 41: Vorgehen im organisatorischen Change Management (Quelle: Eigene Darstellung)

Folgende notwendige Schritte und Aktivitäten werden im nachfolgenden Vorgehensmodell kurz skizziert (Kostka / Münch 2002).

Vorgehensschritte	Aktivitäten
1. Bewusstsein für Veränderungsbedarf schaffen	<ul style="list-style-type: none"> • Relevanten Markt und Wettbewerbssituation untersuchen und evaluieren • Chancen und Risiken erkennen • Potenzielle Krisen antizipieren • Konsequenzen frühzeitig ableiten
2. Ziele definieren und Strategien entwickeln	<ul style="list-style-type: none"> • Gruppe zusammenstellen, die genügend Überzeugung, Kompetenz und Macht besitzt, den Wandel zu gestalten • Ziele entwickeln, die für Veränderungsbestreben richtungsweisend sind • Strategien entwickeln, die zur Realisierung der Ziele beitragen • Indikatoren, Zielerreichungsgrade und Maßnahmen ableiten
3. Ziele und Strategien kommunizieren	<ul style="list-style-type: none"> • Möglichkeiten schaffen und nutzen, um Ziele und Strategien zu kommunizieren • Führungskräfte leben vor, was sie von den Mitarbeiterinnen und Mitarbeitern erwarten (Vorbildfunktion)
4. Kurzfristig sichtbare Erfolge planen	<ul style="list-style-type: none"> • Große Projekte in kleine, übersichtliche Pakete und Aktivitäten zerlegen, um damit sichtbare Leistungsverbesserungen planbar zu machen • Erfolge kommunizieren und Mitarbeiterinnen und Mitarbeiter dafür belohnen
5. Prozessorientierte Steuerung	<ul style="list-style-type: none"> • Strukturen auf die Veränderten Rahmenbedingungen ausrichten • Mitarbeiterinnen und Mitarbeiter an der Neugestaltung beteiligen

	<p>tung beteiligen und Hindernisse beseitigen</p> <ul style="list-style-type: none"> • Zu Risikobereitschaft, Eigeninitiative und konkreten Handlungen ermutigen
6. Veränderungen institutionalisieren	<ul style="list-style-type: none"> • Wachsende Glaubwürdigkeit nutzen, um alle Strukturen und Verfahren, welche nicht zur Zielerreichung beitragen, zu verändern • Mitarbeiterinnen und Mitarbeiter entwickeln, fördern und weiterentwickeln, damit diese den Wandel gestalten können • Den Veränderungsprozess mit neuen Projekten, Themen und Impulsen in Gang halten und beleben
7. Neue Verhaltensweisen kultivieren	<ul style="list-style-type: none"> • Neue Verhaltensweisen in den Unternehmenswerten und Normen etablieren • Beziehung zwischen verändertem Verhalten und Erfolgen aus Veränderungen herausheben • Maßnahmen entwickeln, welche die Führungsentwicklung und –nachfolge sicherstellen

Tabelle 8: Vorgehensweise für Change Management

Um einen tiefgreifenden Wandel zu gestalten muss jede dieser Stufen komplett durchlaufen werden. Dabei ist in der Praxis jedoch nicht eine starre sequenzielle Bearbeitung der einzelnen Stufen angebracht. Aufgrund von neuen Erkenntnissen und Lernfortschritten sind Iterationen notwendig und sinnvoll, um das Veränderungsprojekt auf neue Gegebenheiten anpassen zu können.

5.2.5 Modul B "IT-Architektur und IT-Governance für Prozessketten"

Zur Anwendung der Materialie im Anhang sind dem Leser die zwei folgenden Handreichungen "Vorgehen IT-Architektur" und "Visualisierung von Prozessen und IT-Architektur" an die Hand gegeben.

Vorgehen IT-Architektur

In der nachfolgenden Grafik wird das Vorgehen zur Ableitung einer IT-Architektur schematisch dargestellt (siehe Abbildung 42). Das Primat bei allen Betrachtungen liegt bei den Geschäftsprozessen. Von den Prozessen ausgehend wird erst die IST-Architektur betrachtet und später die SOLL-Architektur bestimmt. Aus der Analyse der IST-Prozesse werden mittels Optimierung und Weiterentwicklung die SOLL-Prozesse entworfen. Für einen möglichst reibungslosen Übergang vom IST zum SOLL werden anschließend Migrationsempfehlungen ausgesprochen.

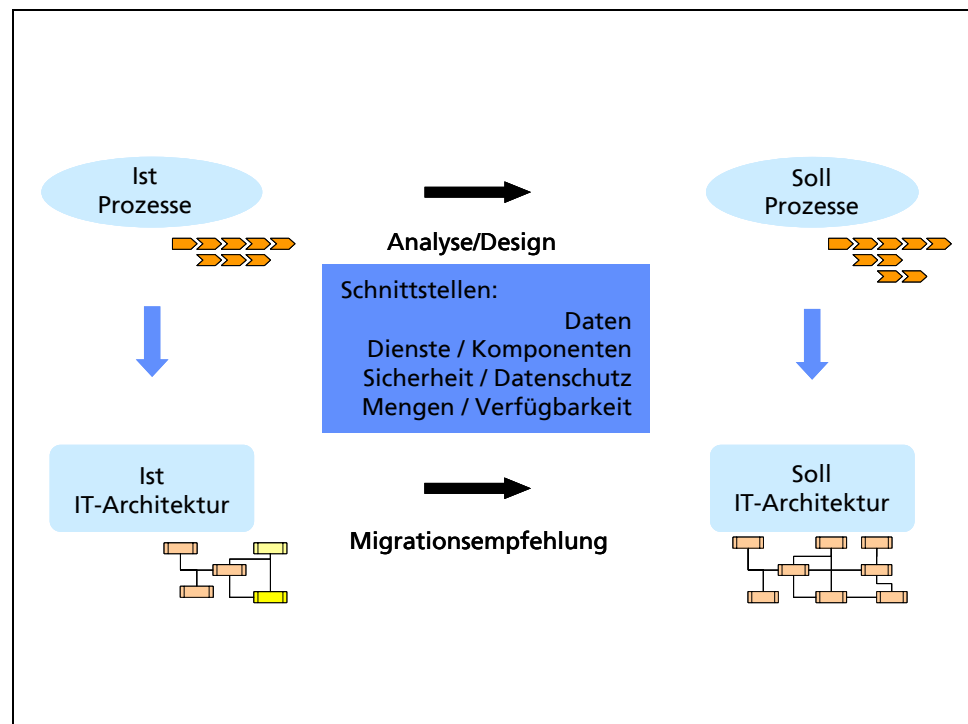


Abbildung 42: Vorgehen IT-Transformation (Quelle: Eigene Darstellung)

Das Hauptaugenmerk liegt dabei, wenn man die Architekturpyramide aus dem IT-Architekturkonzept für die Bundesverwaltung (siehe Abbildung 43) heranzieht, auf den Ebenen zwei und drei. Die Ebene eins, Strategische Ausrichtung, wird natürlich für die Richtung der Weiterentwicklung bestimmend sein.

Ein wichtiger Punkt bei der Beschreibung der IT-Architektur ist die Definition der Schnittstellen. Diese geben an:

- die Daten (fachlichen Inhalt und technische Form), die zwischen den Prozessschritten und Komponenten ausgetauscht werden,
- die Dienste oder Komponenten der IT, zwischen denen Daten ausgetauscht werden,
- die Verbindungen zwischen den Diensten oder Komponenten,
- die nicht funktionalen Eigenschaften, wie Mengenvolumen, Verfügbarkeit, Sicherheit und Datenschutz.

In diesem Vorgehen werden das Architekturkonzept der Bundesverwaltung und der SAGA-Standard berücksichtigt.

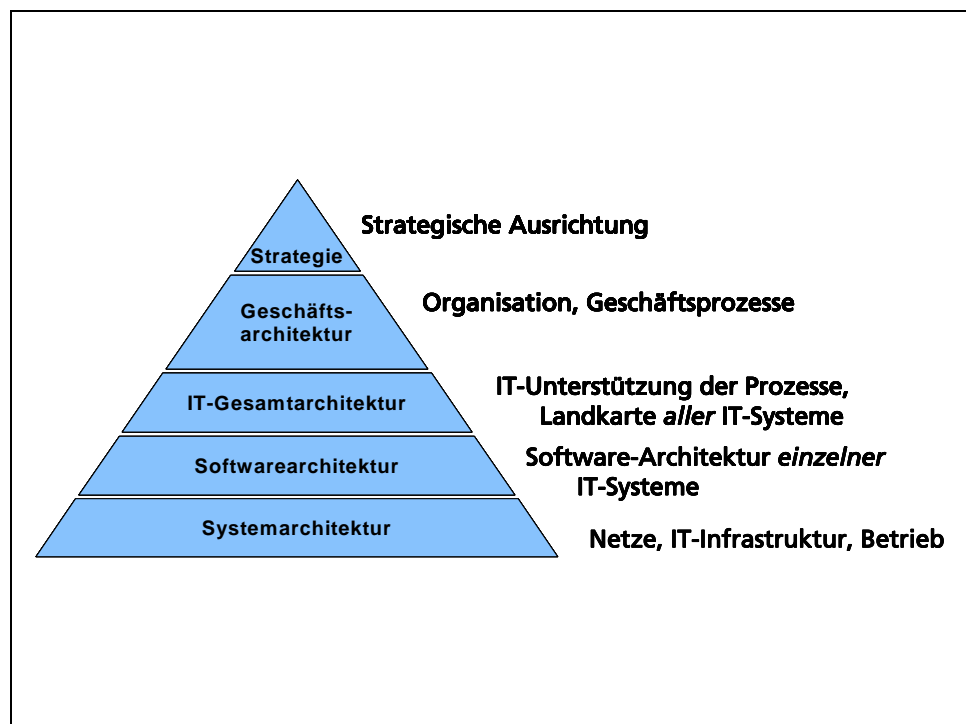


Abbildung 43: Die Architekturpyramide - IT-Architektur nach Architekturkonzept des Bundes (Quelle: KBSt 2007: 5)

Die Planung und Entwicklung der SOLL-Architektur muss sich am Architekturmanagement der Organisationen orientieren. So kann es sein, dass z. B. Komponenten oder Dienste im SOA-Sinne neu entwickelt werden, oder Altanwendungen aus wirtschaftlichen und technischen Gründen bestehen bleiben und mit Hilfe von Fassaden integriert werden. Auf jeden Fall muss

die SOLL-Architektur aber die Anforderungen aus Sicherheitssicht erfüllen. Die gewünschte Referenzarchitektur der Verwaltung ist im "IT-Architekturkonzept für die Bundesverwaltung" und deren Einführung speziell im Kap. 5 beschrieben (KBSt 2007). Für den Prozess, welcher der Analyse und Optimierung hin zur SOLL-Architektur dient, ist es notwendig, dass sich alle Stakeholder aktiv beteiligen (Interviews, Workshops), wie es zum Beispiel in der Architecture Tradeoff Analysis Method (ATAM) (Clements et al. 2001) gefordert wird.

Visualisierung von Prozessen und IT-Architektur

Gegenstand der Betrachtung sind alle Prozessketten, Prozesse oder Prozessschritte (im folgenden Prozessbaustein genannt), die zwischen mindestens zwei der Parteien Bank, Staat, Bürgerinnen und Bürger stattfinden bzw. stattfinden könnten, wenn sie modifiziert werden würden.

Wichtig ist danach die Zuordnung der relevanten Prozessbausteine zu den IT-Komponenten, das sind Fachanwendungen (oder Module davon) oder technische Infrastrukturkomponenten.

Im ersten Schritt wird nur die Grobarchitektur aufgenommen. Eine geeignete Sicht (Visualisierung) dafür sind die aus dem Portfoliomanagement bekannten Darstellungen der Softwarekartographie (Ernst et al. 2007), (TUM SEBIS 2005), (Lankes et al. 2005), darunter besonders die "Process Support Map" (siehe Abbildung 44). Ein Ausschnitt der Prozesslandkarte, d. h. Prozessbausteine (PA) werden oben in der Horizontalen dargestellt. Darunter werden die den PA zugehörigen Fachanwendungen oder Dienste dargestellt. Diese werden noch einmal vertikal differenziert nach der zur Anwendung gehörigen Organisation oder Lokation innerhalb der Organisation. Durch Farben, zusätzliche Symbole oder Annotationen können weitere Aspekte dargestellt werden.

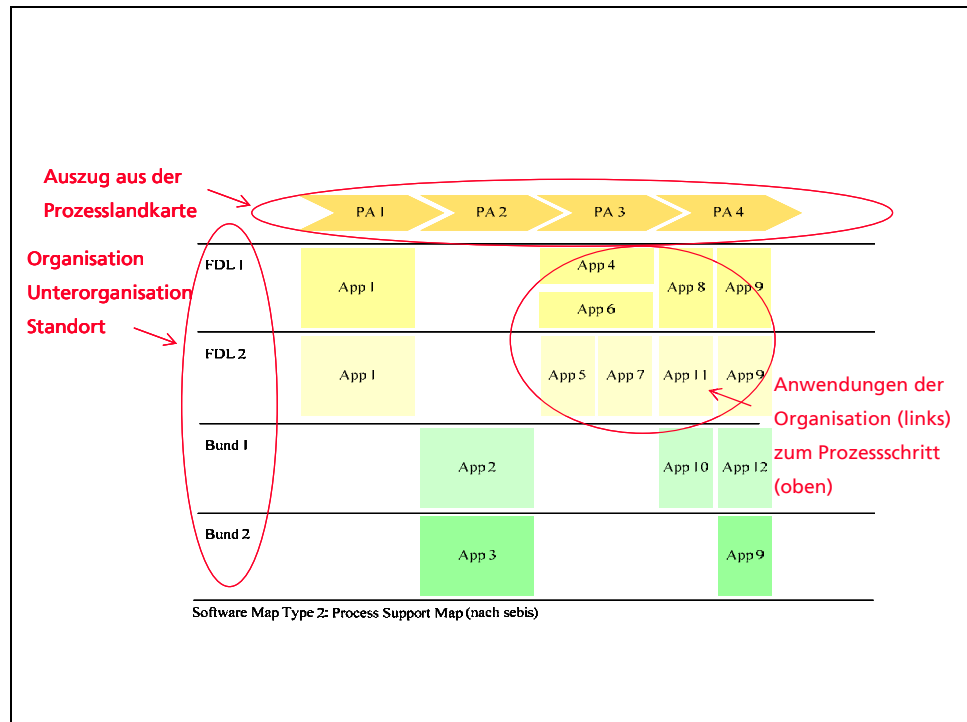


Abbildung 44: Beispiel für eine Process Support Map (Quelle: Eigene Darstellung)

Für die Zusammenhänge zwischen den Anwendungen auf dieser Ebene eignen sich neben UML und Cluster Maps die Block Diagramme der Fundamental Modeling Concepts (FMC) (www.fmc-modeling.org), bekannt aus dem SAP Umfeld. Diese verdeutlichen besonders die menschlichen Akteurrinnen und Akteure, die maschinellen Agenten, die Datenspeicher / Kanäle und die Zusammenhänge zwischen allen (als Beispiel siehe Abbildung 44). Agenten, die man zum Teil als Software-Komponenten auffassen kann, werden durch Rechtecke dargestellt. Datenspeicher oder Kanäle werden als abgerundete Kästen oder als Kreise gezeichnet, verbunden werden immer nur Agenten mit Datenspeicher / Kanälen.

Das Modul B enthält Fragen für die Interviews zur Erfassung der Architektur nach dem geschilderten Vorgehen. Für die Visualisierung wird auf Werkzeuge der Visualisierungsmethoden in der zitierten Literatur verwiesen.

5.2.6 Modul C "IT-Sicherheitsmechanismen und Regelwerke für Prozessketten"

FDL-Prozessketten müssen – unabhängig von ihrem Level – die Vorgaben des IT-Grundschutzes für die anzuwendenden Sicherheitsmechanismen und Regelwerke erfüllen. Es stellt sich die Frage, wie viel Schutz die IT-Anwendungen und informationstechnischen Systeme der Prozessketten benötigen, mit denen vertrauliche Daten verwaltet und übermittelt werden? Diese Frage ist in einem IT-Sicherheitskonzept, das für jede Prozesskette zu erstellen ist, zu beantworten. In dieses Konzept sind alle Komponenten des Informationsverbunds bzw. der (Teil-)Prozesskette, die in die Verwaltung besonders zu schützender Daten involviert sind, zu berücksichtigen.

Schutzbedarfskategorien und deren Definition

Gemäß BSI-Standard 100/2 ist es für die begründete und nachvollziehbare Einschätzung des Schutzbedarfs erforderlich, diese mit Hilfe von eindeutig definierten Kategorien zu klassifizieren. In der Regel genügt es, die vom BSI empfohlenen folgenden drei Einstufungen zu verwenden. Diese unterscheiden den möglichen Schaden nach der Höhe potenzieller Auswirkungen von Sicherheitsvorfällen. Der Schutzbedarf ist

- **normal**, wenn die Schadensauswirkungen begrenzt und überschaubar sind,
- **hoch**, wenn die Schadensauswirkungen beträchtlich sein können, und
- **sehr hoch**, wenn die Schadensauswirkungen ein existenziell bedrohliches, katastrophales Ausmaß erreichen können.

Bei den Schadensauswirkungen sind die folgenden Schadensszenarien zu berücksichtigen:

- Verstöße gegen Gesetze, Vorschriften oder Verträge,
- Beeinträchtigungen des informationellen Selbstbestimmungsrechts,
- Beeinträchtigungen der persönlichen Unversehrtheit,
- Beeinträchtigungen der Aufgabenerfüllung,
- negative Außenwirkung,
- finanzielle Auswirkungen.

Was diese Schutzbedarfskategorien für FDL-Prozessketten bedeuten, kann aufgrund ihrer Möglichkeiten, mit Schäden fertig zu werden, unterschiedlich sein und muss in speziellen Formulierungen für die einzelnen Teilkomponenten differenziert berücksichtigt werden.

Schutzziele für FDL-Prozessketten

Als Grundwerte der Informationssicherheit unterscheidet der BSI-Standard 100/2 die Schutzziele **Vertraulichkeit**, **Integrität** und **Verfügbarkeit**. Daneben sind bei FDL-Prozessketten **Verbindlichkeit**, **Authentizität** und **Nicht-Abstreitbarkeit** als wesentliche Sicherheitsziele zu berücksichtigen.

- Das Sicherheitsziel **Vertraulichkeit** steht für die Gewährleistung, dass Daten und Informationen vor Unbefugten geheim bleiben. Bei elektronischer Datenübermittlung ist die Vertraulichkeit nicht automatisch gewährleistet. Vertraulichkeit erfordert Schutz vor unbefugter Preisgabe und Kenntnisnahme von Informationen. Vertrauliche Informationen dürfen innerhalb einer Prozesskette ausschließlich Befugten in der zulässigen Weise zugänglich sein. Vertraulichkeit von Daten lässt sich durch Verschlüsselung erreichen, wobei normale vertrauliche Informationen sinnvoll durch Verschlüsselung geschützt werden, aber Informationen mit einem hohen bis sehr hohen Schutzbedarf **zwingend** verschlüsselt werden müssen.

Folgende Verschlüsselungsformen verhindern, dass Dritte die übermittelten Daten mitlesen können:

- E-Mail-Verschlüsselung (PGP / MIME, S / MIME bzw. OSCI) oder Datei-Verschlüsselung (bei vertraulichen Anhängen) bei E-Mail und
 - SSL-Verschlüsselung (ggf. mit Client-Authentifizierung zur Vermeidung von Man-in-the-Middle-Angriffen), VPN-Lösungen, SINA-System des BSI sowie OSCI-Verschlüsselung.
- **Integrität** bezeichnet zum einen das Sicherstellen der Unversehrtheit von Daten und zum anderen die korrekte Funktionsweise von Systemen. Eine Verletzung der Integrität von Daten liegt vor, wenn die Daten selbst, aber auch zusätzliche Angaben zu diesen Daten (Metadaten wie Autor oder Erstellungszeitpunkt) unerlaubt verändert werden.

Die Integrität ist eine Voraussetzung für **Verbindlichkeit**. Je nach Pro-

zesskette müssen sich die FDL auf die Verbindlichkeit von ausgetauschten Dokumenten verlassen können. Dazu tragen folgende Faktoren bei:

- **Authentizität** der Sender und Empfänger (bei der Datenübermittlung) ausgewiesen z. B. durch Signatur bei E-Mail und Signatur oder durch ein SSL-Server-Zertifikat bei Datenübertragung über das Internet,
- **Integrität und Authentizität** der Daten z. B. durch Signaturen bei E-Mail und Internetkommunikation sowie
- **Nicht-Abstreitbarkeit der Datenübermittlung** z. B. durch Signatur und ggf. Zeitstempel bei E-Mail und Internetkommunikation.
- Die **Verfügbarkeit** von FDL-Prozessketten ist vorhanden, wenn sie von den Anwenderinnen und Anwendern zu jedem beliebigen Zeitpunkt wie vorgesehen genutzt werden können. Verfügbarkeit ist also die Nutzbarkeit der für die Datenübermittlung benötigten technischen Einrichtungen, z. B. die Erreichbarkeit eines Web- bzw. Mail-Servers. Die Verfügbarkeit kann durch unbeabsichtigten Ausfall technischer Geräte (z. B. eines Datenbank-Servers) oder auch durch vorsätzliche Angriffe beeinträchtigt werden.

Schutzbedarf und Schutzziele von Level-1 Prozessketten

Im Standardfall orientiert sich der gesamte Schutzbedarf eines einfachen Informationsverbunds, also nach oben stehender Definition einer Level-3 Prozesskette, an den dort verwendeten Daten mit der größten Gefährdung. Dies bedeutet, dass ggf. die Prozesskette die Bedingungen des **sehr hohen Schutzbedarfs** erfüllen muss.

Für Level-1 Prozessketten ist dies aber im Normalfall nicht realistisch, da die Usability dadurch eingeschränkt würde und insbesondere die Kosten explodieren würden.

Deshalb ist es notwendig, die Level-1 Prozesskette sinnvoll in Teilprozesse aufzuteilen. Diese Aufteilung orientiert sich an den Schutzzielen und am Schutzbedarf der Prozessschritte. Dadurch soll sichergestellt werden, dass nur die Teile der Level-1 Prozesskette aufwendig geschützt werden, wo es tatsächlich notwendig ist. Alle übrigen Teile der Prozesskette können dann mit **einem geringerem Aufwand angemessen geschützt** werden.

Bei der Anwendung des IT-Grundschutzes ist zusätzlich zu berücksichtigen, dass diese an sich nur für einen Informationsverbund innerhalb einer organi-

satorischen Einheit (Behörde, Unternehmen) vorgesehen ist. Dies entspricht dem Modell einer Level-3 Prozesskette. Das Modell lässt sich auf Level-2 und Level-1 Prozessketten übertragen, indem der Begriff des Informationsverbunds entsprechend erweitert wird.

Maßnahmenbündel, die den Schutzbedarfsanforderungen gerecht werden, können aus den sehr konkreten und oftmals technisch detaillierten IT-Grundschutz-Katalogen oder den generischen Empfehlungen der Normen ISO 27001/2 abgeleitet werden. Die Checklisten im Anhang zeigen beispielhaft auf, zu welchen Aspekten Maßnahmen und Regelungen erforderlich sind.

5.2.7 Modul D "Die rechtssichere Prozesskette"

Datenschutz

Das Bundesdatenschutzgesetz bzw. die Datenschutzgesetze der Länder, sowie datenschutzrechtliche Regelungen in anderen Normen sind bei allen Vorgängen zu beachten. Es ist darauf hinzuwirken, dass alle Beteiligten datenschutzrechtliche Bestimmungen einhalten. Das Verbot jeglicher Vorratshaltung von personenbezogenen Daten ist zu befolgen. Die Beteiligten haben daher personenbezogene Daten zu löschen, die nicht mehr zur "Zweckbestimmung eines Vertragsverhältnisses oder vertragsähnlichen Vertrauensverhältnisses" (§ 28 Abs. 3 Nr. 4 BDSG) notwendig sind. Dies ist beispielsweise bei der elektronischen Verdachtsanzeige (eVA) von Relevanz.

Elektronischer Personalausweis und qualifizierte elektronische Signatur

Gemäß dem Entwurf des Bundeskabinetts vom 23.07.2008 soll zum 01.11.2010 der ePA eingeführt werden. Mit dem ePA erhält jede Bürgerin und jeder Bürger eine eindeutige elektronische Identität (zum elektronischen Identitätsnachweis siehe §§ 17 ff. Entw-ePA). Damit sollte die Bürgerin und der Bürger alle die Identität betreffenden Aufgaben mit einem einzigen maschinell lesbaren Ausweis erledigen können. Dem neuen ePA kommt zentrale Bedeutung zu. Neben der klassischen hoheitlichen Ausweisfunktion ermöglicht der elektronische Identitätsnachweis den Nachweis der Identität in elektronisch durchgeführten Verfahren (E-Government und E-Business).

Der Bundesgesetzgeber hat in den letzten Jahren die erforderlichen Rechtsgrundlagen dafür geschaffen, bei Dokumenten neben der Schriftform eine elektronische Form einzusetzen. 1997 sind das Signaturgesetz (SigG) sowie

die Signaturverordnung (SigV) erstmals in Kraft getreten; 2001 hat der Gesetzgeber das Regelwerk angepasst und u. a. die (qualifizierte) elektronische Signatur eingeführt. Die Ersetzung der gesetzlich vorgeschriebenen Schriftform durch die elektronische Form ermöglicht gemäß §§ 126, 126a BGB nur der Einsatz einer "qualifizierten elektronischen Signatur" (§ 2 Nr. 3 SigG), nicht hingegen die "elektronische Signatur" (§ 2 Nr. 1 SigG) oder die "fortgeschrittene elektronische Signatur" (§ 2 Nr. 2 SigG).

Bislang verbietet § 492 BGB Absatz 1 Satz 2 bei Verbraucherkreditverträgen ihren Abschluss in elektronischer Form: "Der Abschluss des Vertrags in elektronischer Form ist ausgeschlossen." Gemäß dem Gesetzentwurf der Bundesregierung "Entwurf eines Gesetzes zur Umsetzung der Verbraucherkreditrichtlinie, ..." vom 05.11.2008: Gemäß Ziffer "22. § 492 wird wie folgt geändert: a) Absatz 1 Satz 2 und 5 wird aufgehoben." Mit Inkrafttreten des Gesetzentwurfs wird daher der Vertragsschluss bei Verbraucherkreditgeschäften auf elektronischem Weg möglich.

Die qualifizierte elektronische Signatur des Antragstellers, des Übermittelnden bzw. Abrufenden kann und sollte eingesetzt werden. Dringend erforderlich ist neben elektronischen Personalausweis die bundesweite Einführung einer qualifizierten elektronischen Signatur des Datenübermittelnden bzw. -Abrufenden.

Der ePA und die qualifizierte elektronische Signatur ermöglichen im Vergleich mit den bisherigen Verfahren eine vergleichbare und zum Teil höhere Rechtssicherheit. Sowohl die Nutzung via Internet als auch in der Bankfiliale stellen eine starke Verfahrensvereinfachung (Kosteneinsparung) dar. Die qualifizierte elektronische Signatur kann mit elektronisch vorliegenden Daten bzw. Informationen verknüpft werden und ermöglicht, die Identifikation des Ausstellers der Daten sowie die Prüfung der Integrität der Daten.

EU-Recht-Konformität

Im Rahmen der hier behandelten Themenkomplexe ist die EU-Recht Konformität sicherzustellen.

Elektronische Verdachtsanzeige

Generelle Rechtsgrundlagen zur juristische Beschreibung und Analyse der eVA sind das Bundesdatenschutzgesetz (BDSG) und jeweilige Datenschutzgesetze der Länder, vor allem das Geldwäschegesetz (GwG) vom 13. August 2008 (Gesetz über das Aufspüren von Gewinnen aus schweren Straftaten).

Die Kreditinstitute haben die Verpflichtung, Arbeitsmethoden zu entwickeln, die diesen Gesetzen Rechnung tragen (GwG bzw. § 261 StGB). Sie haben einerseits die Pflicht zur Verdachtsanzeige, andererseits müssen Sie das Persönlichkeitsrecht der Kundin und des Kunden wahren.

Nach Meldung eines Verdachts an Strafverfolgungsbehörden bzw. an das BKA (§ 11 GwG, Zentralstelle für Verdachtsanzeigen) wird das Verfahren technisch und organisatorisch bei diesen Ermittlungsbehörden betrieben.

Die Ermittlungsbehörden sollten das die Anzeige erstattende Kreditinstitut nach Erledigung automatisch vom Ausgang des Verfahrens benachrichtigen. Das Kreditinstitut muss bei Erledigung des Verfahrens die Daten zu diesem Fall löschen. Die Speicherung der Daten ist nicht mehr zur Aufgabenerfüllung erforderlich.

5.3 Das Vorgehen zur PRK-Levelanhebung im Überblick

Die bisher im Rahmen der Studie dargestellten Schritte beschreiben detailliert die Analyse und Gestaltung von Prozessketten zwischen Banken und öffentlicher Verwaltung. Dabei wurden sowohl die Vorgehensschritte als auch der Einsatz geeigneter Methoden und Werkzeuge beschrieben, welche für die Gestaltung und Optimierung von Level-1 Prozessketten herangezogen werden können. Die nachfolgende Abbildung zeigt die Vorgehensschritte zur Levelanhebung im Überblick.

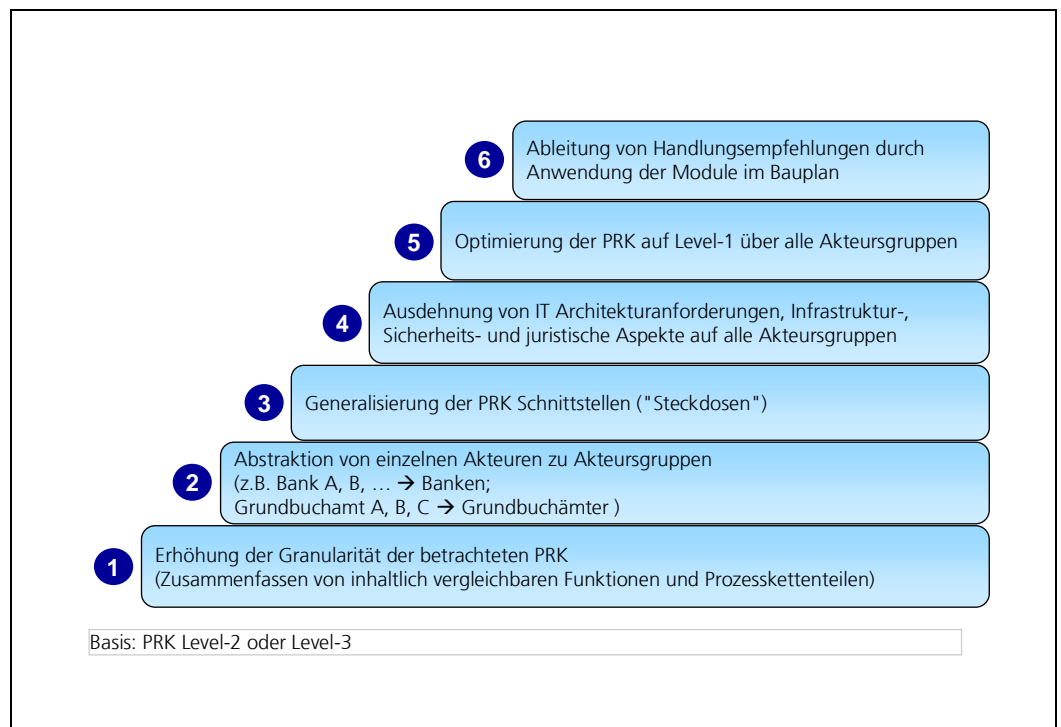


Abbildung 45: Arbeitsschritte zur Levelanhebung im Überblick (Quelle: Eigene Darstellung)

Die einzelnen Arbeitsschritte zur Levelanhebung können folgendermaßen zusammengefasst werden:

1. Ausgangsbasis sind die im Rahmen des Screenings und Scopings identifizierten Level-2 und Level-3 PRK. Im ersten Schritt wird die Granularität der Betrachtung in der Form erhöht, dass vergleichbare Funktionen und Prozesse in neue Prozessteile zusammengefasst werden.

2. Darauf aufbauend werden die beteiligten Akteure in Gruppen zusammengefasst. Dies unterstützt die Abstraktion von einzelnen Akteuren hin zu Akteursgruppen.
3. Entsprechend der Beschreibungen zur PRK-Steckdose werden alle identifizierten Schnittstellen (fachlich, technisch, juristisch) zwischen den Akteursgruppen generalisiert und definiert.
4. In diesem Schritt erfolgt die Ausdehnung der definierten Anforderungen aus Schritt 3 auf alle Akteursgruppen. Die Anforderungen umfassen dabei fachliche, IT-architekturbezogene, IT-sicherheitsbezogene und juristische Aspekte.
5. Anschließend erfolgt die Optimierung der Prozesskette auf Level-1 Ebene über alle Akteursgruppen. Dabei besteht die Möglichkeit, dass partielle Ineffizienzen innerhalb einer Akteursgruppe zugunsten der Gesamtopтимierung der PRK entstehen können.
6. Abschließend werden aufgrund des Einsatzes der in Kap. 5 beschriebenen Module entsprechende Handlungsempfehlungen für eine kontinuierliche Verbesserung der Level-1 PRK erarbeitet.

Anhand dieser Arbeitsschritte können sektorübergreifende Prozessketten zwischen verschiedenen Akteursgruppen gestaltet und optimiert werden. Zur Überprüfung der Wirksamkeit und Praktikabilität des Modells wurde dieses anhand von zwei Fallstudien erprobt und auf seine Handhabbarkeit getestet.

6 Zwei Fallbeispiele: Private Immobilienfinanzierung und Geldwäscheverdachts-Anzeige

Im Rahmen der Fallstudien zur Analyse und Optimierung der **Prozesskette "Private Immobilienfinanzierung"** (Kap. 7) und **Geldwäscheverdachts-Anzeige** (Kap. 8) werden sowohl die in den vorangegangenen Kapiteln beschriebene Vorgehensweise als auch der Einsatz in den vorangegangenen Kapiteln aufgezeigten Module an einer konkreten Prozesskette angewendet.

Die Zielsetzung fokussiert dabei einerseits auf der praktischen Anwendung der zuvor erarbeiteten und beschriebenen Methoden, andererseits auf die Identifikation und Analyse vorhandener Wirtschaftlichkeitspotenziale durch die organisationsübergreifende Optimierung der gesamten Prozesskette.

Die Struktur der Fallstudien orientiert sich am Vorgehensmodell zur Gestaltung von Prozessketten (siehe Kap. 1). Basierend auf dem PRK-Screening der IST-Prozesskette, werden im Rahmen des PRK-Scopings die relevanten Ziele für die Prozesskette "Private Immobilienfinanzierung" ausgewählt. Diese Ziele werden auf Basis von Expertinnen- und Experteneinschätzungen priorisiert und dienen als Basis zur Gestaltung der SOLL-Prozesskette. Die Gestaltung der SOLL-Prozesskette erfolgt durch den Einsatz des PRK-Bauplans. Im abschließenden Teil der Fallstudien erfolgt die Ableitung von Handlungsempfehlungen zur Verbesserung der Prozesskette im Hinblick auf die Zielerreichung und zur Optimierung der organisationsübergreifenden Prozesskettengestaltung.

Es wurden diese beiden Prozessketten für die Fallstudien ausgewählt, da es sich um zwei exemplarische Prozessketten handelt, die **nicht auf Level-1** sind. Im Sinne einer "**problemorientierten Nutzerorientierung**" wurden beide sowohl von den Projektpartner Banken als auch von BMI vorgeschlagen, sie stehen als Vertreter für ein Vielzahl weiterer Prozessketten.

Das PRK-Screening Ergebnis (siehe Kap. 3.2.4 und Anhang I) bildet den Startpunkt für die im folgenden Fallstudien-Ergebnisse, die mittels **erweiter-tem PRK-Screening, spezifischem PRK-Scoping und PRK-Bauplan Ein-satz mit operativen Handlungsempfehlungen** erarbeitet wurden:

- PRK "Private Immobilienfinanzierung"
= ID147, ID148, ID150, ID152 und ID153
(siehe einzelne Ergebnisse im Anhang I)
- PRK "Geldwäscheverdachts-Anzeige"
= ID121
(siehe einzelne Ergebnisse im Anhang I)

Verschiedene Aspekte haben das Autorenteam dazu bewogen die genann-ten Fallstudie auszuwählen.

Gründe für die Auswahl der PRK IMMO

Die Prozesskette der privaten Immobilienfinanzierung wurde ausgewählt aufgrund:

- der hohen Fallzahlen bei Banken für PRK IMMO
- einer breitgefächerten Zielgruppe und föderalen Struktur der Akteure auf Seiten der öffentlichen Verwaltung (alle Banken und deren Kunden, fö-derale Behördenstruktur – KfW, Amtsgerichte etc.)
- der großen identifizierte Optimierungspotenziale bis zu 77 Prozent (Kos-ten + Zeit)
- der hohen Anzahl der internen und externen Schnittstellen
- der Komplexität der PRK (Intern hochkomplex – extern einfach)
- es Grads der technologischen Unterstützung in der PRK – derzeit noch gering
- der Art der nachgelagerten Bearbeitung in den Behörden (manuell pa-pierhaft, Workflow, prozessintegriert)

Gründe für die Auswahl der PRK GVA

Die Prozesskette der elektronischen Geldwäscheverdachtsanzeige wurde ausgewählt aufgrund:

- der Kritikalität (kritikale Prozesse wie im Bereich der Geldwäscheprävention werden manuell papierhaft bedient)
- des derzeit noch geringen Grads der technologischen Unterstützung der PRK
- von identifizierten Optimierungspotenzialen (Kosten, Zeit, Qualität)
- der Anzahl der internen und externen Schnittstellen
- der Komplexität der PRK (Intern hochkomplex – extern einfach)
- der Art der nachgelagerten Bearbeitung in den Behörden (manuell papierhaft, workflow, prozessintegriert)
- der Prozesszeiten der nachgelagerten Bearbeitung bei Behörden

7 Prozesskettenanalyse I: Private Immobilienfinanzierung (IMMO)

Im Rahmen dieser Fallstudie zur Analyse und Optimierung der Prozesskette der privaten Immobilienfinanzierung, werden sowohl die in den vorangegangenen Kapiteln beschriebene Vorgehensweise als auch der Einsatz der in den vorangegangenen Kapiteln aufgezeigten Module an einer konkreten Prozesskette angewendet. Die Zielsetzung fokussiert dabei einerseits auf die praktische Anwendung der zuvor erarbeiteten und beschriebenen Methoden, andererseits auf die Identifikation und Analyse vorhandener Wirtschaftlichkeitspotenziale durch die organisationsübergreifende Optimierung der gesamten Prozesskette.

Die Struktur der Fallstudie orientiert sich am Vorgehensmodell zur Gestaltung von Prozessketten (siehe Kap. 1). Basierend auf dem PRK-Screening der IST-Prozesskette, werden im Rahmen des PRK-Scopings die relevanten Ziele für die Prozesskette "private Immobilienfinanzierung" ausgewählt. Diese Ziele werden auf Basis von Expertinnen- und Experteneinschätzungen priorisiert und dienen als Basis zur Gestaltung der SOLL-Prozesskette. Die Gestaltung der SOLL-Prozesskette erfolgt durch den Einsatz des PRK-Bauplans. Im Abschließenden Teil der Fallstudie erfolgt die Ableitung von Handlungsempfehlungen zur Verbesserung der Prozesskette im Hinblick auf die Zielerreichung und zur Optimierung der organisationsübergreifenden Prozesskettengestaltung.

Die im nachfolgenden illustrierte Prozesskette beschreibt die einzelnen Teilprozesse und Aufgaben, die gewöhnlich zur Gewährung einer Immobilienfinanzierung an einer Privatkundin oder eines Privatkunden in einer Universalbank anfallen. Der Prozess beginnt mit der Beratung von Kundinnen und Kunden. Er endet mit der Herauslegung / Auszahlung des Kredites. Darüber hinaus werden die (Pflege-)Prozesse beschrieben, die im Lebenszyklus einer Immobilienfinanzierung anfallen (können).

Dabei ist vor allem in der Beschreibung des IST-Zustandes auf die Prozesse innerhalb einer Bank fokussiert, da diese Perspektive aktuell zum Management des Prozesses zugrunde gelegt wird.

Die nachstehend aufgeführten Kriterien und Leitlinien, die hier grundsätzlichen Charakter haben sollen, dienen dazu, den Geschäftsprozess zur privaten Immobilienfinanzierung konkret zu definieren. Denn nur dann ist eine

eindeutige Analyse und Vergleichbarkeit und darüber hinaus auch eine zielgerichtete Weiterentwicklung gewährleistet.

Die folgenden Kriterien und Leitlinien können natürlich bankindividuell unterschiedlich sein:

Kriterien

- Das maximale Finanzierungsvolumen (pro Einzelgeschäft) ist definiert auf der bankindividuellen Risikotragfähigkeit; in der Regel bedient der Prozess das nicht-risikorelevante Geschäft
- Das maximale Finanzierungsvolumen berücksichtigt die bankindividuellen Betragsgrenzen, die für Immobilienfinanzierungen im Rahmen eines Gesamtengagements gelten
- Über diesen Prozess wird die Immobilienfinanzierung für das Kundensegment Privatkunden (Einzelkunden / Gemeinschaftskunden) dargestellt

Leitlinien

- Der Prozessablauf entspricht den gesetzlichen / prüfungsrechtlichen Vorschriften
- Eine fallabschließende Bearbeitung während des Gesprächs mit Kundinnen und Kunden ist gewährleistet; Kundinnen und Kunden erhalten im Minimum die (mündliche) Kreditzusage
- Die Kreditentscheidung erfolgt in Einzelkompetenz der Berater Markt
- Die Verwaltungsaufgaben / die Vertragserstellung werden durch die Kreditsachbearbeiterinnen und Kreditsachbearbeiter Marktfolge durchgeführt
- Für die Objektbewertung wird ein "vereinfachtes Verfahren" herangezogen (d. h. Bewertung erfolgt anhand eines Kriterienkatalogs durch Bankmitarbeiterin oder Bankmitarbeiter; es wird kein "Baugutachten" z. B. durch Architekten erstellt)

7.1 Die IST-Prozesskette

Das nachfolgende Prinzipbild verdeutlicht die einzelnen Phasen des Lebenszyklus der Prozesskette "private Immobilienfinanzierung" im IST (siehe Abbildung 46). Dabei illustriert die Abbildung einerseits den bankinternen Prozess und stellt darüber hinaus auch die B2G-Schnittstellen dar, welche die Prozesskette gewöhnlich durchläuft.

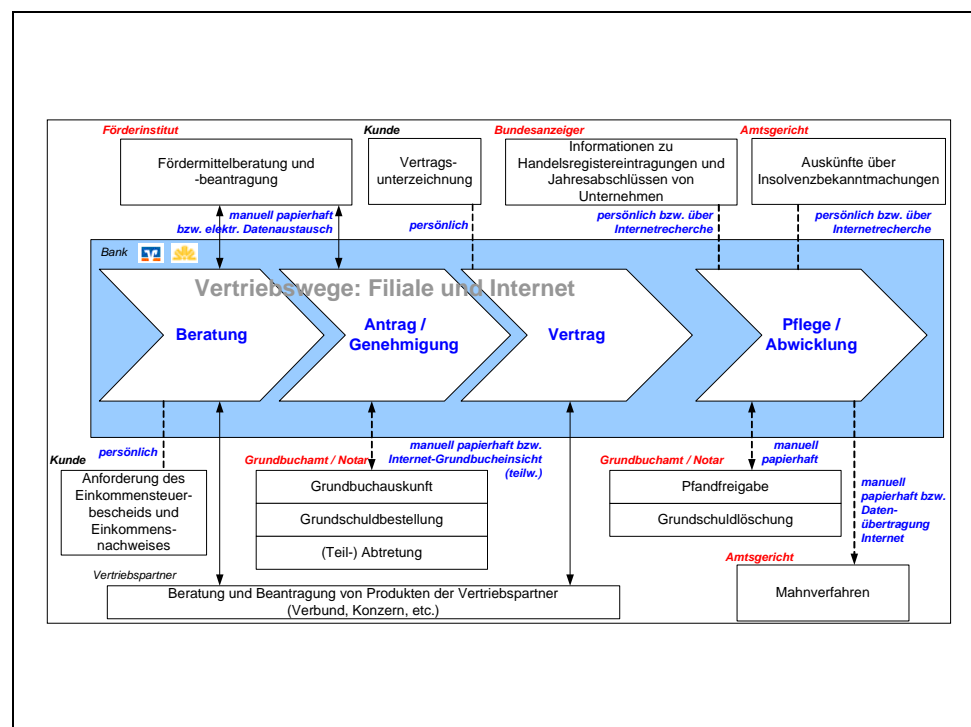


Abbildung 46: IMMO IST-Situation Lebenszyklus Kreditbearbeitung (Quelle: Eigene Darstellung)

Im Rahmen der Prozesskette zur privaten Immobilienfinanzierung bestehen zahlreiche Schnittstellen zu Einrichtungen der öffentlichen Verwaltung und weiteren Partnerorganisationen von Banken. Aus diesem Grund werden folgende Prozessbeteiligte in der Analyse zur IST-Situation mit einbezogen:

Kundin und Kunde, Bank, Förderinstitut, Finanzamt, Grundbuchamt, Amtsgericht, Notare, Insolvenzgericht, Bundesanzeiger sowie die Vertriebspartner der Banken (z. B. angeschlossenen Bausparkassen, Versicherungen etc.).

Des Weiteren zeigt die Abbildung 46, dass im Rahmen der Prozesskette zahlreiche Medienbrüche und Schnittstellenproblematiken auftreten. Diese Schnittstellenprobleme treten insbesondere bei der Interaktion der Bank mit

Kundinnen und Kunden, Förderinstituten, Grundbuchämtern und Notariaten als auch bei den Amtsgerichten und dem Bundesanzeiger auf.

Das Handling und die Überbrückung dieser Medienbrüche wird im Kap. 7.3 detaillierter untersucht und entsprechende Lösungen dazu vorgestellt.

Die folgenden Abbildungen verdeutlichen nochmals die gesamte IST-Prozesskette, sowohl bei einer Kreditvergabe als Neugeschäft, als auch die Prozesskette, welche während der Laufzeit einer privaten Immobilienfinanzierung durchlaufen wird (Pflegeprozesse).¹³ Im Vordergrund der Darstellungen stehen hier die einzelnen Akteure mit den ihr zugeordneten Aufgaben und das Ausmaß in dem die Prozesse durch die Anzahl der Schnittstellen mit Übergabe-, Transport- und Einarbeitungsunterbrechungen betroffen sind. In der Regel sind diese Schnittstellen auch dadurch gekennzeichnet, dass bei der Ergebnisübergabe zwischen den Akteuren Medienbrüche zu verzeichnen sind. Die Prozesskette wird dabei als Prozess Flussdiagramm dargestellt, dem eine akteursbezogene Perspektive zugrunde liegt. Diese Methode hat den Vorteil, dass die Schnittstellen zwischen den unterschiedlichen Akteuren innerhalb der Prozesskette sehr gut dargestellt werden können (siehe Abbildung 47 bis Abbildung 51).

¹³ Im Rahmen der Fallstudie wird die Prozesskette anhand von Process Charts, UML Diagrammen und Process Support Maps modelliert.

Neugeschäftsprozess

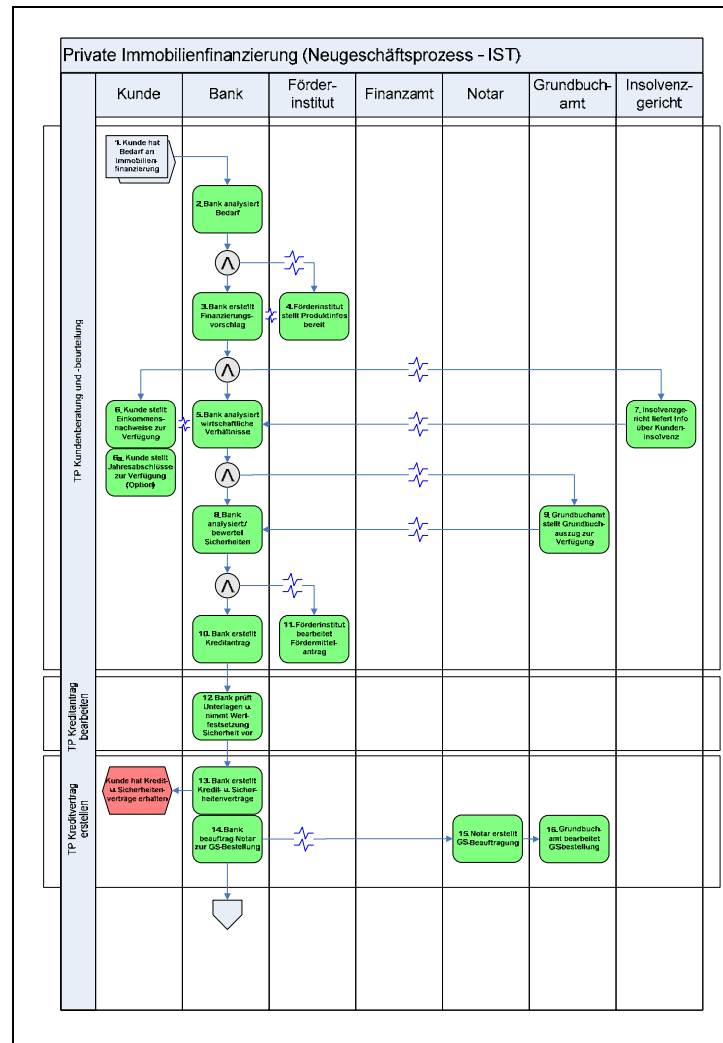


Abbildung 47: IMMO IST-Prozesskette Immobilienfinanzierung Neugeschäft (I) (Quelle: Eigene Darstellung)

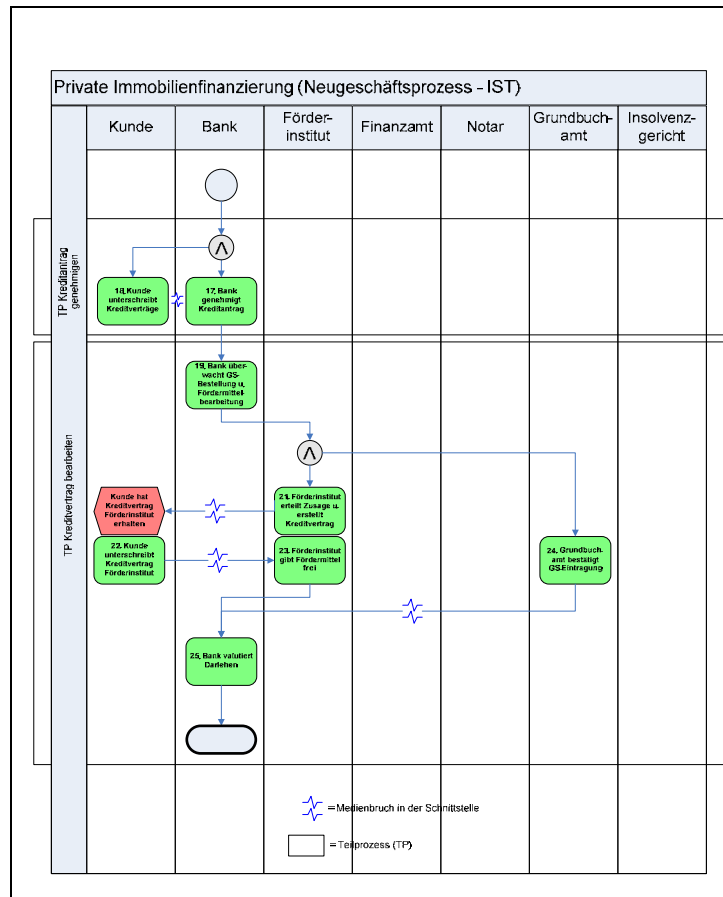


Abbildung 48: IMMO IST-Prozesskette Immobilienfinanzierung Neugeschäft (II) (Quelle: Eigene Darstellung)

Pflegeprozesse

Bei der Variante des Pflegeprozesses sind die unterschiedlichen Akteure wie folgt in den Prozess mit einbezogen:

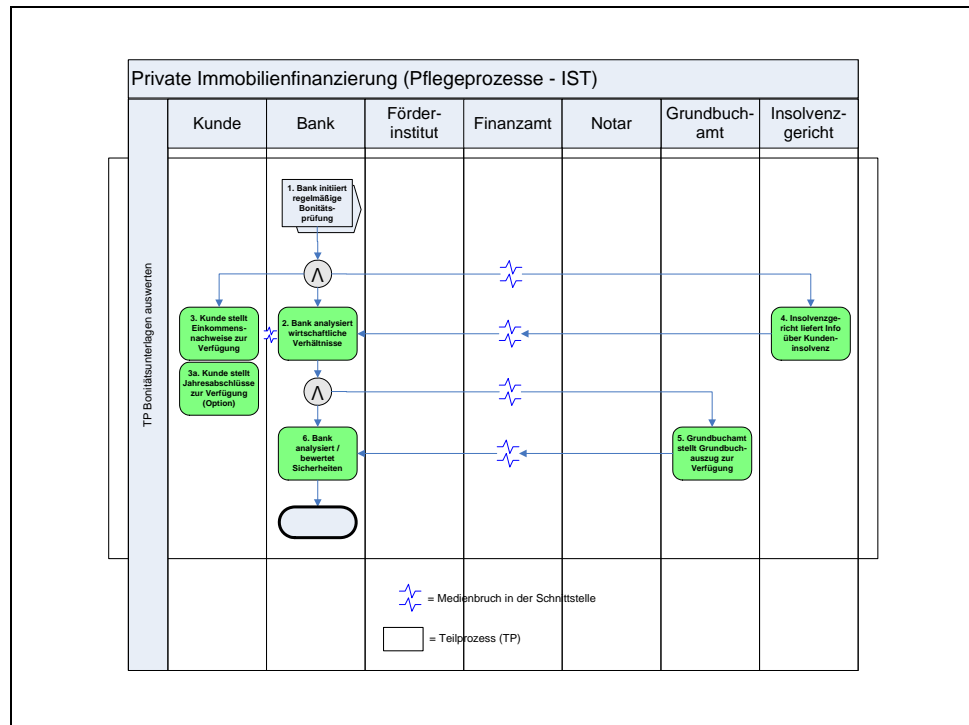


Abbildung 49: IMMO IST-Prozesskette Immobilienfinanzierung Pflege (Quelle: Eigene Darstellung)

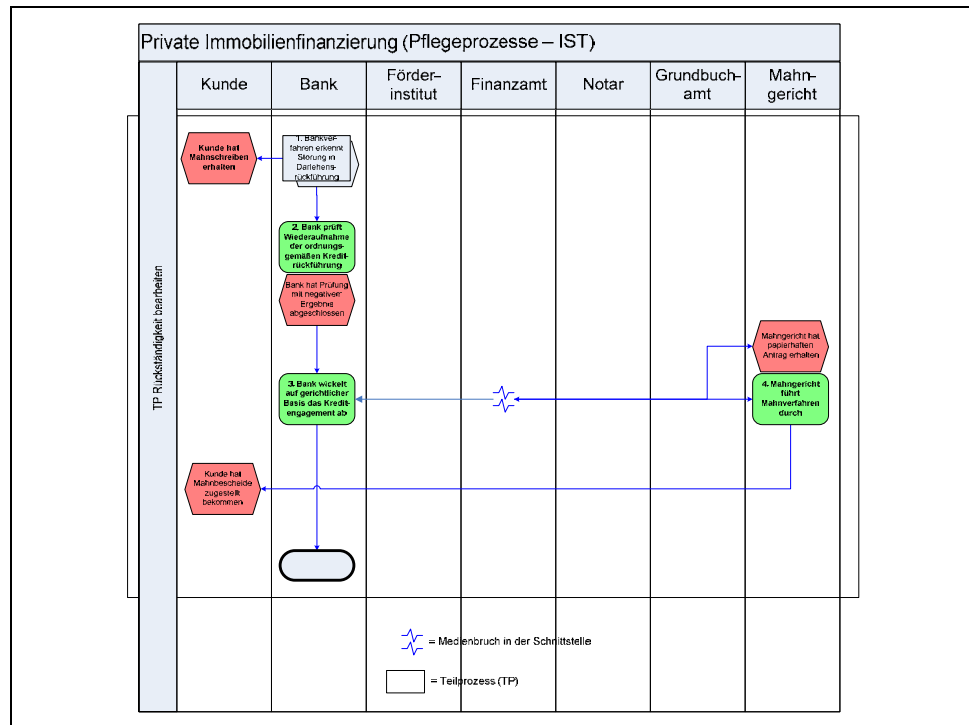


Abbildung 50: IMMO IST-Prozesskette Immobilienfinanzierung Pflege Rückständigkeit (Quelle: Eigene Darstellung)

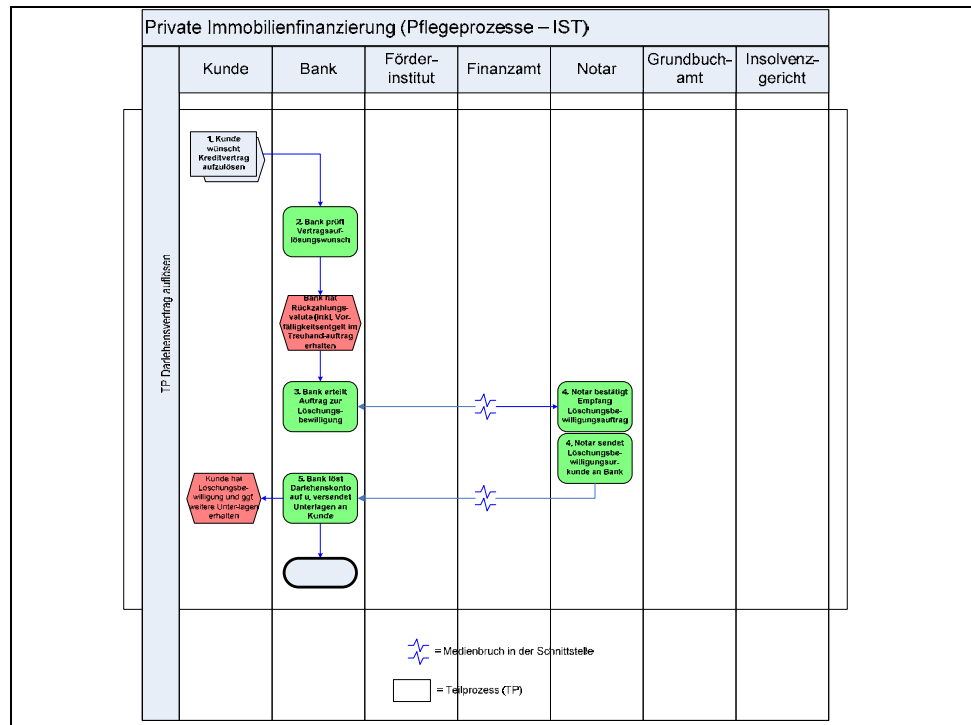


Abbildung 51: IMMO IST-Prozesskette Immobilienfinanzierung Pflege Vertragsauflösung (Quelle: Eigene Darstellung)

7.1.1 Wirtschaftliche, prozessuale und organisatorische Beschreibung und Analyse

Die Prozesskette "Private Immobilienfinanzierung" mit ihren Teilprozessen

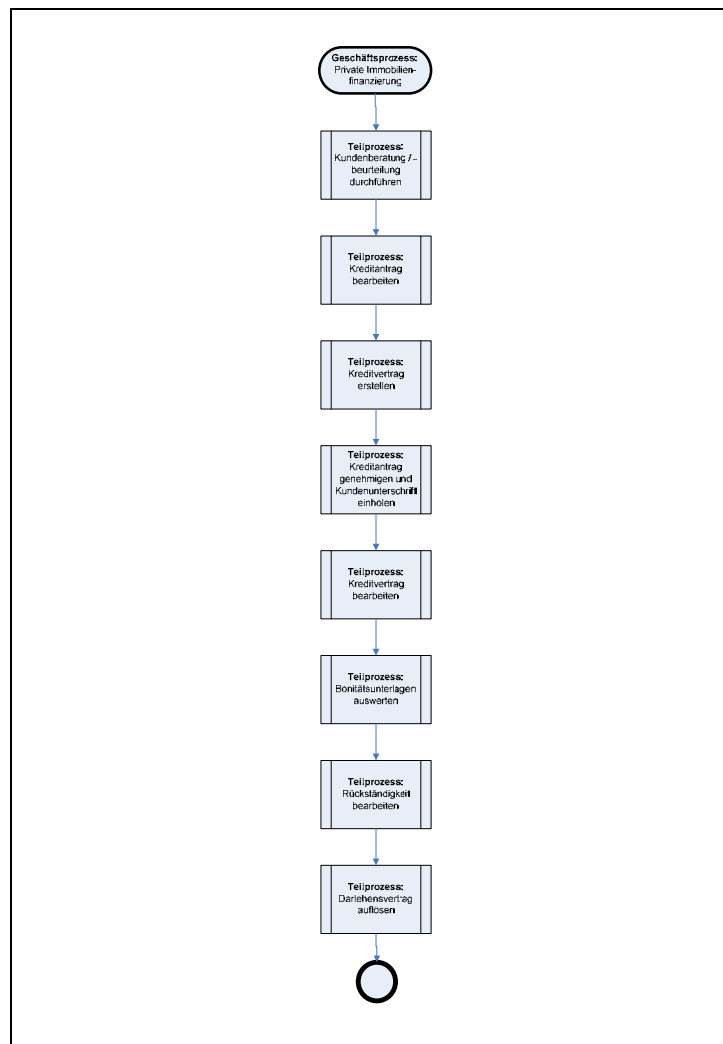


Abbildung 52: IMMO Überblick Prozesskette Immobilienfinanzierung mit Teilprozessen (Quelle: GAD eG)

Die in ihren Teilprozessen beschriebene Prozesskette "Private Immobilienfinanzierung" im IST, stellt bereits den Ablauf in optimierter Form dar, d. h. die Beschreibungen im Kap. 7.3 zur Prozesskette Level-1 (= SOLL) basieren demnach auf dem IST-Geschäftsprozess. Dies bedeutet jedoch auch, dass die Optimierung der Prozesskette bisher lediglich bankintern stattgefunden

hat. Eine Optimierung der gesamten Prozesskette hat aufgrund von organisatorischen, technischen und juristischen Herausforderungen noch nicht stattgefunden. Daher zeigt diese Prozesskette, das Potenzial auf, welches durch die Optimierung der einzelnen Prozesse zwischen verschiedenen Organisationen erschlossen werden kann.

Die Prozesskette "Private Immobilienfinanzierung" beinhaltet die Finanzierung einer überwiegend privat genutzten Immobilie. Dies kann z. B. ein Einfamilienhaus oder eine Eigentumswohnung sein, welches durch eine natürliche Person finanziert wird. Der Prozessauslöser ist der Wunsch von Kundinnen und Kunden, eine Immobilie zu kaufen oder zu bauen, welche ganz oder teilweise durch die Bank finanziert werden soll. Das primäre Ziel der Prozesskette ist in einem ersten Schritt die Auszahlung des Darlehensbetrages an Kunden, in einem zweiten Schritt die Auflösung des Darlehensvertrages durch Rückzahlung der Schuld.

Die Prozesskette "Private Immobilienfinanzierung" besteht aus einer Vielzahl von Teilprozessen, die durch mehrere Prozessbeteiligte und Aufgabenträger ausgeführt werden. Der Hauptprozess der "Privaten Immobilienfinanzierung" besteht aus den Teilprozessen "Kreditberatung und Kreditbeurteilung durchführen", "Kreditantrag bearbeiten", "Kreditvertrag erstellen", "Kreditantrag genehmigen und Kundenunterschrift einholen" und "Kreditvertrag bearbeiten". Die Teilprozesse "Bonitätsunterlagen auswerten", "Rückständigkeit bearbeiten" und "Darlehensvertrag auflösen sind Pflegeprozesse, die während der Laufzeit eines Darlehensvertrages anfallen bzw. anfallen können.

Die Komplexität der Prozesskette "Private Immobilienfinanzierung", welche maßgeblich durch das Risikopotenzial determiniert wird, ist in der Realität in unterschiedlichen Ausprägungsformen vorhanden. Nichtrisikorelevante Fälle (gemäß den Mindestanforderungen an das Risikomanagement – MaRisk) können in Einzelkompetenz des Marktes entschieden bzw. genehmigt werden. Risikorelevante Fälle werden über einen komplexeren, qualifizierteren Prozess abgebildet. Dargestellt wird hier der einfache Prozess, der sich insbesondere durch die Einzelkompetenz im Markt auszeichnet.

Die in diesem Prozess einzureichenden Unterlagen erstrecken sich im Wesentlichen auf die drei Oberbegriffe

- Persönliche Unterlagen
- Objektunterlagen
- Sonstige Unterlagen, falls eine weitere Sicherheit gestellt werden soll.

Prozessbezeichnung [Objekt / Verrichtung]	Private Immobilienfinanzierung durchführen
Kurzbeschreibung [wesentliche Kernpunkte / Aufgaben und Rahmenbedingungen]	Der Prozess Private Immobilienfinanzierung beinhaltet die Finanzierung einer überwiegend privat genutzten Immobilie, wie ein Einfamilienhaus oder Eigentumswohnung, durch eine natürliche Person.
Prozessauslöser [Bezeichnung des Ereignisses, das den Prozess auslöst]	Wunsch von Kundinnen oder Kunden, eine Immobilie zu kaufen oder zu bauen, welches teilweise / bzw. ganz durch die Bank finanziert werden soll.
Prozessziel / Prozessergebnis [Beschreibung, welcher Zustand zu erreichen ist]	Auszahlung des Darlehensbetrages an Kundinnen oder Kunden
Prozesszuständigkeit [Aufgabenträger für die operative Durchführung des Prozesses]	Mehrere Akteure: Finanzierungsberaterinnen und Finanzberater, Kreditsachbearbeiterinnen und Kreditsachbearbeiter Marktfolge
Mitgeltende Unterlagen [zu berücksichtigende Informationen]	Informationen zum Objekt, Besicherungsunterlagen, Persönliche Unterlagen.
Prozessvoraussetzungen [fachlich, nicht IT-]	

bezogen]	
Schnittstellen / Abhängigkeiten [zu anderen Prozessen; Gründe: gesetzliche / organisatorische Anforderungen; Hol- oder Bringschuld]	
Medien / Medienbrüche [Darstellung der im Prozessverlauf verwendeten Medien]	Bilaterales Gespräch der Kundinnen oder Kunden mit Beraterinnen und Beratern, elektronische Weitergabe der Daten zu Kreditsachbearbeiterinnen und Kreditsachbearbeitern
Durchlaufzeit [pro Vorgang]	Keine Angabe
Häufigkeit des Prozessdurchlaufs [pro Zeiteinheit]	Keine Angabe

Tabelle 9: Systematische Beschreibung der PRK IMMO im Überblick

Teilprozess "Kundenberatung und -beurteilung durchführen"

Der Teilprozess "Kundenberatung und -beurteilung durchführen" beinhaltet die Beratung von Kundinnen oder Kunden über die Finanzierung einer privat genutzten Immobilie. Zusätzlich zur Beratung werden Kundinnen und Kunden hinsichtlich ihrer Bonität beurteilt, um hier eine Kreditwürdigkeit festzustellen (siehe Abbildung 53).

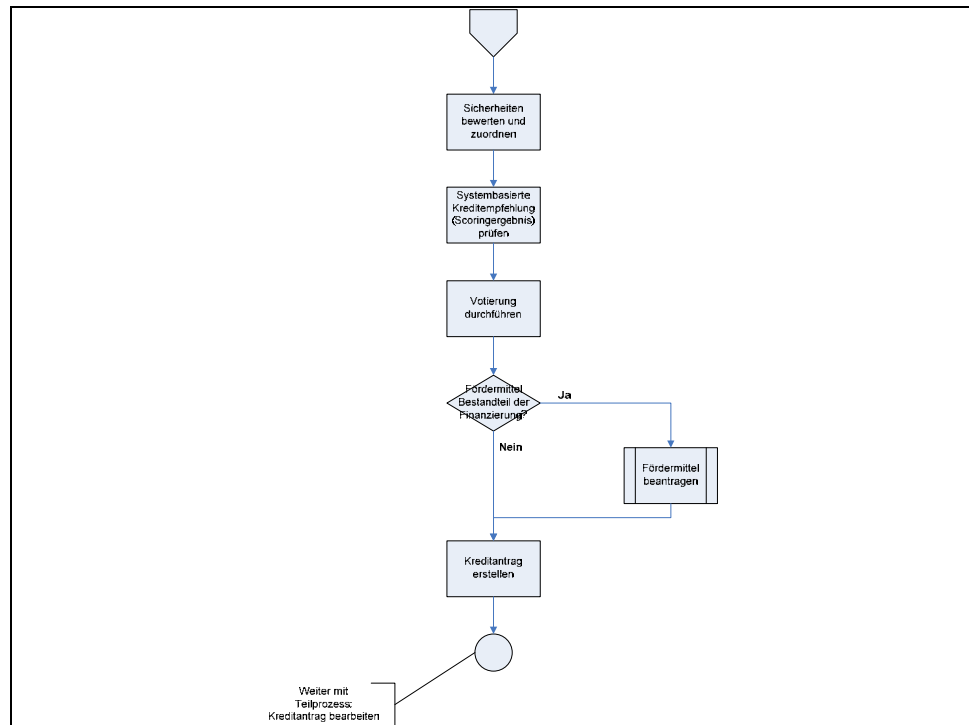


Abbildung 53: IMMO Teilprozess Kundenberatung (Quelle: GAD eG)

In einem ersten Schritt ist der Bedarf zu ermitteln, der insgesamt für die Finanzierung der Immobilie aufgebracht werden muss. Das Ziel dieser Analyse ist die Ermittlung der Finanzierungshöhe, um eine geeignete Finanzierung aufsetzen zu können. Hierbei ist zu prüfen, welche Finanzierungsmittel eingesetzt werden können, hier insbesondere die Möglichkeit der Zuhilfenahme von öffentlichen Förderprogrammen.

In einem zweiten Schritt sind die kundenbezogenen Daten durch das bilaterale Gespräch der Kundinnen oder Kunden mit Beraterinnen und Beratern zu ermitteln. Neben der Anlage bzw. Aktualisierung des Kundenstamms ist die Einholung von externen Auskünften erforderlich, um das interne Kundenbild durch externe Informationen zu prüfen bzw. anzureichern (SCHUFA, evtl. Handelsregisterinformationen, wenn Kunden Gesellschafter eines Unternehmens ist). An dieser Stelle ist die erste organisationsübergreifende Schnittstelle zwischen der Bank als Institution und der externen Auskunftsstelle im Rahmen der Prozesskette erreicht.

Um Aussagen zur Bonität von Kundinnen oder Kunden ableiten zu können, ist neben einer Aufstellung des Vermögens und der Schulden auch die Berechnung des Kapitaldienstes unerlässlich. Durch die Bewertung und Zuord-

nung von Sicherheiten zum Finanzierungsvorhaben sind Beraterinnen und Berater in der Lage, ein erstes Votum abzugeben, ob die gewünschte Kreditvergabe durchgeführt werden kann. Falls dieses Votum positiv ist, können die Informationen in die Marktfolge, evtl. auch zum Förderinstitut, weitergeleitet werden, um eine detaillierte Prüfung der Kundinnen oder Kunden - und Objektunterlagen ausführen zu können.

Neben der Erlangung der Weiterbearbeitungsreife durch die Marktfolge ist auch die Abgabe eines Kundenangebotes ein Ergebnis des Teilprozesses "Kundenberatung und -beurteilung durchführen".

Prozessbezeichnung [Objekt / Verrichtung]	Kundenberatung und -beurteilung durchführen
Kurzbeschreibung [wesentliche Kernpunkte / Aufgaben und Rahmenbedingungen]	Der Teilprozess Kundenberatung und -beurteilung beinhaltet die Beratung der Kundinnen und Kunden über die Finanzierung einer privat genutzten Immobilie, inklusive der anschließenden Beurteilung von Kunden, ob dieser kreditwürdig ist.
Prozessauslöser [Bezeichnung des Ereignisses, das den Prozess auslöst]	Wunsch von Kunden, eine Immobilie zu kaufen oder zu bauen, welches teilweise / bzw. ganz durch die Bank finanziert werden soll.
Prozessziel / Prozessergebnis [Beschreibung, welcher Zustand zu erreichen ist]	Abschluss der Beratung in Form eines konkreten Angebotes und Herstellung der Reife dieser Beratung für eine Übergabe in die Kreditsachbearbeitung.
Prozesszuständigkeit [Aufgabenträger für die operative Durchführung des Prozesses]	Beratung Markt
Mitgeltende Unterlagen	Informationen zum Objekt, Besicherungsunterlagen, Persönliche Unterla-

[zu berücksichtigende Informationen]	gen.
Prozessvoraussetzungen [fachlich, nicht IT-bezogen]	
Schnittstellen / Abhängigkeiten [zu anderen Prozessen; Gründe: gesetzliche / organisatorische Anforderungen; Hol- oder Bringschuld]	"Kreditantrag bearbeiten"
Medien / Medienbrüche [Darstellung der im Prozessverlauf verwendeten Medien]	Bilaterales Gespräch der Kundinnen oder Kunden mit Beraterinnen und Beratern, Eingabe der Beratungsdaten in das Bankenverfahren. Einsicht ins Handelsregister muss über das Internet erfolgen.
Durchlaufzeit [pro Vorgang]	Keine Angabe
Häufigkeit des Prozessdurchlaufs [pro Zeiteinheit]	Keine Angabe

Tabelle 10: Systematische Beschreibung TP "Kundenberatung und –bewertung"

Teilprozess "Kreditantrag bearbeiten"

Nach Abschluss der Kreditberatung erfolgt eine detaillierte Prüfung und Aufarbeitung der Kundeninformationen und der Objektunterlagen durch Mitarbeiterinnen und Mitarbeiter in der Marktfolge der Bank (siehe Abbildung 54).

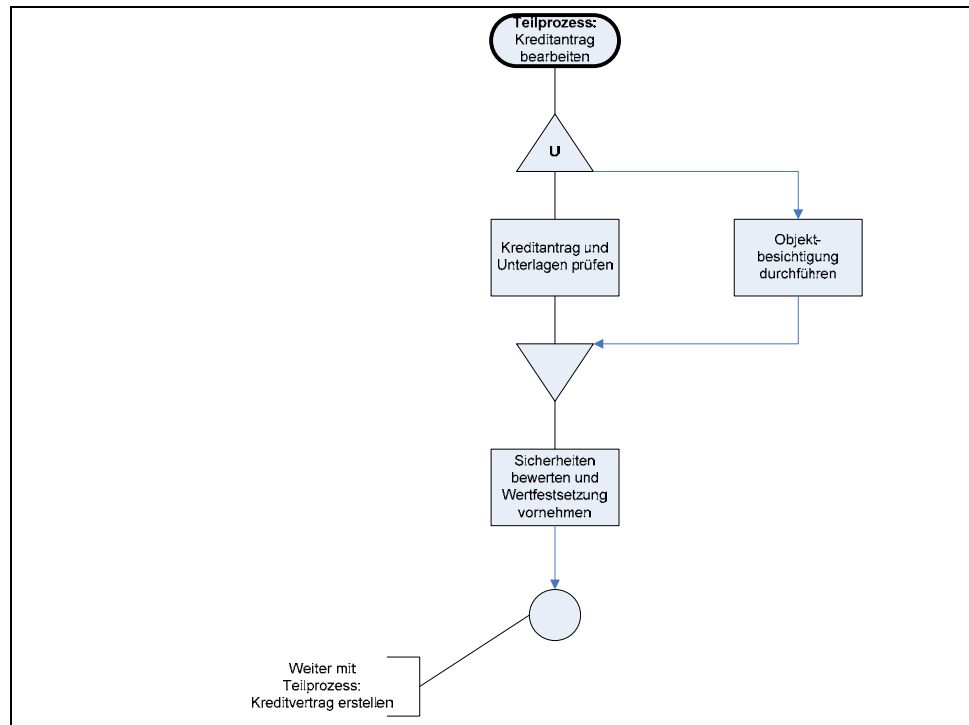


Abbildung 54: IMMO Teilprozess Kreditantrag (Quelle: GAD eG)

Die entsprechenden Finanzierungsdaten werden im Banksystem gepflegt bzw. ergänzt. Das zu finanzierende Objekt wird erfasst. Ggf. ist hier eine Objektbesichtigung vorangegangen. Diese kann durch Dritte durchgeführt worden sein. Die Sicherheiten werden erfasst und es erfolgt eine Wertermittlung des Objektes. Nach Aufarbeitung der Personen- und Objektdaten ist die Voraussetzung für die Erstellung der Kredit- und Sicherheitenverträge gegeben.

Prozessbezeichnung [Objekt / Verrichtung]	Kreditantrag bearbeiten
Kurzbeschreibung [wesentliche Kernpunkte / Aufgaben und Rahmenbedingungen]	Der Teilprozess Kreditbeantragung beinhaltet die Prüfung und die Bewertung des Kreditantrages und der Sicherheiten, inkl. einer etwaigen Objektbesichtigung.
Prozessauslöser	Die Beratung ist abgeschlossen, Kundinnen oder Kunden haben sich für das An-

[Bezeichnung des Ereignisses, das den Prozess auslöst]	gebot positiv entschieden.
Prozessziel / Prozessergebnis [Beschreibung, welcher Zustand zu erreichen ist]	Alle relevanten Personen- und Objektdaten sind gepflegt, so dass ein Vertrag erstellt werden kann.
Prozesszuständigkeit [Aufgabenträger für die operative Durchführung des Prozesses]	Beratung Markt
Mitgeltende Unterlagen [zu berücksichtigende Informationen]	Informationen zum Objekt, Besichtigungsunterlagen, Persönliche Unterlagen.
Prozessvoraussetzungen [fachlich, nicht IT-bezogen]	
Schnittstellen / Abhängigkeiten [zu anderen Prozessen; Gründe: gesetzliche / organisatorische Anforderungen; Hol- oder Bringschuld]	"Kundenberatung und –beurteilung durchführen" "Kreditvertrag erstellen"
Medien / Medienbrüche [Darstellung der im Prozessverlauf verwendeten Medien]	Überarbeitung und Ergänzung der Finanzierungsdaten im Bankenverfahren. Daten wurden aus dem TP "Kundenberatung und –beurteilung durchführen" übernommen und stehen zur weiteren Bearbeitung bereit. Die Objektbesichtigung erfolgt durch eine

	Mitarbeiterin oder einen Mitarbeiter.
Durchlaufzeit [pro Vorgang]	Keine Angabe
Häufigkeit des Prozess- durchlaufs [pro Zeiteinheit]	Keine Angabe

Tabelle 11: Systematische Beschreibung des TP "Kreditantrag bearbeiten"

Teilprozess "Kreditvertrag erstellen"

Nach Aufbereitung der Kundinnen- oder Kundendaten sowie Objektdaten erfolgt die Erstellung der Sicherheiten- und Kreditverträge. Die Verträge werden durch die Systemeingaben befüllt und können gedruckt werden (siehe Abbildung 55).

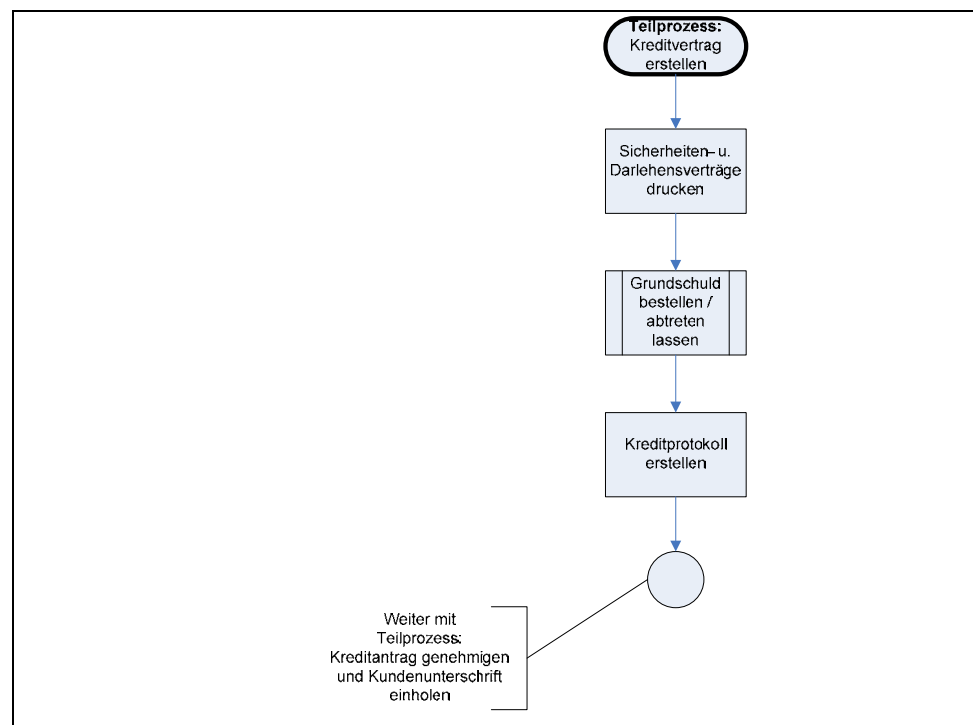


Abbildung 55: IMMO Teilprozess Kreditvertrag (Quelle: GAD eG)

Um eine valide Kreditgenehmigung durch den Markt zu erreichen, sind entsprechende Voraussetzungen zu erfüllen. Hier ist insbesondere die Bestellung bzw. die Abtretung der Grundschuld zu nennen, die heute manuell bestellt bzw. beantragt werden muss. Daneben wird durch das System in komprimierter Form ein Kreditprotokoll erstellt, welches die Basis für die Kreditentscheidung ist. Der Inhalt des Kreditprotokolls setzt sich aus den bereits vorhandenen und den zu beantragenden Finanzierungen, den Objekt-, den Sicherheiten-, den Vermögens- und den Kundendaten zusammen.

Prozessbezeichnung [Objekt / Verrichtung]	Kreditvertrag erstellen
Kurzbeschreibung [wesentliche Kernpunkte / Aufgaben und Rahmenbedingungen]	Der Teilprozess beinhaltet den Druck der Kredit- und Sicherheitenverträge und die Vorbereitung des Kreditantrages für eine Kreditgenehmigung.
Prozessauslöser [Bezeichnung des Ereignisses, das den Prozess auslöst]	Die Kreditbeantragung ist abgeschlossen, der Kredit kann grundsätzlich vergeben werden.
Prozessziel / Prozessergebnis [Beschreibung, welcher Zustand zu erreichen ist]	Die Verträge sind gedruckt und liegen zur Unterschrift bereit.
Prozesszuständigkeit [Aufgabenträger für die operative Durchführung des Prozesses]	Sachbearbeitung Marktfolge
Mitgeltende Unterlagen [zu berücksichtigende Informationen]	Kredit- und Sicherheitenverträge

Prozessvoraussetzungen [fachlich, nicht IT-bezogen]	
Schnittstellen / Abhängigkeiten [zu anderen Prozessen; Gründe: gesetzliche / organisatorische Anforderungen; Hol- oder Bringschuld]	"Kreditantrag bearbeiten" "Kreditantrag genehmigen und Kundenunterschrift einholen"
Medien / Medienbrüche [Darstellung der im Prozessverlauf verwendeten Medien]	Medienbruch bei der Bestellung oder Abtretung einer Grundschuld.
Durchlaufzeit [pro Vorgang]	Keine Angabe
Häufigkeit des Prozessdurchlaufs [pro Zeiteinheit]	Keine Angabe

Tabelle 12: Systematische Beschreibung des TP "Kreditvertrag erstellen"

Teilprozess "Kreditantrag genehmigen und Kundenunterschrift einholen"

Auf Basis des Kreditprotokolls wird nun die Kreditgenehmigung durch die Beraterinnen und Berater geprüft und erteilt (siehe Abbildung 56).

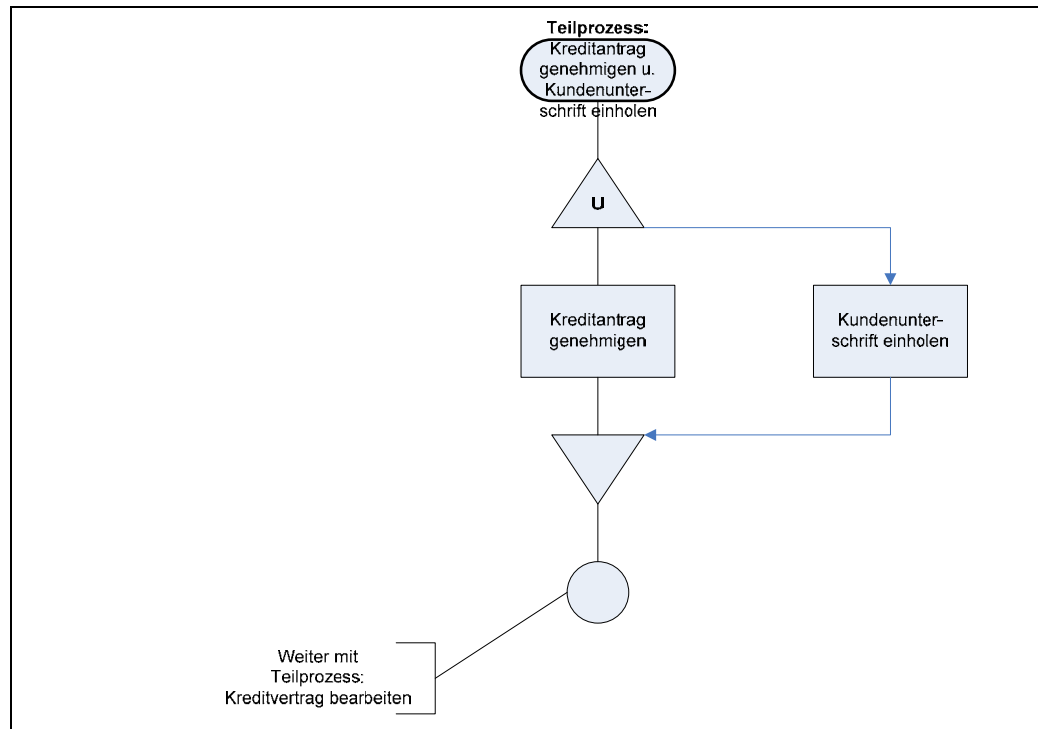


Abbildung 56: IMMO Teilprozess Kreditgenehmigung (Quelle: GAD eG)

Neben der qualifizierten Prüfung der Finanzierung ist ebenfalls die Überprüfung der erforderlichen Unterlagen notwendig. Hier ist insbesondere nochmals die persönlichen Unterlagen (Selbstauskunft, Gehaltsnachweise, Versicherungsnachweise, Personalausweis, etc.) und die Objektunterlagen (Baupläne, Wohnflächenberechnung, Versicherungsnachweise, Grundbuchauszug, Objektfotos, Kaufvertrag, etc.) zu nennen.

Falls alle Voraussetzungen erfüllt sind, kann die Mitarbeiterin oder der Mitarbeiter die (technische) Genehmigung erteilen und die Kundenunterschrift einholen. Diese Unterschrift erfolgt vor den Augen der Beraterin oder des Beraters. Dieser Schritt erfordert die Anwesenheit der Kundin oder des Kunden in der Bank und stellt somit eine weitere Schnittstelle dar, welche die Bank im Rahmen des Prozesskettenmanagements zu berücksichtigen hat.

Prozessbezeichnung [Objekt / Verrichtung]	Kreditantrag genehmigen und Kundenunterschrift einholen
Kurzbeschreibung	Der Teilprozess beinhaltet die Kreditgenehmigung und die Einholung der Unter-

[wesentliche Kernpunkte / Aufgaben und Rahmenbedingungen]	schrift der Kundin oder des Kunden.
Prozessauslöser [Bezeichnung des Ereignisses, das den Prozess auslöst]	Die Kreditverträge sind erstellt und alle Daten bzw. Informationen zur Finanzierung liegen der Bank vor.
Prozessziel / Prozessergebnis [Beschreibung, welcher Zustand zu erreichen ist]	Die Verträge sind von Kundin oder Kunde zu unterschrieben.
Prozesszuständigkeit [Aufgabenträger für die operative Durchführung des Prozesses]	Beratung Markt
Mitgeltende Unterlagen [zu berücksichtigende Informationen]	Kredit- und Sicherheitenverträge
Prozessvoraussetzungen [fachlich, nicht IT-bezogen]	
Schnittstellen / Abhängigkeiten [zu anderen Prozessen; Gründe: gesetzliche / organisatorische Anforderungen; Hol- oder Bringschuld]	"Kreditvertrag erstellen" "Kreditvertrag bearbeiten"

<p>Medien / Medienbrüche</p> <p>[Darstellung der im Prozessverlauf verwendeten Medien]</p>	<p>Die Unterschrift der Kundin oder des Kunden erfolgt manuell vor den Augen der Bankmitarbeiterin oder des Bankmitarbeiters.</p>
<p>Durchlaufzeit</p> <p>[pro Vorgang]</p>	<p>Keine Angabe</p>
<p>Häufigkeit des Prozessdurchlaufs</p> <p>[pro Zeiteinheit]</p>	<p>Keine Angabe</p>

Tabelle 13: Systematische Beschreibung des TP "Kreditantrag genehmigen und Kundenunterschrift einholen"

Teilprozess "Kreditvertrag bearbeiten"

Nach Genehmigung und Kundenunterschrift werden nochmals die Darlehensverträge in der Marktfolge geprüft und die entsprechenden Darlehenskonten im Bankverfahren angelegt (siehe Abbildung 57).

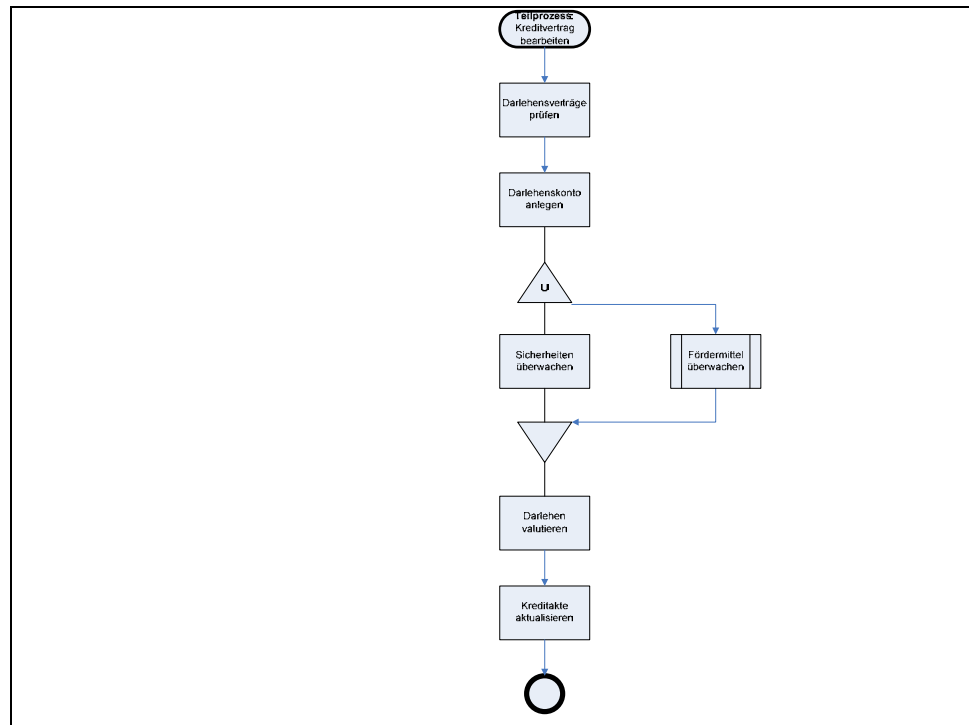


Abbildung 57: IMMO Teilprozess Kreditabschluss (Quelle: GAD eG)

Bevor die Valutierung durchgeführt werden kann, ist eine genaue Prüfung der Auszahlungsvoraussetzungen durchzuführen. Sind alle Unterlagen eingereicht? Ist die Fälligkeit des Kaufpreises erreicht? Ist die Sicherheitenstellung rechtlich gegeben und erfolgt?

Sind diese Auszahlungsvoraussetzungen erfüllt, kann der Darlehensbetrag valutiert werden. Die Unterlagen werden archiviert und die Kreditakte aktualisiert. Damit ist der Hauptprozess der Kreditvergabe beendet.

Prozessbezeichnung [Objekt / Verrichtung]	Kreditvertrag bearbeiten
Kurzbeschreibung [wesentliche Kernpunkte / Aufgaben und Rahmenbedingungen]	Der Teilprozess beinhaltet die Prüfung der Darlehensvereinbarungen (insb. der Sicherheitenstellung) und die Darlehensauszahlung.

<p>Prozessauslöser</p> <p>[Bezeichnung des Ereignisses, das den Prozess auslöst]</p>	<p>Die Kundenunterschrift liegt vor.</p>
<p>Prozessziel / Prozessergebnis</p> <p>[Beschreibung, welcher Zustand zu erreichen ist]</p>	<p>Die Darlehenssumme ist ausgezahlt und die Kreditakte (inkl. aller verwendeten Unterlagen) ist archiviert.</p>
<p>Prozesszuständigkeit</p> <p>[Aufgabenträger für die operative Durchführung des Prozesses]</p>	<p>Sachbearbeitung Marktfolge</p>
<p>Mitgeltende Unterlagen</p> <p>[zu berücksichtigende Informationen]</p>	<p>Kredit- und Sicherheitenverträge, Unterlagen zum Objekt, Besicherungsunterlagen, Persönliche Unterlagen.</p>
<p>Prozessvoraussetzungen</p> <p>[fachlich, nicht IT-bezogen]</p>	
<p>Schnittstellen / Abhängigkeiten</p> <p>[zu anderen Prozessen; Gründe: gesetzliche / organisatorische Anforderungen; Hol- oder Bring-schuld]</p>	<p>"Kreditantrag genehmigen und Kundenunterschrift einholen"</p>
<p>Medien / Medienbrüche</p> <p>[Darstellung der im Prozessverlauf verwendeten Medien]</p>	<p>Manuelle Überwachung der Sicherheiten.</p>

Durchlaufzeit [pro Vorgang]	Keine Angabe
Häufigkeit des Prozess- durchlaufs [pro Zeiteinheit]	Keine Angabe

Tabelle 14: Systematische Beschreibung des TP "Kreditvertrag bearbeiten"

Teilprozess "Bonitätsunterlagen auswerten"

Im Rahmen der Darlehenspflege und -überprüfung kann es aus Sicht von Kreditgebern erforderlich sein, die bonitätsmäßige Einschätzung von Kundinnen und Kunden zu aktualisieren (siehe hierzu auch die Bestimmungen des §18 KWG). Zur Prüfung der aktuellen wirtschaftlichen Verhältnisse werden von Kreditnehmerinnen und Kreditnehmern entsprechende Unterlagen, wie Vermögensauswertungen, Einkommensteuerunterlagen, Gehaltsnachweise etc. angefordert. Neben den wirtschaftlichen Verhältnissen kann auch eine Überprüfung der Sicherheitenstellung veranlasst werden. Dies kann bspw. eine Objektbesichtigung nach sich ziehen, die dann zu einer neuen Wertermittlung führt (siehe Abbildung 58).

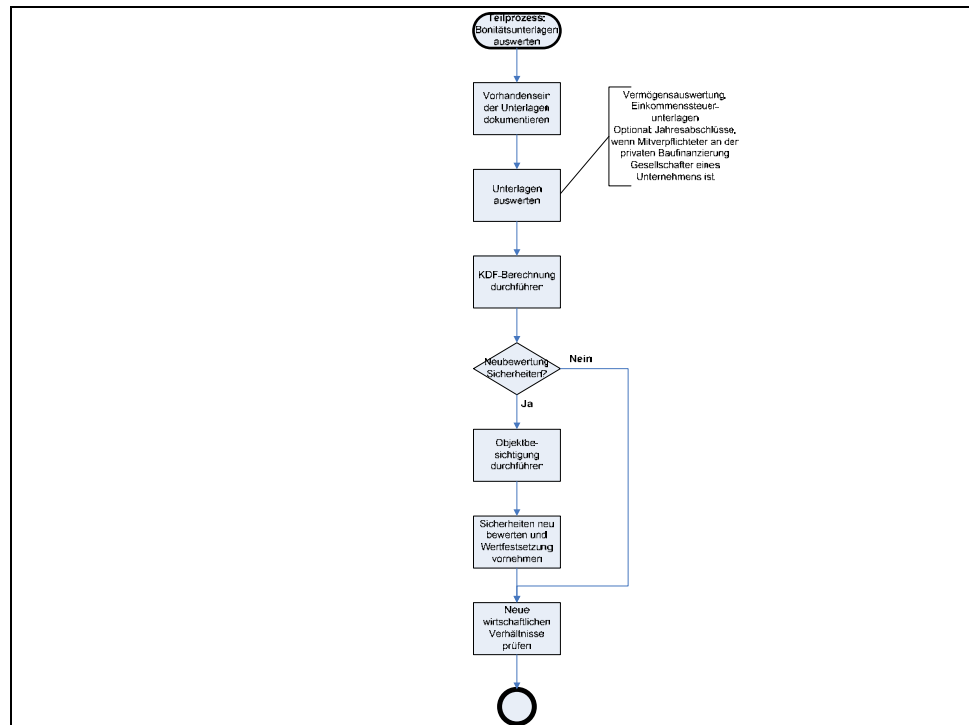


Abbildung 58: IMMO Teilprozess Bonitätsunterlagen (Quelle: GAD eG)

Die angeforderten Unterlagen werden überprüft und im System dokumentiert. Die Analyse dieser Unterlagen erfolgt durch die Sachbearbeitung der Marktfolge und wird im Bankverfahren hinterlegt. Das Ergebnis ist die Aktualisierung der Bonität von Kunden. Dieses neue Ergebnis wird durch die Sachbearbeitung überprüft und kann ggf. aufsetzende Maßnahmen veranlassen (Intensivbetreuung der Kundin oder des Kunden, Sanierung von Kunden, Forderung neuer Sicherheitenstellungen, etc.).

<p>Prozessbezeichnung</p> <p>[Objekt / Verrichtung]</p>	<p>Bonitätsunterlagen auswerten</p>
<p>Kurzbeschreibung</p> <p>[wesentliche Kernpunkte / Aufgaben und Rahmenbedingungen]</p>	<p>Zur Prüfung der aktuellen wirtschaftlichen Verhältnisse werden von Kreditnehmerinnen und Kreditnehmern entsprechende Unterlagen, wie Vermögensauswertungen, Einkommenssteuerunterlagen etc. angefordert und ausgewertet</p>

<p>Prozessauslöser</p> <p>[Bezeichnung des Ereignisses, das den Prozess auslöst]</p>	<p>Eingang der angeforderten Unterlagen</p> <p>Ggf. TP Rückständigkeit bearbeiten</p>
<p>Prozessziel / Prozessergebnis</p> <p>[Beschreibung, welcher Zustand zu erreichen ist]</p>	<p>Die Auswertung der Bonitätsunterlagen gibt Aufschluss über die aktuellen wirtschaftlichen Verhältnisse der Kreditnehmerinnen und Kreditnehmer; sie sind dann Entscheidungsgrundlage für die Fortführung oder die vorzeitige Rückführung / Abwicklung des Kreditverhältnisses</p>
<p>Prozesszuständigkeit</p> <p>[Aufgabenträger für die operative Durchführung des Prozesses]</p>	<p>Kreditsachbearbeiterinnen und Kreditsachbearbeitern Marktfolge / Beraterinnen und Berater Markt</p>
<p>Mitgeltende Unterlagen</p> <p>[zu berücksichtigende Informationen]</p>	<p>Kreditakte; angeforderte Bonitätsunterlagen</p>
<p>Prozessvoraussetzungen</p> <p>[fachlich, nicht IT-bezogen]</p>	<p>Bestehendes Darlehensverhältnis</p>
<p>Schnittstellen / Abhängigkeiten</p> <p>[zu anderen Prozessen; Gründe: gesetzliche / organisatorische Anforderungen; Hol- oder Bringschuld]</p>	<p>Zu Prozess:</p> <ul style="list-style-type: none"> • Anforderungen des Einkommenssteuerbescheides / Grundlage ist § 18 KWG / Bringschuld des Kunden • Optional, wenn Mitverpflichteter Gesellschafter einer Unternehmung ist: Anforderung von Handelsregisterauszügen und Jahresabschlüssen / Grundlage ist § 18 KWG / Bringschuld der Kundin oder des

	Kunden
Medien / Medienbrüche [Darstellung der im Prozessverlauf verwendeten Medien]	Manuelle Anforderung Bonitätsunterlagen
Durchlaufzeit [pro Vorgang]	Keine Angabe
Häufigkeit des Prozessdurchlaufs [pro Zeiteinheit]	Keine Angabe

Tabelle 15: Systematische Beschreibung des TP "Bonitätsunterlagen auswerten"

Teilprozess "Rückständigkeit bearbeiten"

Während der Darlehenslaufzeit kann es zu Zahlungsstörungen von Kreditnehmerinnen und Kreditnehmern kommen. Diese Zahlungsstörungen werden durch das System erkannt und müssen von Beraterinnen und Beratern geprüft und weiter analysiert werden. Der Teilprozess "Rückständigkeit bearbeiten" kann daher auch der Prozessauslöser für den Teilprozess "Bonitätsunterlagen auswerten" sein, um die Bonität von Kunden neu zu analysieren (siehe Abbildung 59).

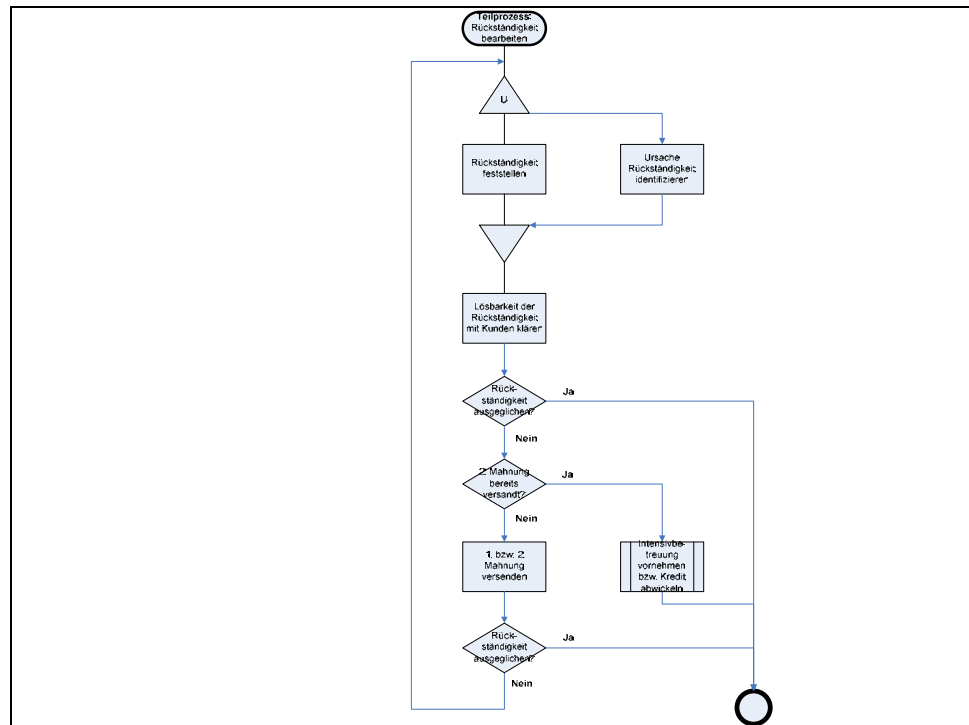


Abbildung 59: IMMO Teilprozess Rückständigkeit (Quelle: GAD eG)

Nach Feststellung der Rückständigkeit nehmen Beraterinnen und Berater Kontakt zu den Kreditnehmerinnen und Kreditnehmern auf und hinterfragen die Gründe für diese Zahlungsstörung. Sind Kundinnen oder Kunden nicht in der Lage, diese Rückständigkeit auszugleichen, erfolgt die erste Mahnung. Reagieren Kundinnen oder Kunden auch nach der ersten Mahnung nicht, kommt es zur zweiten Mahnung. Wenn auch danach die Rückständigkeit nicht ausgeglichen ist, werden Kunde nochmals kontaktiert und es werden Lösungswege diskutiert. Falls auch hier kein Lösungsweg durch Kundinnen oder Kunden aufgezeigt werden kann, wird dieser in die Intensivbetreuung übergeben oder direkt in die Abwicklung übernommen.

Prozessbezeichnung	Rückständigkeit bearbeiten
[Objekt / Verrichtung]	
Kurzbeschreibung	Eine Zahlungsstörung / Rückständigkeit der Kundinnen und Kunden wird erkannt. Sie muss von Beraterinnen und Beratern geprüft und weiter analysiert werden. Ggf. muss ein
[wesentliche Kernpunkte / Aufgaben und Rahmenbe-]	

dingungen]	Mahnverfahren abgestoßen werden.
Prozessauslöser [Bezeichnung des Ereignisses, das den Prozess auslöst]	Rückständigkeit liegt vor
Prozessziel / Prozessergebnis [Beschreibung, welcher Zustand zu erreichen ist]	Rückständigkeit ausgeglichen oder Abwicklung der Kundin oder des Kunden angestoßen.
Prozesszuständigkeit [Aufgabenträger für die operative Durchführung des Prozesses]	Beraterinnen und Berater Markt / Kredit-sachbearbeiterinnen und Kreditsachbearbeiter Marktfolge
Mitgeltende Unterlagen [zu berücksichtigende Informationen]	keine
Prozessvoraussetzungen [fachlich, nicht IT-bezogen]	Das Bankverfahren erkennt automatisch die Rückständigkeit
Schnittstellen / Abhängigkeiten [zu anderen Prozessen; Gründe: gesetzliche / organisatorische Anforderungen; Hol- oder Bring-schuld]	Der Teilprozess "Rückständigkeit bearbeiten" kann der Prozessauslöser für den Teilprozess "Bonitätsunterlagen auswerten" sein, um die Bonität der Kundin oder des Kunden neu zu analysieren. Ferner kann der Prozess Auslöser einer Abwicklung, Sanierung oder Intensivbetreuung der Kundin oder des Kunden sein (gem. MaRisk)
Medien / Medienbrüche [Darstellung der im Prozessverlauf verwendeten	

Medien]	
Durchlaufzeit [pro Vorgang]	Keine Angabe
Häufigkeit des Prozess- durchlaufs [pro Zeiteinheit]	Keine Angabe

Tabelle 16: Systematische Beschreibung des TP "Rückständigkeit bearbeiten"

Teilprozess "Darlehensvertrag auflösen"

Der Teilprozess startet mit dem Wunsch der Kundin oder des Kunden, den Kreditvertrag aufzulösen. Eine Auflösung ist jedoch nur in bestimmten Fällen zulässig:

Kreditnehmerinnen und Kreditnehmer können einen Darlehensvertrag mit veränderlichem Zinssatz jederzeit unter Einhaltung einer Kündigungsfrist von drei Monaten kündigen (§ 489 Abs. 2 BGB). Kreditnehmerinnen und Kreditnehmer können einen Darlehensvertrag mit festem Zinssatz in folgenden Situationen kündigen (§ 489 BGB):

- Wenn die Zinsbindung endet, unter Einhaltung einer Kündigungsfrist von einem Monat frühestens vor dem Ablauf des Tages, an dem die Zinsbindung endet.
- Nach Ablauf von zehn Jahren unter Einhaltung einer Kündigungsfrist von sechs Monaten.

Neben diesen gesetzlichen Kündigungsmöglichkeiten, bei denen keine Vorfalligkeitsentschädigung anfällt, hat der Bundesgerichtshof ein Kündigungsrecht in folgenden Fällen angenommen:

- Beim Verkauf der Immobilie.
- Wenn die Bank eine Ausweitung des Kredites ablehnt und damit eine wirtschaftliche Nutzung des Objektes verhindert.

In diesen Fällen kann der Kreditgeber jedoch Vorfalligkeitsentschädigung verlangen (siehe Abbildung 60).

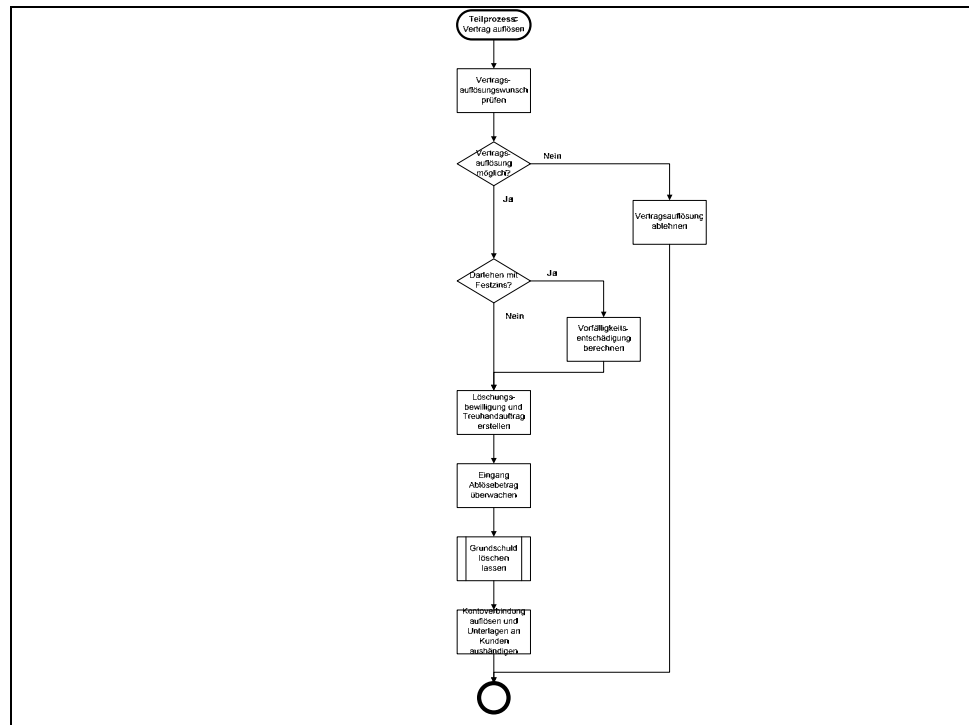


Abbildung 60: IMMO Teilprozess Vertragsauflösung (Quelle: GAD eG)

Sind die oben angeführten Voraussetzungen nicht gegeben, obliegt es der Bank, den Wunsch von Kundinnen oder Kunden abzulehnen. Ist eine der Voraussetzungen erfüllt, ist eine Auflösung ggf. mit der Berechnung einer Vorfälligkeitsentschädigung möglich. Hierbei muss eine Löschungsbewilligung und ein Treuhandauftrag erstellt werden. Die Überweisung der Ablösesumme erfolgt dann unter der Maßgabe des Treuhandauftrags. Die Bank darf nur über das Geld verfügen, wenn er im Gegenzug die Bedingungen des Treuhandauftrags erfüllt und die Übertragung der jeweiligen Sicherheiten durchführt (hier die Löschung der Grundschuld veranlasst). Nach Durchführung dieser Tätigkeiten kann das Darlehnskonto aufgelöst werden.

Damit ist Beschreibung der Prozesskette "private Immobilienfinanzierung" von der fachlichen Perspektive im Rahmen des PRK-Screenings abgeschlossen. Für eine ganzheitliche Betrachtung und Analyse des Lebenszyklus der Prozesskette reicht jedoch die Berücksichtigung der fachlichen Perspektive nicht aus. Daher werden im folgenden noch ergänzende Beschreibungen aus Sicht der IT-Architektur und IT-Sicherheit sowie aus juristischer Sichtweise ergänzt und das PRK-Screening damit vervollständigt.

Prozessbezeichnung [Objekt / Verrichtung]	Darlehensvertrag auflösen
Kurzbeschreibung [wesentliche Kernpunkte / Aufgaben und Rahmenbedingungen]	Der Wunsch von Kundinnen oder Kunden zur Darlehensauflösung liegt dem Kreditgeber vor. Der Kreditgeber prüft die Möglichkeit zur Beendigung des Engagements und wickelt die Auflösung des Darlehensvertrages, evtl. mit Berechnung einer Vorfälligkeitsentschädigung, ab und gibt die Sicherheitenstellung frei.
Prozessauslöser [Bezeichnung des Ereignisses, das den Prozess auslöst]	Wunsch der Kundin oder des Kunden zur Vertragsauflösung liegt der Bank vor.
Prozessziel / Prozessergebnis [Beschreibung, welcher Zustand zu erreichen ist]	Das bestehende Darlehen wurde aufgelöst.
Prozesszuständigkeit [Aufgabenträger für die operative Durchführung des Prozesses]	Beraterinnen und Berater Markt / Kredit-sachbearbeiterinnen und Kreditsachbearbeiter Marktfolge
Mitgeltende Unterlagen [zu berücksichtigende Informationen]	Treuhandauftrag, Löschungsbewilligung
Prozessvoraussetzungen [fachlich, nicht IT-bezogen]	Voraussetzung gem. § 489 BGB liegt vor
Schnittstellen / Abhängigkeiten	Bringschuld von Kundinnen oder Kunden, Voraussetzungen des § 489 BGB liegen

[zu anderen Prozessen; Gründe: gesetzliche / organisatorische Anforderungen; Hol- oder Bringschuld]	vor.
Medien / Medienbrüche [Darstellung der im Prozessverlauf verwendeten Medien]	Die Freigabe / Löschung der Grundschild muss manuell erfolgen.
Durchlaufzeit [pro Vorgang]	Keine Angabe
Häufigkeit des Prozessdurchlaufs [pro Zeiteinheit]	Keine Angabe

Tabelle 17: Systematische Beschreibung des TP "Darlehnsvertrag auflösen"

7.1.2 IT-architektonische Beschreibung und Analyse

Die IT-architektonische Perspektive beschreibt die zuvor dargestellte Prozesskette aufgrund einer IT- bezogenen Sichtweise und zeigt vor diesem Hintergrund das Zusammenspiel der unterschiedlichen Systeme und Anwendungen, die bei den Prozessbeteiligten im Einsatz sind. Darüber hinaus werden technische Schnittstellen beschrieben und eventuelle Medienbrüche dargestellt.

Die im Rahmen der Prozesskette zum privaten Immobilienkredit beteiligten Parteien sind in der Abbildung 61 dargestellt. Bei der adressierten Prozesskette geht es an vielen Stellen der Prozesskette darum, bei einem externen Partner etwas zu beantragen (Verträge, Auskünfte, Urkunden, etc.), welche dieser auf Grundlage einer Beauftragung durch Kundinnen und Kunden oder aufgrund eines berechtigten Interesses an die Bank liefert.

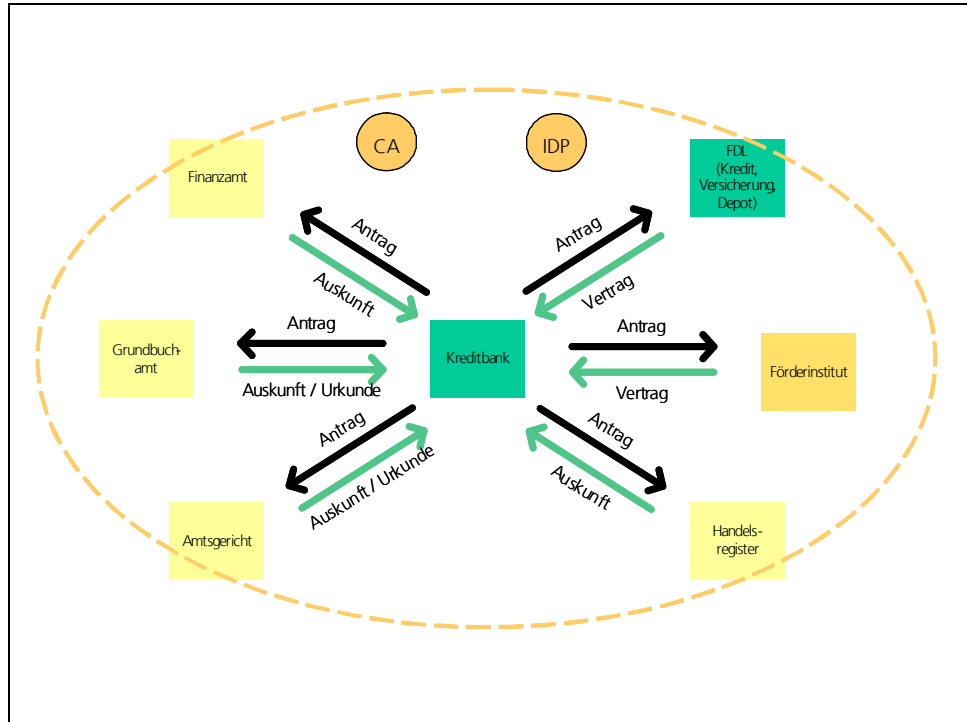


Abbildung 61: IMMO und die beteiligten Parteien (Quelle: Eigene Darstellung)

Die IST-Analyse im Rahmen des PRK-Screenings zeigt, dass derzeit noch nicht alle aufgeführten Parteien direkt und unmittelbar in die Prozesskette mit einbezogen sind. Einige Institutionen der öffentlichen Verwaltung sind nur indirekt beteiligt, beispielsweise wenn die Kundin oder der Kunde Dokumente von dieser Partei vorlegt (z. B. Einkommensbescheid des Finanzamts). Des Weiteren gibt es Partner, Certificate Authority / Zertifizierungsstelle (CA) und Identity Provider (IDP), die aufgrund der Papierform bzw. des praktizierten Zulassungsmanagement zu den elektronischen Verfahren noch nicht oder nur rudimentär beteiligt sind.

Die Partizipation der einzelnen Parteien an der Prozesskette lässt sich ebenfalls anhand einer Process Support Map illustrieren. Diese zeigt die verwendeten Systeme und Anwendungen, die im Rahmen der Abwicklung der Prozesskette eingesetzt werden und zeigt Anhaltspunkte auf, an welchen Stellen des Prozesses mit Inkompatibilitäten gerechnet werden kann und wo kritische Schnittstellen zwischen den Partnern angesiedelt sind. In der Abbildung 62 ist die zugehörige Prozess Support Map zu sehen, in der versucht wurde IST- und SOLL-Architektur anschaulich gegenüber zu stellen. Die Abbildung zeigt, dass z. B. beim Bundesanzeiger der aktuelle HTTP-

Server zukünftig durch einen Webservice zu ersetzt ist, um dadurch diesen Partner besser in die Prozesskette integrieren zu können.

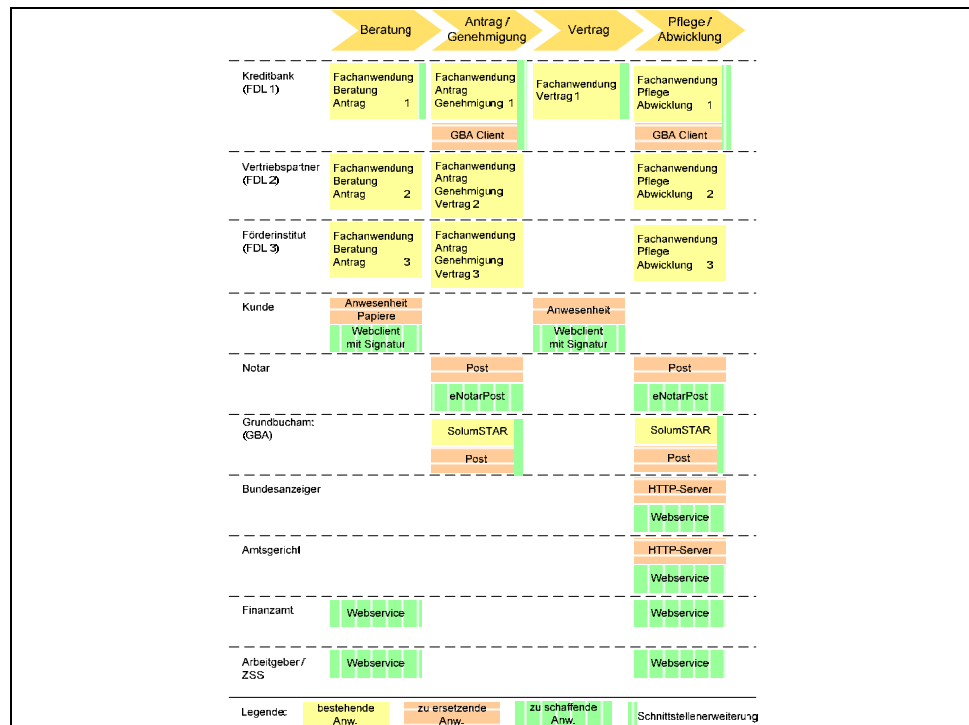


Abbildung 62: IMMO Process Support Map für die Prozesskette "Private Immobilienfinanzierung" (Quelle: Eigene Darstellung)

Aufgrund des großen Umfangs für die Beschreibung aller möglichen Schnittstellen und Anwendungen im Rahmen der Prozesskette, werden in den anschließenden Abschnitten zwei beispielhafte organisationsübergreifende Prozesse dargestellt und im Rahmen der Screening-Phase beschrieben. Dabei handelt es sich um die Prozesse zwischen Bank und Förderinstitut, sowie zwischen Bank und Grundbuchamt.

Das Förderinstitut

Die IST-Situation bezogen auf den Prozess der Fördermittelbeantragung zwischen der Bank und Förderinstitut ist in der Abbildung 63 dargestellt. Derzeit wird in vielen Banken der Antrag auf Fördermittel im Institut ausgedruckt, von Kundinnen oder Kunden unterschrieben und auf dem Postweg verschickt. Dieser Antrag wird anschließend beim Förderinstitut weiter bearbeitet. Der Vertrag kommt zurück zur Bank und wird in den Kundenvorgang eingepflegt.

An dieser Stelle ist anzumerken, dass in einigen Banken bzw. Bankengruppen die Übermittlung des Antrages für bereits schon heute elektronisch durchgeführt werden kann. Da dies jedoch noch nicht der Standardfall ist, wurden an dieser Stelle weiterhin von einer manuellen, papierbasierten Übermittlung ausgegangen.

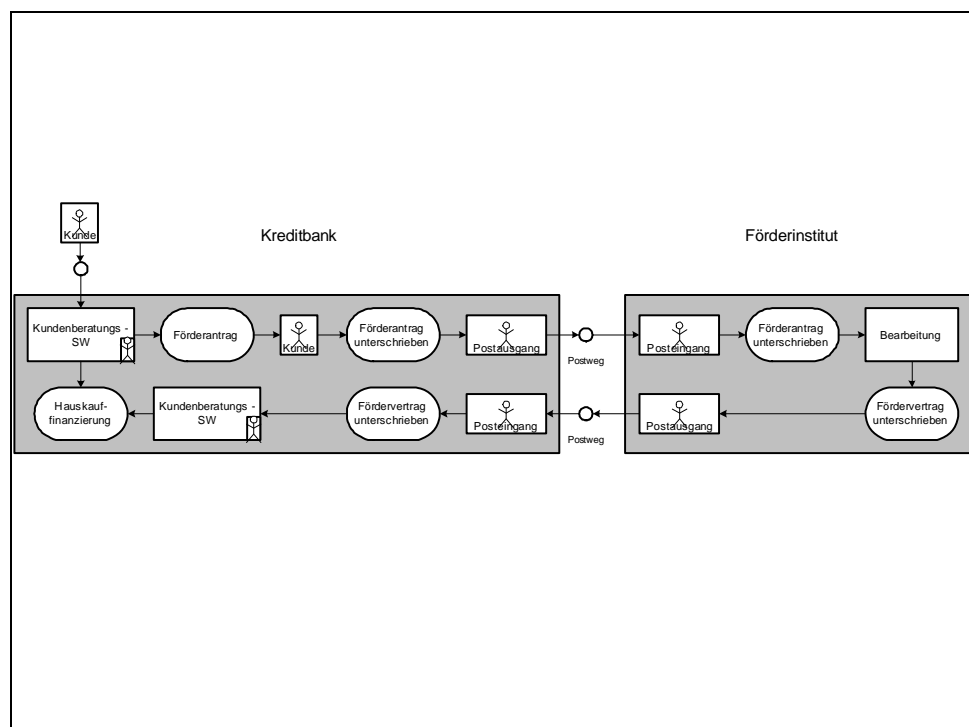


Abbildung 63: IMMO IST-Architektur Förderinstitut (Quelle: Eigene Darstellung)

Im Rahmen der Prozesskette private Immobilienfinanzierung bestehen die im Einsatz befindlichen Kundenberatungs-Software aus mehreren verschiedenen Komponenten, welche im Rahmen der Kundenberatung sowohl bank-eigene als auch Produkte der Förderinstitute berücksichtigen. Die verschiedenen Komponenten können dabei ohne Anbindung zur Kundenberatungs-Software stehen oder über Schnittstellen mit dieser verbunden sein.

Im Rahmen des PRK-Screenings bezogen auf die IST-Situation wurden die Prozesse und Anwendungen des Förderinstituts nicht weiter strukturiert.

Das Grundbuchamt

Im Rahmen des PRK-Screenings der Prozesskette zur privaten Immobilienfinanzierung wurde als zweites Beispiel die Teilprozesse zwischen der Bank und dem Grundbuchamt herangezogen. Die betrachteten Prozessschritte, welches das Grundbuchamt mit einbeziehen sind im wesentlichen, Einsicht in das Grundbuch sowie das Bestellen und Löschen einer Grundschuld.

Die Einsicht in das Grundbuchamt ist bereits heute manuell elektronisch möglich (siehe Abbildung 64 und Tabelle 18). Damit ist ein schneller Zugang zu den jeweils relevanten Daten gegeben. Als Einschränkung dabei ist festzuhalten, dass die Daten des Grundbuchamtes nicht als XML-Dokument vorliegen, sondern in der Regel als PDF-Dokumente verfügbar sind. Daher ist auch hier ein Medienbruch zu verzeichnen, da die relevanten Daten nicht unmittelbar bei den Empfängern weiter verarbeitet werden können. Die Daten müssen von Bankmitarbeiterinnen und Bankmitarbeitern manuell in das System der Bank eingegeben werden. Ein weiterer bestehender Nachteil ist der, dass man von der bundesweiten Internetseite nur manuell auf die Länderseiten weiter navigieren kann und erst von diesen gelangt man in die eigentliche Anwendung des Grundbuchamtes.

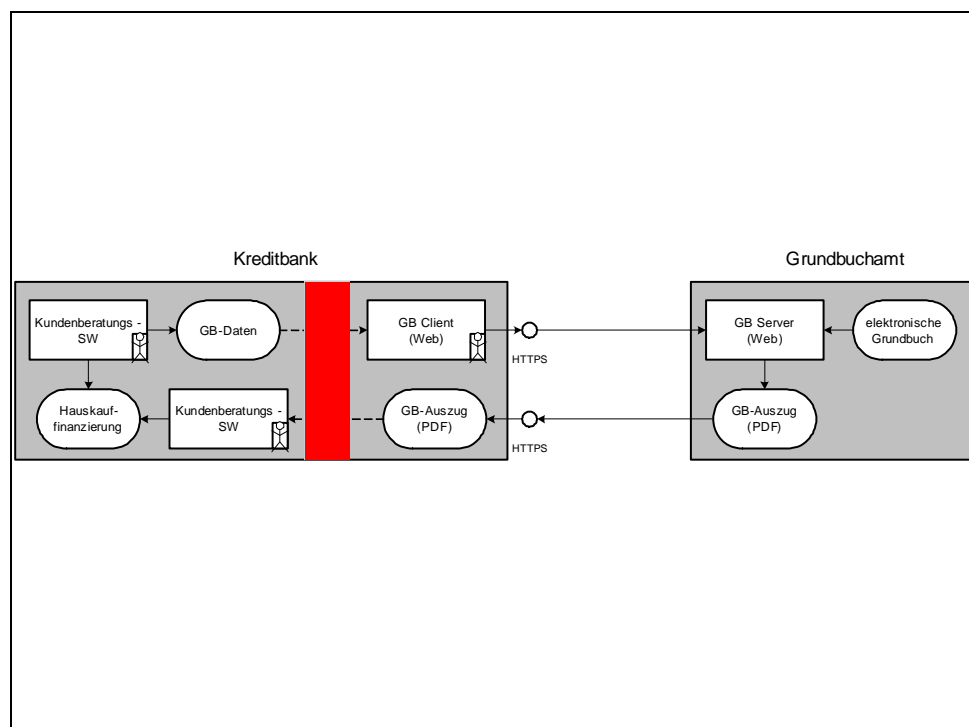


Abbildung 64: IMMO IST-Architektur Grundbuchamt (Einsicht) (Quelle: Eigenen Darstellung)

Des Weiteren erfolgt die Eintragung einer Grundbuchsschuld heute ausschließlich manuell über Papierdokumente und dem Postweg. Auch hier sind noch zahlreiche Potenziale zur Optimierung der Prozesskette im Rahmen der Immobilienfinanzierung gegeben.

Der Bearbeitungsstand eigener Anträge kann aber über den elektronischen Weg eingesehen werden. Man kann auch eine nicht rechtsgültige Vorabmitteilung über den erfolgten Eintrag (Status und Antragsnummer) per E-Mail erhalten (siehe Abbildung 65).

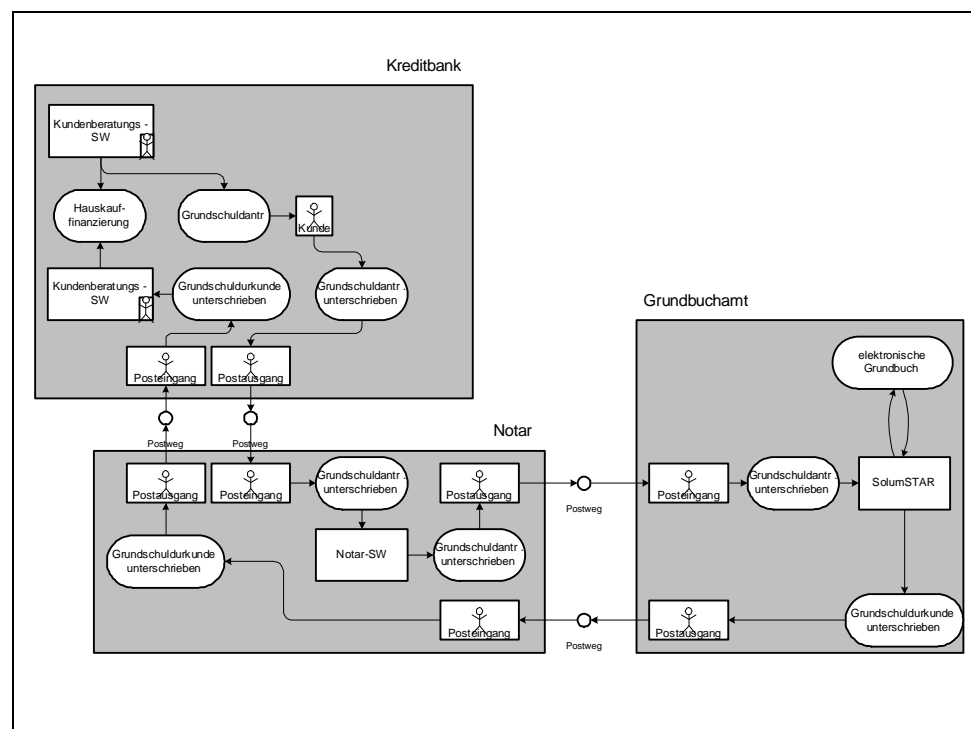


Abbildung 65: IMMO IST-Architektur des Grundbuchamt (Grundschuld) (Quelle: Eigene Darstellung)

Die vorangegangenen Betrachtung der IT-Architekturen und Anwendungen im Rahmen des PRK-Screenings der Prozesskette zur privaten Immobilienfinanzierung zeigen, dass an vielen Stellen der vorhandenen Prozesse zahlreiche Informationen, mit unterschiedlichen Kritikalitäten, zwischen verschiedenen Parteien ausgetauscht werden. Dies zeigt die hohe Anforderungen an Sicherheit im allgemeinen und der IT-Sicherheit im speziellen, welche im Rahmen der IST-Analyse zu beachten ist. Aus diesem Grund werden im folgenden Kapitel ausgewählte Aspekte zur IT-Sicherheit untersucht.

7.1.3 Sicherheitstechnische Beschreibung und Analyse

Im Rahmen des PRK-Screenings der Prozesskette zur privaten Immobilienfinanzierung werden im folgenden ausgewählte Aspekte zur IT-Sicherheit untersucht. Diese Analyse fokussiert dabei ebenfalls auf die Prozesse zwischen Banken und Förderinstituten beziehungsweise zwischen Banken und Grundbuchämtern.

Datenaustausch Förderinstitut

Der Datenaustausch findet derzeit zum größten Teil manuell d. h. in Papierform per Post statt. Da es sich um personenbezogene Daten handelt, ist von einem hohen Schutzbedarf auszugehen. Gefährdet sind u. a. die Vertraulichkeit und die Authentizität. Beispielsweise könnten unberechtigte Dritte Einblick in die Daten erhalten und daraus einen persönlichen Vorteil ziehen oder durch Fälschung von Daten unberechtigterweise Fördergelder abrufen. Die eigenhändige Unterschrift und der Transport per Post kann dafür als ausreichend sicher angesehen werden, ist aber nicht immun gegen Angriffe wie z. B. das Fälschen von Unterschriften oder das Abfangen bzw. die Manipulation der Briefpost. Dies ist ggf. schon mit sehr wenig Aufwand für Angreifer möglich. Die Abbildung 66 zeigt beispielsweise das Versenden der relevanten Daten an das Förderinstitut sowie mögliche Schwachstellen, die potenzielle Angreifer nutzen könnte.

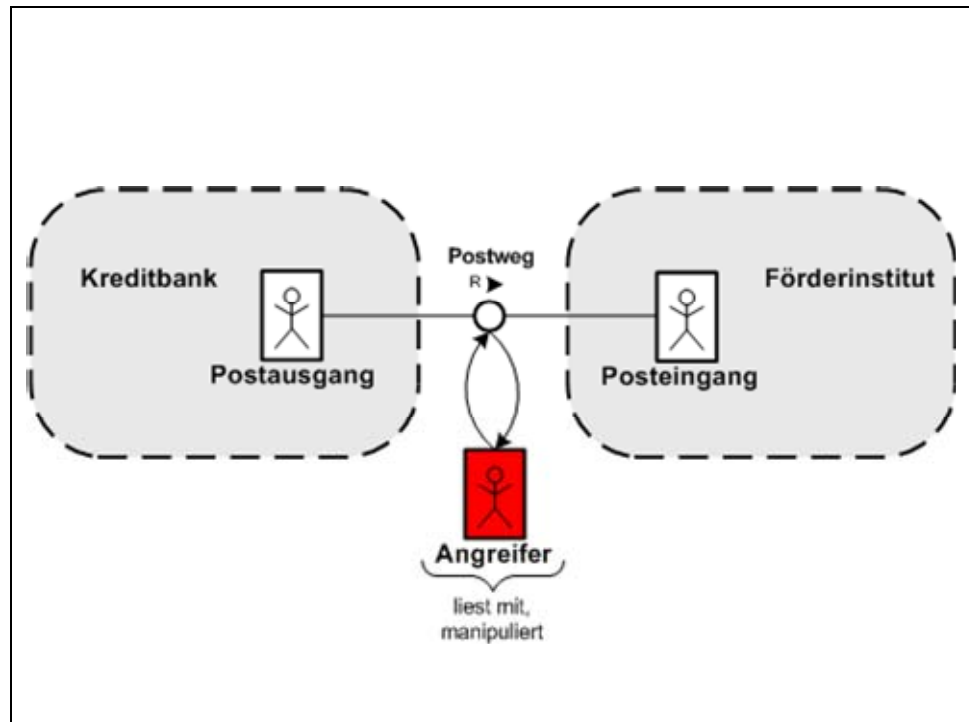


Abbildung 66: IMMO Datenaustausch zwischen Bank und Förderinstitut (Quelle Eigene Darstellung)

Eine elektronische Lösung mit angemessenen Verfahren zur Signatur und zur Verschlüsselung würde das Sicherheitsniveau schon mit geringem Aufwand deutlich erhöhen.

Datenaustausch elektronisches Grundbuch

Entsprechend dem Vorgehen bei der IT-Architektur wird auch im Bereich der IT-Sicherheit der Prozess zwischen Bank und Grundbuchamt untersucht. Der Datenaustausch mit dem Grundbuchamt besteht im wesentlichen aus zwei Teilprozessen, die Einsicht in das Grundbuch und das Bestellen einer Grundschuld.

Einsicht in das Grundbuch

Zur Einsicht in das Grundbuch ist immer ein "berechtigtes Interesse" erforderlich. Dies muss durch Notare und öffentlich bestellte Ingenieure i. d. R. nicht im Einzelfall nachgewiesen werden, so dass für diese Personengruppen grundsätzlich eine uneingeschränkte Grundbucheinsicht möglich ist. Dagegen sind einer Bank, in der Grundbuchverfügung genannte Versorgungsunternehmen und Privatpersonen, nur eine eingeschränkte Einsicht-

nahme erlaubt. Dazu muss aber für jeden Einzelfall ein berechtigtes Interesse nachgewiesen werden.

Die Einsicht in das Grundbuch ist folglich nur registrierten und dazu berechtigten Nutzern (d. h. Gerichte, Behörden, Notariate und öffentlich bestellte Ingenieure s. o.) möglich. Der Zugang erfolgt i.d. R. über eine HTTPS-Verbindung mit Anmeldenamen und Passwort. Eine Clientauthentifizierung mit Client-Zertifikaten ist dabei grundsätzlich nicht vorgesehen. Die Abbildung 67 zeigt beispielsweise den Abruf der Daten beim Grundbuchamt durch die Kreditbank.

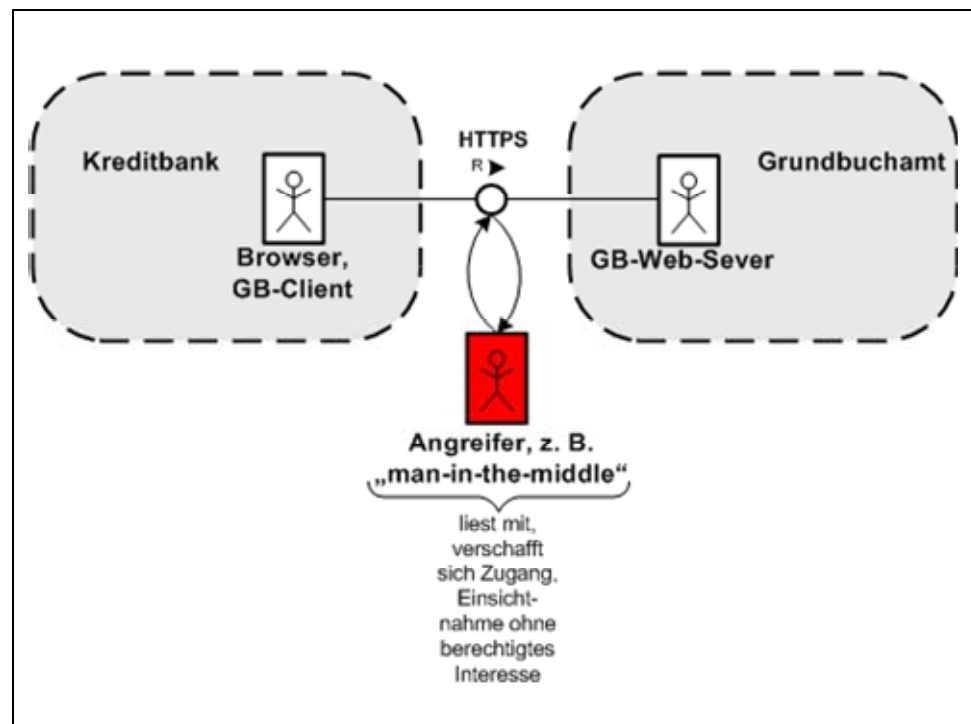


Abbildung 67: IMMO Dateneinsicht Grundbuch (Quelle: Eigene Darstellung)

Im Rahmen der Prozessanalyse zeigt sich, dass eine elektronische Lösung mit bilateralen Kommunikationsmöglichkeiten und angemessenen Verfahren zur Signatur und zur Verschlüsselung den dargestellten Prozess hinsichtlich der Effizienz und des Sicherheitsniveaus erhöhen würde.

Bestellen einer Grundschuld

Neben dem Prozess der Grundbucheinsicht ist die Bestellung einer Grundschuld im Rahmen des PRK-Screenings analysiert worden. Der Datenaus-

tausch findet komplett manuell d. h. in Papierform per Post statt. Dies gilt sowohl für die Kommunikation zwischen Kreditbank und Notar als auch für die Kommunikation zwischen Notare und Grundbuchämter. Da es sich um personenbezogene Daten handelt und dadurch ein hohes Schadenspotential besteht, ist von einem sehr hohen Schutzbedarf auszugehen. Gefährdet sind u. a. die Vertraulichkeit und die Authentizität. Denkbar ist z. B. die Fälschung von Unterschriften, Siegel etc. durch Manipulationen während des Postversands, denn das Abfangen bzw. die Manipulation der Briefpost ist ggf. schon mit sehr wenig Aufwand für Angreifer möglich.

Statusinformationen zum Verfahren werden über unverschlüsselte E-Mails versendet. Hierüber könnten unberechtigte Dritte auf unzulässiger Weise Informationen über das Verfahren erhalten. Die Abbildung 68 zeigt beispielhaft den Versand der Daten zu Notare.

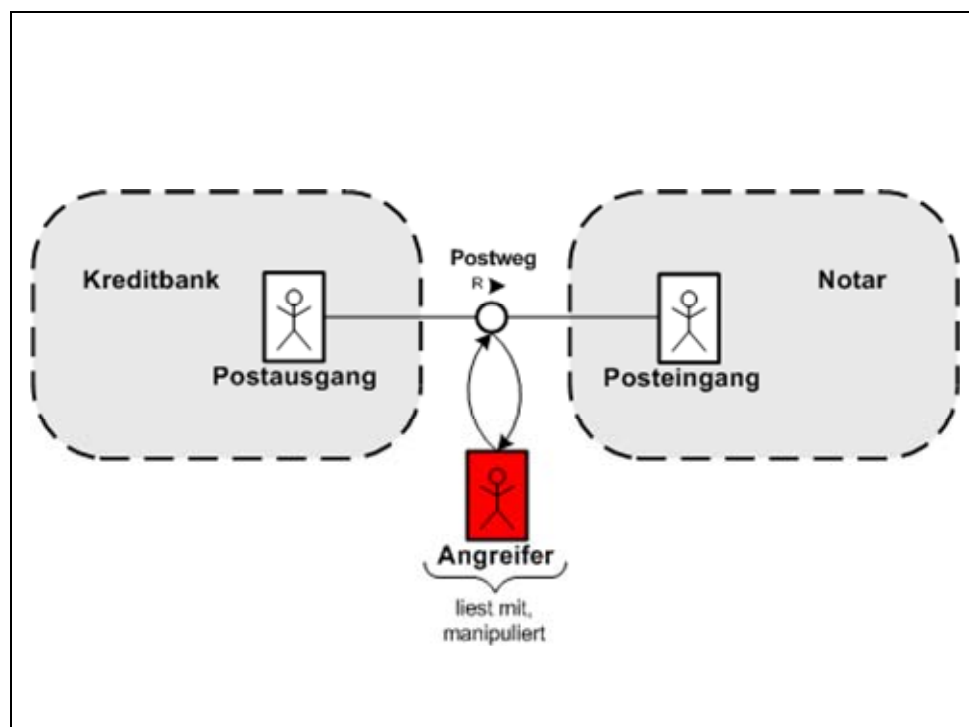


Abbildung 68: IMMO Datenaustausch Grundbuch (Quelle: Eigene Darstellung)

Aufgrund der Analyse zeigt sich, dass eine elektronische Lösung mit angemessenen Verfahren zur Signatur und zur Verschlüsselung im Rahmen dieses Prozesses sowohl die Effizienz als auch das Sicherheitsniveau erhöhen können würde. Für vergleichbare Prozesse gibt es mittlerweile erprobte Lösungen, beispielsweise das IT-Fachverfahren "Elektronisches Handelsregis-

ter", bei dem Anträge der Notare nur noch elektronisch gestellt werden können und qualifizierte elektronische Signaturen zum Einsatz kommen. Die Orientierung an derartigen Beispielen bietet sich daher an.

Damit ist das PRK-Screening aus Sicht der IT-Sicherheit abgeschlossen. Wie eingangs bereits dargestellt, ist für eine umfassende Analyse der Prozesskette zur privaten Immobilienfinanzierung noch die juristische Perspektive ausstehend. Diese wird im folgenden Kapitel dargestellt.

7.1.4 Juristische Beschreibung und Analyse

Das PRK-Screening aus juristischer Sicht fokussiert sich auf einzelne Aspekte der Prozesskette, bei denen besondere gesetzliche Vorschriften und Normen Beachtung finden. Die juristische Analyse und Beschreibung bezieht sich auf die gesamte Prozesskette des privaten Immobilienkredites. Im folgenden sollen die in der Abbildung 46 dargestellten Phasen des Geschäftsprozesses "private Immobilienfinanzierung" aus juristischer Sicht betrachtet werden.

Kunde – Persönliche Vertragsunterzeichnung

Verträge unterliegen normalerweise keiner besonderen Form; sie können mündlich, via Telefax, via E-Mail, schriftlich usw. abgeschlossen werden. Für besondere Vertragstypen hat der Gesetzgeber besondere Formen des Vertragsschlusses und damit seiner Willenserklärungen auferlegt.

Eine besondere Form des Vertragsschlusses – Schriftform - ist beispielsweise im Rahmen der vorliegenden Thematik in folgenden Bereichen zwingend vorgeschrieben:

- beim Verbraucherdarlehensvertrag (§ 492 BGB),
- bei der Bürgschaft (§ 766 BGB),
- beim Schuldversprechen (§ 780 BGB) und
- beim Schuldanerkennnisses (§ 781 BGB).

Daher sind Verbraucherdarlehensverträge gemäß § 492 Absatz 1 Satz 1 BGB, "soweit nicht eine strengere Form vorgeschrieben ist, schriftlich abzuschließen." und in Satz 3: "Der Schriftform ist genügt, wenn Antrag und Annahme durch die Vertragsparteien jeweils getrennt schriftlich erklärt wer-

den." Die Kreditinstitute erstellen demnach die Kreditverträge in der gesetzlich geforderten Schriftform.

Immobilienkreditverträge werden gem. § 492 Absatz 1a Satz 2 BGB grundsätzlich als Verbraucherkreditverträge angesehen: "Immobilienkreditverträge sind Verbraucherkreditverträge, bei denen die Zurverfügungstellung des Darlehens von der Sicherung durch ein Grundpfandrecht abhängig gemacht wird und zu Bedingungen erfolgt, die für grundpfandrechtl. abgesicherte Kreditverträge und deren Zwischenfinanzierung üblich sind; ...".

Fördermittelberatung und -beantragung, Beratung und Beantragung von Produkten der Vertriebspartner (Verbund, Konzern, etc.)

Im Vorfeld und / oder im Rahmen des Vertragsschlusses ist Beratung erforderlich, unter anderem auch Fördermittelberatung und -beantragung. Entsprechende Anträge werden in der Regel schriftlich gestellt. In diesem Zusammenhang und bei Beantragung eines Kredits ist Aufklärung von Kundinnen und Kunden erforderlich, wohin deren Daten übermittelt werden.

Anforderung des Einkommensteuerbescheid und Einkommensnachweises

Für die im Rahmen des Kreditvertrages vorbereitende Prüfung der Bonität von zukünftigen Kreditnehmerinnen und Kreditnehmern ist gem. § 18 KWG u. a. bei Kreditsummen größer 750.000 Euro das Kreditinstitut verpflichtet, sich die "wirtschaftlichen Verhältnisse" offen legen zu lassen. Diese Bringschuld von Kunden wird in der Regel auch auf Baufinanzierungen mit geringerer Kreditsumme angewandt.

Grundbuchamt

Im Bereich der privaten Immobilienfinanzierung geht es im wesentlichen um Einsicht in das Grundbuch und Bestellen einer Grundschuld. Daneben kennt das BGB weitere Rechte an Immobilien: das Erbbaurecht, das dingliche Vorkaufsrecht, die Dienstbarkeit und die Reallast.

Grundbuchauskunft

Ein Einsichtsrecht in das Grundbuch hat gem. § 12 GBO nur derjenige, der ein berechtigtes Interesse darlegen kann. Dies gilt nicht nur im Hinblick auf Eigentumsverhältnisse an dem Grundstück, sondern auch für Auskünfte aus Abteilung 3 des Grundbuchs (Rechte und Lasten des Grundstücks). Das Kreditinstitut kann bei der Eigentümerin oder dem Eigentümer im Rahmen

des Kreditantragsverfahrens Zustimmung zur Einsichtnahme in das Grundbuch einholen. Schriftform ist nicht erforderlich; entsprechende Verträge sind aus Beweisgründen - Nachweis des berechtigten Interesses gegenüber dem Grundbuchamt - schriftlich ausgestaltet.

Möglich ist die Grundbuchauskunft über das klassische schriftliche Verfahren. Daneben gibt es zwischenzeitlich auch die Möglichkeit, via Antrag am automatisierten Grundbuch-Abfrageverfahren ("Internet-Grundbucheinsicht") teilzunehmen. Neben Notaren, Gerichten und Behörden, können auch Kreditinstitute über ein Anmeldeverfahren zugelassen werden. Die Abfrage sind gebührenpflichtig.

§ 12 GBO (Darlegung eines berechtigten Interesses) findet auch hier Anwendung. Das Kreditinstitut bestätigt dies im Rahmen des Antrags auf Teilnahme. Siehe dazu beispielhaft im Teilnahmeantrag des "Elektronisches Grundbuch Nordrhein-Westfalen" (SolumSTAR):

"Ich versichere / Wir versichern, Einsicht in das Grundbuch und in die gemäß § 12a GBO geführten Verzeichnisse nur in dem nach den §§ 12, 12 a und 12 b GBO und §§ 80 ff. Grundbuchverfügung zulässigen Umfang zu nehmen. Das berechtigte Interesse an der jeweiligen Einsichtnahme in das Grundbuch wird vor jedem Abruf durch Angabe eines der oben angegebenen Gründe dargelegt (§ 82 Abs. 2 bzw. § 86 a Abs. 1 Grundbuchverfügung). Mir / Uns ist bekannt, dass die Abrufdaten für die Kontrolle der Rechtmäßigkeit von Abrufen protokolliert werden (§ 83 Abs. 1 Grundbuchverfügung)."

Grundschuldbestellung

Sowohl die Übertragung des Eigentums und Belastungen an einem Grundstück setzen eine notarielle Beurkundung und eine Eintragung im Grundbuch voraus (siehe § 873 Abs. 1 BGB). "Vor der Eintragung sind die Beteiligten an die Einigung nur gebunden, wenn die Erklärungen notariell beurkundet oder vor dem Grundbuchamt abgegeben oder bei diesem eingereicht sind oder wenn Berechtigte dem anderen Teil eine den Vorschriften der Grundbuchordnung entsprechende Eintragungsbewilligung ausgehändigt hat" (§ 873 Absatz 2 BGB).

Pfandfreigabe, Grundschuldlöschung

Grundbuchlösungen in Abteilung 3 des Grundbuchs sind nur auf Antrag an das Grundbuchamt zulässig. Dabei haben Eigentümerinnen und Eigentümer eine Löschungsbewilligung seines Kreditinstituts, für das die Grundschuld eingetragen ist, vorzulegen.

Informationen zu Handelsregistereintragen und Jahresabschlüssen von Unternehmen

Im Gegensatz zum Grundbuch ist das Handelsregister ein öffentliches Verzeichnis, § 9 Absatz 1 Satz 1 HGB: "Die Einsichtnahme in das Handelsregister sowie in die zum Handelsregister eingereichten Dokumente ist jedem zu Informationszwecken gestattet." Das Handelsregister wird von den Gerichten elektronisch geführt (§ 8 Absatz 1 HGB). Gemäß § 12 Absatz 1 HGB sind Anmeldungen zur Eintragung in das Handelsregister elektronisch in öffentlich beglaubigter Form einzureichen.

Die gesetzlichen Vertreter von Kapitalgesellschaften haben für ihre Kapitalgesellschaft den Jahresabschluss und andere Dokumente beim Betreiber des elektronischen Bundesanzeigers elektronisch einzureichen (§§ 325 ff., 339 HGB).

Über das "Gemeinsame Registerportal der Länder" (www.handelsregister.de) können kostenfreie und je nach Inhalt kostenpflichtige Recherchen durchgeführt werden.

Ein Datenabruf ist datenschutzrechtlich zulässig.

Auskünfte über Insolvenzbekanntmachungen

Insolvenzen werden öffentlich bekannt gemacht (§ 9 Absatz 1 InsO i.V.m. § 8b Absatz 2 Ziffer 11 HGB). Informationen dazu können unter <https://www.insolvenzbekanntmachungen.de> abgerufen werden.

Ein Datenabruf ist datenschutzrechtlich zulässig.

Elektronischer Datenaustausch im Mahnverfahren

Das Mahnverfahren ist in §§ 688 ff. ZPO geregelt. "Wegen eines Anspruchs, der die Zahlung einer bestimmten Geldsumme in Euro zum Gegenstand hat, ist auf Antrag des Antragstellers ein Mahnbescheid zu erlassen." (§ 688 Absatz 1 ZPO). Gemäß § 688 Absatz 2 Nr. 1 ZPO ist das Mahnverfahren bei bestimmten Verbraucherkreditverträgen nicht anwendbar: "...wenn der nach den §§ 492, 502 des Bürgerlichen Gesetzbuchs anzugebende effektive oder anfängliche effektive Jahreszins den bei Vertragsschluss geltenden Basiszinssatz nach § 247 des Bürgerlichen Gesetzbuchs um mehr als zwölf Prozentpunkte übersteigt;"

Alternativ zur handschriftlichen Unterzeichnung (§ 690 Absatz 2 ZPO) des Mahnantrags, kann er gemäß § 690 Absatz 3 ZPO auch "in einer nur ma-

schinell lesbaren Form übermittelt werden...". Ab 01.12.2008 ist für Rechtsanwälte nur noch der elektronische Mahnantrag möglich; § 690 Absatz 3 ZPO: "Der Antrag kann in einer nur maschinell lesbaren Form übermittelt werden, wenn diese dem Gericht für seine maschinelle Bearbeitung geeignet erscheint. Wird der Antrag von einem Rechtsanwalt gestellt, ist nur diese Form der Antragstellung zulässig. Der handschriftlichen Unterzeichnung bedarf es nicht, wenn in anderer Weise gewährleistet ist, dass der Antrag nicht ohne den Willen des Antragstellers übermittelt wird."

Damit sind die aus Sicht des Autorenteam's wichtigsten juristischen Aspekte im Rahmen des PRK-Screenings der Prozesskette private Immobilienfinanzierung dargestellt.

Das PRK-Screening bezogen auf die IST-Situation hat gezeigt, dass derzeit noch zahlreiche Potenziale zur Verbesserung der organisationsübergreifenden Prozesskette vorhanden sind. Alle dargestellten Perspektiven haben beispielhaft gezeigt, dass durch eine organisationsübergreifende Optimierung zusätzliche Optimierungspotenziale erschlossen werden können.

Um diese Potenziale zu erschließen, ist jedoch auch die Festlegung relevanter Ziele notwendig, welche den angestrebten SOLL-Zustand der zukünftigen Prozesskette repräsentieren.

7.2 Ziele und Anforderungen an die Prozesskette Level-1

Dieses Kapitel adressiert den zweiten Schritt im Vorgehensmodell zur Gestaltung von Prozessketten, nämlich das PRK-Scoping auf potenzielle Ziele zur Gestaltung und zum Management von Level-1 Prozessketten.

Wie im Rahmen der vorhergegangenen Kapitel der Machbarkeitsstudie bereits dargestellt, repräsentieren Ziele bezogen auf die Prozesskette einen zukünftig gewünschten Zustand. Die Struktur der hier beschriebenen Ziele orientiert sich an der in der Machbarkeitsstudie vorgenommenen Unterteilung der Zieldimensionen. Aufgrund der ganzheitlichen Betrachtungsweise dieser Fallstudie werden demnach die nachfolgend beschriebenen Ziele in die Zieldimensionen fachlich / wirtschaftliche, IT-bezogene und juristische Ziele unterteilt. Die nachfolgend aufgeführten Ziele sind auf Basis von Expertinnen- und Experteneinschätzungen für diese Fallstudie vorgenommen worden.

Als Resultat dieser Einschätzung wurden im Rahmen dieser Fallstudie nachfolgend aufgeführte Ziele identifiziert und für die weiteren Arbeiten zugrunde gelegt.

Wirtschaftliche Zielsetzungen für Prozessketten:

Die nachfolgend aufgeführten wirtschaftliche Ziele fokussieren hauptsächlich auf drei Dimensionen: Performance, Kosten, und Qualität von Prozessketten.

- Das Ziel der stetigen Verbesserung der **Performance** der betrachteten Prozesskette adressiert die Optimierung der Effizienz und Effektivität der Prozesse. Ein bedeutender Faktor dabei ist die Reduzierung der Prozesszeiten.
Im Rahmen der Verbesserung und Optimierung der dargestellten Prozessketten zwischen Banken und Einrichtungen der öffentlichen Verwaltung sind die Zielsetzung, neben den Bearbeitungszeiten vorrangig die Transport- und Liegezeiten in den Prozessketten zwischen den FDL und den Institutionen der öffentlichen Verwaltung durch elektronischen Datenaustausch zu reduzieren.
Die Bearbeitungszeit eines Geschäftsprozesses ist ein Faktor zur Bestimmung der Mitarbeiterkapazität.
Die Durchlaufzeit eines Geschäftsprozesses ist ein weiterer Faktor, der Auswirkungen auf die Ausgestaltung der Operational Level Agreements (OLA), also der unternehmensinternen Sicht und der übergeordneten Service Level Agreements (SLA), der Endkundensicht hat. [IMMO 1]
- Die unterschiedlichen Faktoren der Prozesskettenperformance determinieren sehr stark auch die anfallenden **Kosten** für die Prozesskette zwischen Banken und Einrichtungen der öffentlichen Verwaltung. Auf eine detaillierte Aufzählung der verschiedenen Kostenverursacher sowie der Kostenarten wird an dieser Stelle verzichtet. [IMMO 2]
- Die dritte Zieldimension bezüglich der wirtschaftlichen Ziele besteht in der Steigerung der **Qualität** der gestalteten Prozesskette sowie deren Leistungserstellungsprozess. Sowohl die Mitarbeiterkapazität als auch die internen / externen Service Level sind neben anderen kritische Faktoren im Wertschöpfungsprozess. Die Qualität des Wertschöpfungsprozesses hat letztendlich dann auch Auswirkungen auf die Produktivität eines Unternehmens und deren Wettbewerbsfähigkeit. [IMMO 3]

Neben den wirtschaftlichen Zielen müssen im Rahmen eine ganzheitlichen Sichtweise auch Ziele aus den Bereichen IT und Recht berücksichtigt werden.

Für die IT-Architektur ergeben sich folgende Ziele:

- Die Realisierung eines hohen Grades an Automatisierung der Prozesskette über die Grenzen der jeweiligen beteiligten Institutionen hinaus. Dies setzt eine durchgängige und medienbruchfreie Gestaltung der Prozesse, Infrastrukturen und Anwendungen, sowie die Etablierung von einheitlichen technischen Schnittstellen voraus. [IMMO 4]
- Die Umsetzung eines gemeinsamen Standards für ein flexibles Identitätsmanagement unter Beibehaltung der Verantwortlichkeiten der einzelnen Institutionen für ihre Mitarbeiterinnen und Mitarbeiter. [IMMO 5]
- Verwendung sicherer Kommunikationsmittel im Rahmen der gesamten Prozesskette. [IMMO 6]

Ziele im Bereich IT-Sicherheit

- Ein wichtiges Ziel aus dem Bereich der IT-Sicherheit ist die durchgängige Verwendung von angemessener und standardisierter Verschlüsselung bzw. elektronischer Signatur. Es muss dabei die organisationsübergreifende Arbeitsteiligkeit berücksichtigt werden. Die Verschlüsselungsverfahren sollen dabei transparent einsetzbar sein. Signaturen müssen jederzeit problemlos überprüfbar sein. Es ist eine Ausgewogenheit zwischen Sicherheit, Kosten und Benutzbarkeit notwendig. [IMMO 7]
- Ein weiteres Ziel adressiert die Nutzung standardisierter Schnittstellen im Rahmen der Gestaltung von Level-1 Prozessketten. Weiterhin ist es sinnvoll zur Optimierung der externen Schnittstellen (s. o.), Verfahren wie ELENA (Elektronischer Entgeltnachweis) in die Level-1 Prozesskette zu integrieren. Hierüber könnte z. B. der Einkommensnachweis der Kundinnen oder des Kunden in elektronischer Form der Kreditbank zur Verfügung gestellt werden. Die Freigabe der Daten erfolgt auch hier mittels elektronischer Signatur. [IMMO 8]

Zielsetzung aufgrund der juristischen Perspektive

Aus juristischer Sichtweise steht die Einhaltung gesetzlicher Normen und Vorschriften als grundlegende Zielsetzung fest. Dies bedeutet die Gestaltung und Umsetzung von Level-1 Prozessketten darf nicht gegen Gesetze, Normen, Verordnungen oder andere rechtlich vorgeschriebene Regelungen verstoßen. [IMMO 9]

Die Beschreibung der oben genannten Ziele zeigt, dass zwischen den einzelnen Zieldimensionen und Zielen zum Teil große Abhängigkeiten bestehen

und es möglicherweise auch zu Zielkonflikten in der realen Umsetzung kommen kann. Daher ist es notwendig, dass im Rahmen des Prozesskettenmanagements die hier aufgeführten Ziele für den konkreten Einzelfall natürlich noch angepasst und mit geeigneten Indikatoren und Messverfahren ergänzt werden müssen, sowie mögliche Zielkonflikte gemanagt werden müssen.

Wie im einleitenden Kapitel dieser Fallstudie gezeigt, läuft der gesamte Wertschöpfungsprozess der privaten Immobilienfinanzierung nicht nur innerhalb der eigenen Organisation ab, sondern bindet arbeitsteilig auch andere Unternehmen (in diesem Fall Institutionen der öffentlichen Verwaltung) ein. Die kontinuierliche Verbesserung der Geschäftsprozesse muss demnach in einer end-to-end-Betrachtung erfolgen, d. h. neben der innerbetrieblichen Prozessoptimierung sind insbesondere auch die Schnittstellen zu anderen Unternehmen (Institutionen der öffentlichen Verwaltung) zu betrachten und zu optimieren.

Daher ist die Anhebung der Betrachtungsebene auf das Level-1 für diese Prozesskette von zentraler Bedeutung. Diese stellt sicher, dass vorhandene Optimierungspotenziale über alle beteiligten Partner identifiziert werden und bildet die Grundlage zur Ableitung von Handlungsempfehlungen, um den angestrebten SOLL-Zustand zukünftig erreichen zu können. Im nachfolgenden Kapitel wird daher auf Basis des Bauplans für Prozessketten des Level-1, die SOLL-Prozesskette für die private Immobilienfinanzierung aufgezeigt.

7.3 Die Prozesskette Level-1

Der dritte Teil dieser Fallstudie adressiert im Rahmen des Vorgehensmodells einen Vorschlag zur Umsetzung einer SOLL-Prozesskette des Level-1 mit Hilfe des Prozessketten Bauplans. Dabei wird vor allem auf die durchgängige Gestaltung der Prozesskette aus fachlicher Sicht, der Gestaltung geeigneter Schnittstellen aus IT-Sicht, der Definition von angemessenen Sicherheitsregelungen für die IT sowie die Berücksichtigung von relevanten gesetzlichen Vorschriften abgezielt.

Das nachfolgende Prinzipbild verdeutlicht die einzelnen Phasen des Lebenszyklus des Geschäftsprozesses "private Immobilienfinanzierung" im SOLL und stellt insbesondere die B2G-Schnittstellen dar, welche die Prozesskette gewöhnlich durchläuft (siehe Abbildung 69).

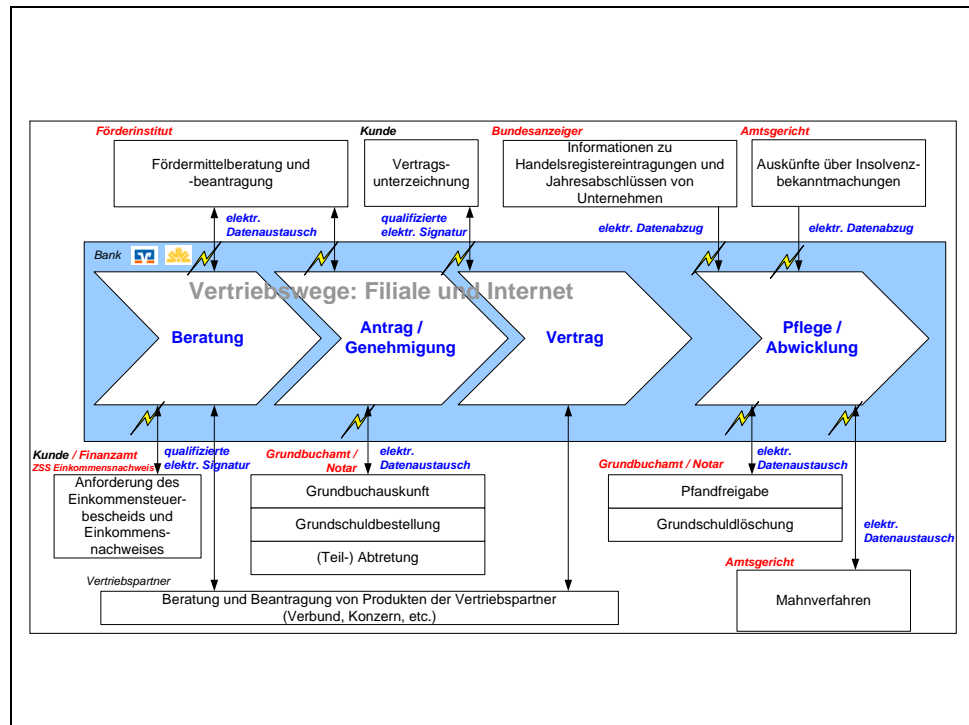


Abbildung 69: IMMO SOLL-Prozesskette zur privaten Immobilienfinanzierung (Quelle: Eigene Darstellung)

Bei der Gestaltung der Prozesskette Level-1 steht nicht die Optimierung der innerbetrieblichen Arbeitsabläufe im Vordergrund, sondern die Betrachtung der B2G-Thematik und damit die organisationsübergreifende Optimierung der gesamten Prozesskette über die verschiedenen Partner hinweg.

Gegenüber der Abbildung des IST- Zustandes erfolgt der Ergebnis- / Datenaustausch zwischen den FDL und den Institutionen der öffentlichen Verwaltung in den einzelnen Phasen des privaten Immobilienfinanzierungsprozesses auf elektronischem Wege.

Entsprechend der Darstellung der IST-Prozesskette wird auch an dieser Stelle wieder auf die drei Sichten fokussiert, um eine ganzheitliche Betrachtung der SOLL-Prozesskette durchzuführen.

7.3.1 Wirtschaftliche, prozessuale und organisatorische Beschreibung und Analyse

Die nachfolgende Abbildung zeigt die Prozesskette einer Kreditvergabe (**Neugeschäftsprozess**) zum Zwecke einer privaten Immobilienfinanzierung im SOLL.

In den Schnittstellen erfolgt die Ergebnisübergabe zwischen den einzelnen Akteuren medienbruchfrei und weitestgehend automatisiert (siehe Abbildung 70 bis Abbildung 72).

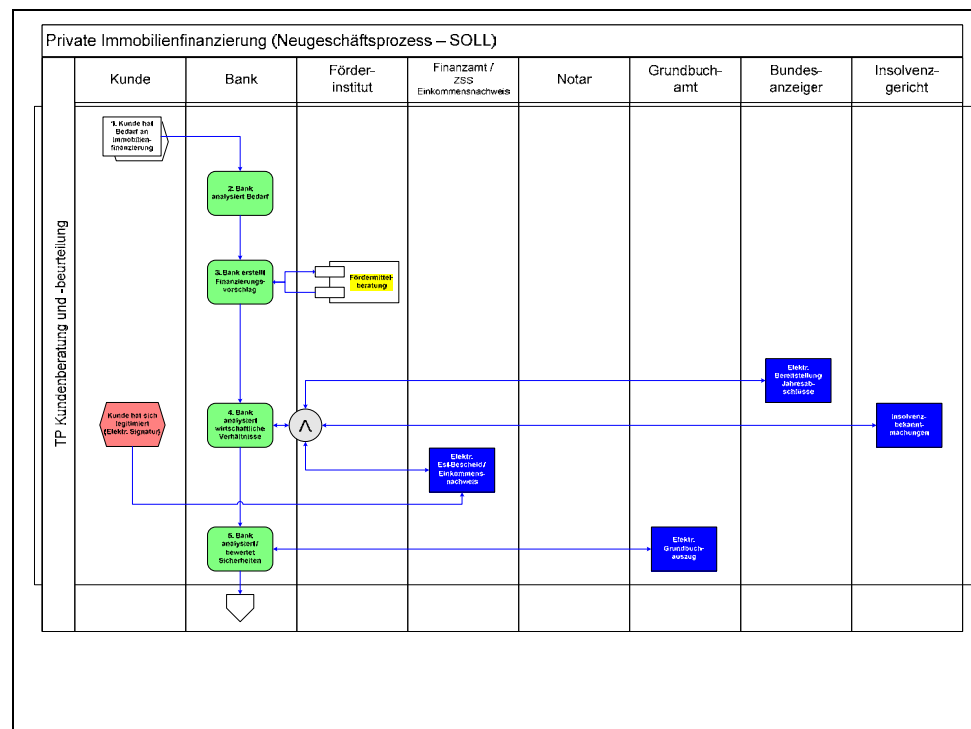


Abbildung 70: IMMO SOLL-Prozesskette private Immobilienfinanzierung I (Quelle: Eigene Darstellung)

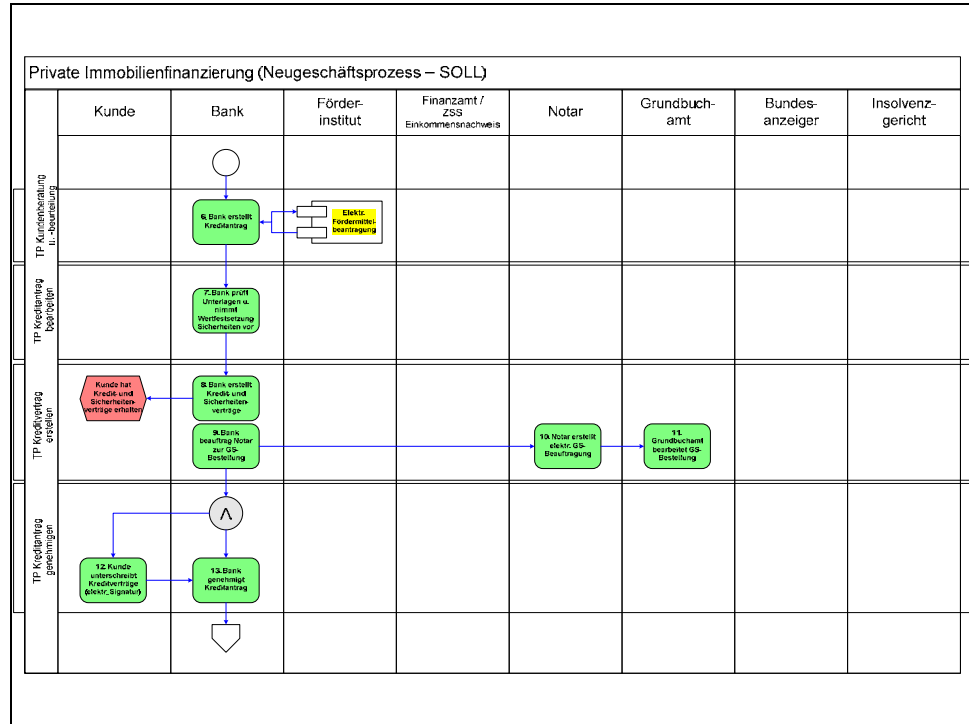


Abbildung 71: IMMO SOLL-Prozesskette private Immobilienfinanzierung II (Quelle: Eigene Darstellung)

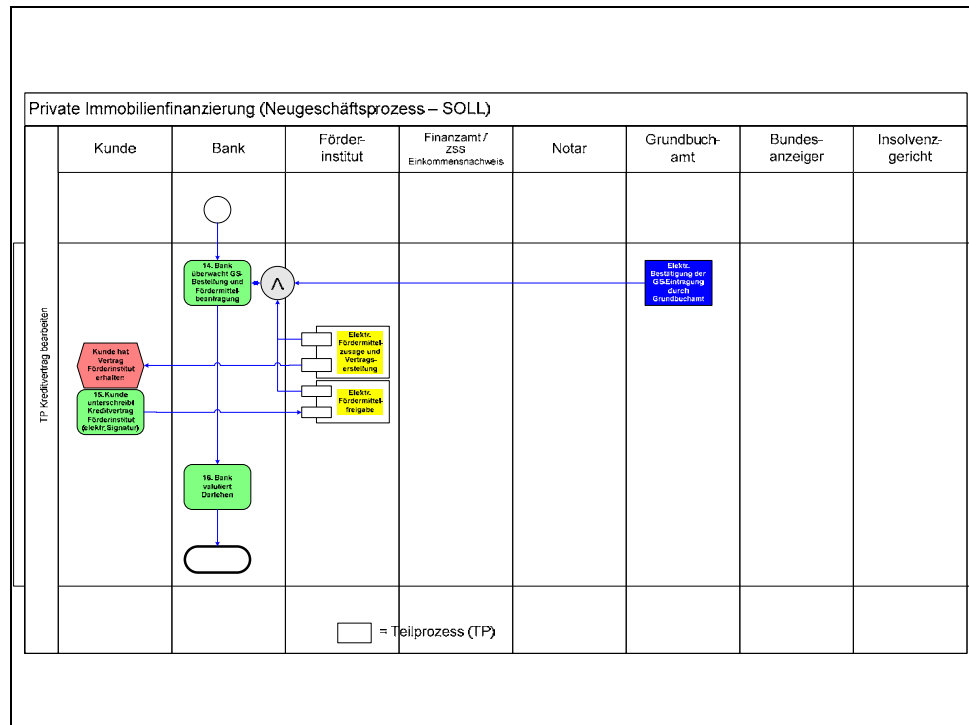


Abbildung 72: IMMO SOLL-Prozesskette private Immobilienfinanzierung III (Quelle: Eigene Darstellung)

Die Beschreibung der Prozesskette erfolgt auf Ebene der Teilprozesse unter besonderer Herausstellung der B2G-Schnittstellenthematik.

Teilprozess " Kundenberatung und -beurteilung"

Der Teilprozess "Kundenberatung und -beurteilung" beinhaltet die Beratung über die Finanzierung (mit bankeigenen Produkten und / oder öffentlichen Fördermitteln) einer privat genutzten Immobilie, inklusive der anschließenden Beurteilung der Kreditwürdigkeit von Kundinnen und Kunden.

Die **Fördermittelberatung** ist integrativer Bestandteil der allgemeinen Finanzierungsberatung (siehe Abbildung 73):

- Über eine elektronische Beratungsplattform erfolgt der Zugriff auf alle jeweils gültigen Fördermittelprogramme und deren Konditionen.
- Bereits in der Finanzierungsberatung erfasste Daten / Informationen zu Kunden bzw. zum Gesamtfinanzierungskonzept (insbes. zum Finanzierungszweck) werden automatisiert in die Fördermittelberatung übernommen.

- Auf Basis dieser Daten / Informationen erfolgt die konkrete Fördermittelberatung mit dem Ergebnis eines Finanzierungsvorschlags, der dann automatisiert als Bestandteil des Gesamtfinanzierungskonzepts im Bankverfahren zur Verfügung steht.
- Mit Akzeptanz des Gesamtfinanzierungskonzepts durch Bank und Kundinnen und Kunden erfolgt elektronisch die Beantragung der Fördermittel bei dem jeweiligen Förderinstitut.

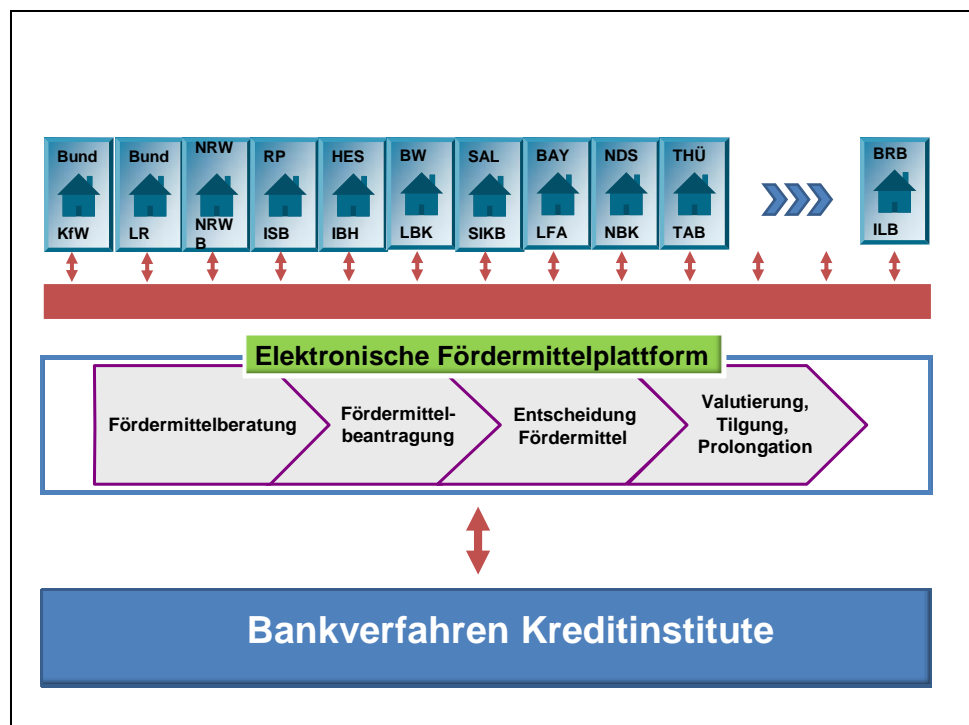


Abbildung 73: IMMO Prinzipbild Fördermittelberatung-Beantragung (Quelle: Eigene Darstellung)

Zur Beurteilung der wirtschaftlichen Verhältnisse werden berücksichtigt:

- Der Einkommensnachweis
Der elektronisch in einer zentralen Speicherstelle (ZSS Einkommensnachweis) zur Verfügung stehende Einkommensnachweis wird mit Einwilligung von Kunden (Legitimation erfolgt über eine qualifizierte elektronische Signatur auf einer Signaturkarte) dem anfragenden Kreditinstitut elektronisch zur Verfügung gestellt. Die Daten zum Einkommensnachweis werden in der Kundenakte im Bankverfahren hinterlegt.

- **Der Einkommensteuerbescheid**
Der elektronisch bei dem für Kundinnen und Kunden zuständigen Finanzamt zur Verfügung stehende Einkommensteuerbescheid wird mit Einwilligung der Kundin oder des Kunden (Legitimation erfolgt über eine qualifizierte elektronische Signatur auf einer Signaturkarte) dem anfragenden Kreditinstitut zur Verfügung gestellt. Die Daten zum Einkommensteuerbescheid werden in der Kundenakte im Bankverfahren hinterlegt.
- **Die Insolvenzbekanntmachung**
Das jeweilige Kreditinstitut ist gesetzlich verpflichtet, permanent zu prüfen, für welche ihrer Kundinnen oder Kunden bzw. potentielle Kundinnen oder Kunden (z. B. Nichtkunde als Interessent für eine Finanzierungsberatung) das Insolvenzverfahren eröffnet wurde.
Die auf **einer** elektronischen Plattform zur Verfügung stehenden Informationen zu Insolvenzbekanntmachungen **aller** bundesdeutschen Insolvenzgerichte können automatisiert und (nach bestimmten Kriterien, z. B. nach Postleitzahlgebieten) sortiert ausgelesen werden und für Zwecke des Kreditinstitutes weiter verwendet werden.
- **Die Jahresabschlüsse**
Zur Beurteilung der wirtschaftlichen Verhältnisse kommen die Jahresabschlüsse nur dann zum Tragen, wenn ein Mitverpflichteter an der privaten Immobilienfinanzierung Gesellschafter eines Unternehmen ist und dessen wirtschaftlichen Verhältnisse auch maßgeblich für die Beurteilung der Immobilienfinanzierung sind.
Die Abschlüsse (Bilanzen), sofern sie in Deutschland publiziert sind, werden auf elektronischem Weg beim Bundesanzeiger angefordert und für Zwecke des Kreditinstitutes weiter verwendet (z. B. Grundlage für Bilanzanalysen und für Ratings).
- **Der Grundbuchauszug**
Die elektronische Anforderung eines aktuellen Grundbuchauszuges vom Grundbuchamt dient zur Analyse bzw. Bewertung der für die private Immobilienfinanzierung gestellten dinglichen Sicherheiten. Auf Basis der Objektdaten wird das zuständige Grundbuchamt (Amtsgericht) automatisch ermittelt. Die konkrete Ausgestaltung der Prozesse zur elektronischen Grundbuchauskunft und Grundschuldbestellung bzw. Grundschuldabtretung obliegt dem Projekt IFD (Initiative Finanzstandort Deutschland, www.finanzstandort.de). Die Initiative Finanzstandort Deutschland (IFD) hat sich zum Ziel gesetzt, den deutschen Finanzstandort mit Innovationen, Impulsen und Reformvorschlägen zu fördern. Ein Teilgebiet der IFD-Initiative ist unter anderem die Optimierung übergreifender Geschäftsprozesse hier im Bereich der Grundbuchauskunft

und Grundschuldbestellung bzw. Grundschuldabtretung und -löschung. Die Umsetzung der Projektergebnisse ist für die Jahre 2010 - 2012 geplant.

Teilprozess "Kreditantrag bearbeiten"

Der Teilprozess "Kreditantrag bearbeiten" beinhaltet die Prüfung und die Bewertung des Kreditantrages und der Sicherheiten. Eine Grundlage für die Bewertung der Sicherheiten kann die Objektbesichtigung sein.

Eine Interaktion mit Institutionen der öffentlichen Verwaltung findet in diesem Teilprozess nicht statt.

Teilprozess "Kreditvertrag erstellen"

Der Teilprozess "Kreditvertrag erstellen" beinhaltet den Druck der Kredit- und Sicherheitenverträge und die Vorbereitung des Kreditantrages für eine Kreditgenehmigung.

Darüber hinaus erfolgt in dieser Prozessphase die Initiierung und Abwicklung der **Grundschuldbestellung**. Ggf. kann die Sicherheitenhereinnahme auch im Rahmen einer Grundschuldabtretung erfolgen.

- Das Kreditinstitut versendet elektronisch den Auftrag zur Bestellung der Grundschuld an den Notar. Die für den Auftrag notwendigen Objekt- und Kundendaten werden automatisiert den Kreditantragsunterlagen entnommen. Die für die Bestellung zuständige Notare werden ebenfalls automatisiert ermittelt bzw. wird von den Kundinnen und Kunden vorgegeben.
- Nach erfolgtem Präsenztermin zwischen Kundinnen und Kunden und Notaren zur Beurkundung bzw. Beglaubigung, beantragen Notare auf elektronischem Weg die Eintragung der Grundschuld beim Grundbuchamt.

Teilprozess "Kreditantrag genehmigen"

Der Teilprozess beinhaltet die Kreditgenehmigung und die Einholung der Unterschrift von Kundinnen und Kunden.

Die Kreditverträge werden von Kundinnen und Kunden mit **qualifizierter Signatur** unterschrieben.

Teilprozess "Kreditvertrag bearbeiten"

Der Teilprozess beinhaltet die Prüfung der Finanzierungsvereinbarungen (insbes. der Sicherheitenstellung) und die Auszahlung der Darlehensmittel.

Das **Grundbuchamt** nimmt die Eintragung der beantragten Grundschuld im elektronischen Grundbuch vor und übermittelt auf elektronischem Weg den Vollzug der Eintragung und die zur Eintragung gekommenen Daten an den Notar und das Kreditinstitut. Die an das Kreditinstitut übermittelten Daten zur Grundschuld aktualisieren automatisch die Objekt- und Sicherhendaten im Bankverfahren.

Das **Förderinstitut** erteilt auf elektronischem Weg die Kreditzusage und stellt den abgeschlossenen Kreditvertrag elektronisch bereit. Die Kundin oder der Kunde unterschreibt mit qualifizierter elektronischer Signatur.

Mit geleisteter Unterschrift der Kundin oder des Kunden wird automatisch eine Nachricht an das Kreditinstitut generiert. Dies initiiert automatisch die weiteren Bearbeitungsschritte (z. B. Anlage der Fördermittelkonten) im Bankverfahren.

Die freigegebenen Fördermittel werden z. B. nach Baufortschritt elektronisch beim Förderinstitut abgerufen. Die darauf folgenden Bearbeitungsschritte (Mittelauszahlung, Verbuchung der Fördermittel etc.) beim Kreditinstitut werden im Bankverfahren automatisch gestartet.

Nach kompletter Auszahlung der Darlehensmittel und Erfüllung aller Finanzierungsvereinbarung (inkl. der Sicherheitenbestellung) ist der Neugeschäftsprozess abgeschlossen.

Während der Darlehenslaufzeit kommen nunmehr die Maßnahmen zur "Überwachung" des Darlehens im Rahmen des **Pflegeprozesses** zum Tragen.

Die nachfolgenden Abbildungen zeigen die Prozessketten zur "Überwachung" eines bestehenden Kreditgeschäftes (Pflegeprozess) im SOLL (siehe Abbildung 74 bis und Abbildung 76).

Teilprozess "Bonitätsunterlagen auswerten"

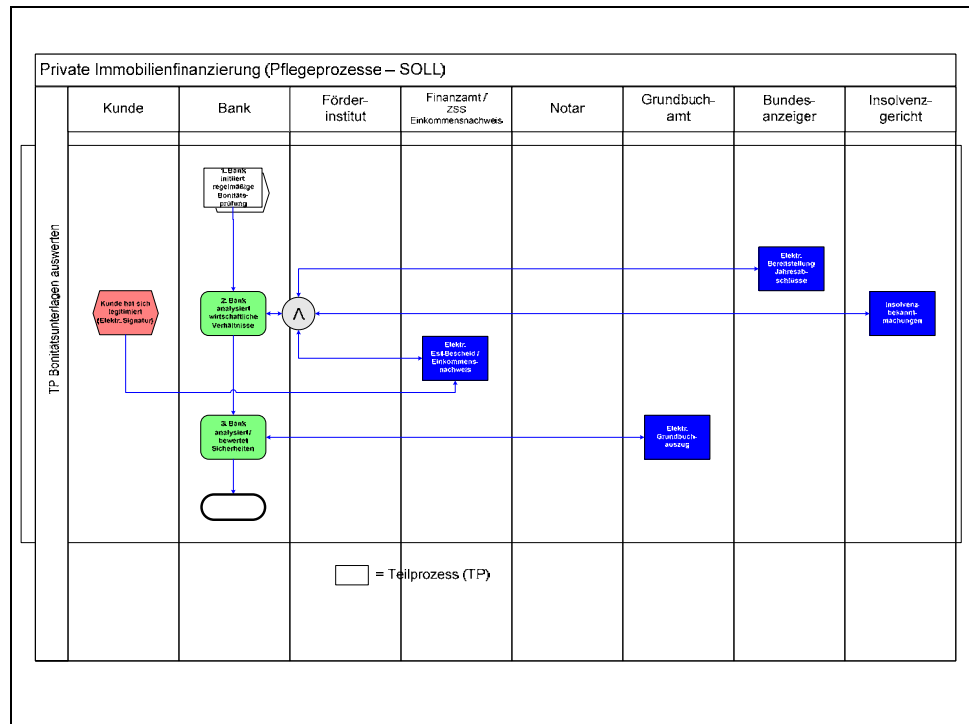


Abbildung 74: IMMO SOLL-Prozesskette private Immobilienfinanzierung Pflegethemen (Quelle: Eigene Darstellung)

Zur laufenden **Beurteilung der aktuellen wirtschaftlichen Verhältnisse** werden von Kreditnehmerinnen und Kreditnehmern zu definierten Stichtagen entsprechende Unterlagen angefordert. Die Details hierzu sind bereits im Teilprozess "Kundenberatung und -beurteilung" dargestellt worden.

- Der Einkommensnachweis (Erläuterungen dazu siehe Ausführungen zum SOLL-Prozess Neugeschäft)
- Der Einkommensteuerbescheid (Erläuterungen dazu siehe Ausführungen zum SOLL-Prozess Neugeschäft)
- Die Insolvenzbekanntmachung (Erläuterungen dazu siehe Ausführungen zum SOLL-Prozess Neugeschäft)

- Die Jahresabschlüsse
(Erläuterungen dazu siehe Ausführungen zum SOLL-Prozess Neugeschäft)
- Der Grundbuchauszug
Die elektronische Anforderung eines aktuellen **Grundbuchauszuges vom Grundbuchamt** dient zur Analyse, ob weitere Eintragungen im Grundbuch eine Neubewertung der für die private Immobilienfinanzierung gestellten dinglichen Sicherheiten notwendig macht. Auf Basis der Objektdaten wird das zuständige Grundbuchamt (Amtsgericht) automatisch ermittelt.

Teilprozess "Rückständigkeit bearbeiten"

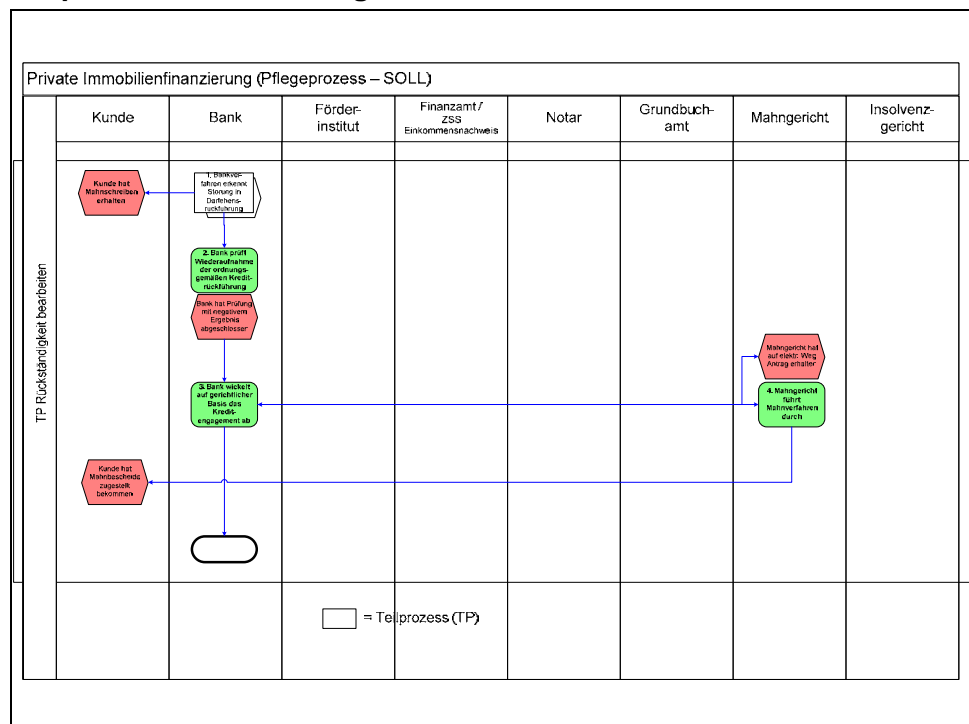


Abbildung 75: IMMO Teilprozess Rückständigkeit (Quelle: Eigene Darstellung)

Eine Zahlungsstörung bzw. Rückständigkeit in der Darlehensrückführung durch Kundinnen oder Kunden wird vom operativen Bankverfahren erkannt. Kunden werden darüber durch sog. Mahnschreiben, die er von der Bank in entsprechenden Zeiträumen erhält, informiert. Kann mit den Kundinnen oder Kunden dann immer noch keine Einigung erzielt werden, die ordnungsgemäße Rückführung des Darlehens wieder aufzunehmen, geht das Engagement in die Abwicklung, d. h. ein Mahnverfahren wird eingeleitet.

Die **Abwicklung des Mahnverfahrens** (Antrag Mahnbescheid bis Titulierung) erfolgt im bidirektionalen elektronischem Datenaustausch mit den zentralen **Mahngerichten** in der Bundesrepublik Deutschland und im Rahmen des Europäischen Mahnverfahrens.

Die Daten bzw. Informationen, die zur Beantragung des Mahnbescheides notwendig sind, werden dem operativen Bankverfahren entnommen bzw. umgekehrt geltend für die Daten / Informationen, die von den Mahngerichten übermittelt werden.

Teilprozess "Darlehensvertrag auflösen"

Der Teilprozess "Darlehensvertrag auflösen" wird durch den Wunsch von Kundinnen oder Kunden zur vorzeitigen Auflösung des Darlehensvertrages initiiert. Der Kreditgeber prüft die Möglichkeit zur vorzeitigen Beendigung des Kreditengagements und wickelt die Auflösung des Darlehensvertrages, ggf. unter Berücksichtigung einer Vorfälligkeitsentschädigung ab.

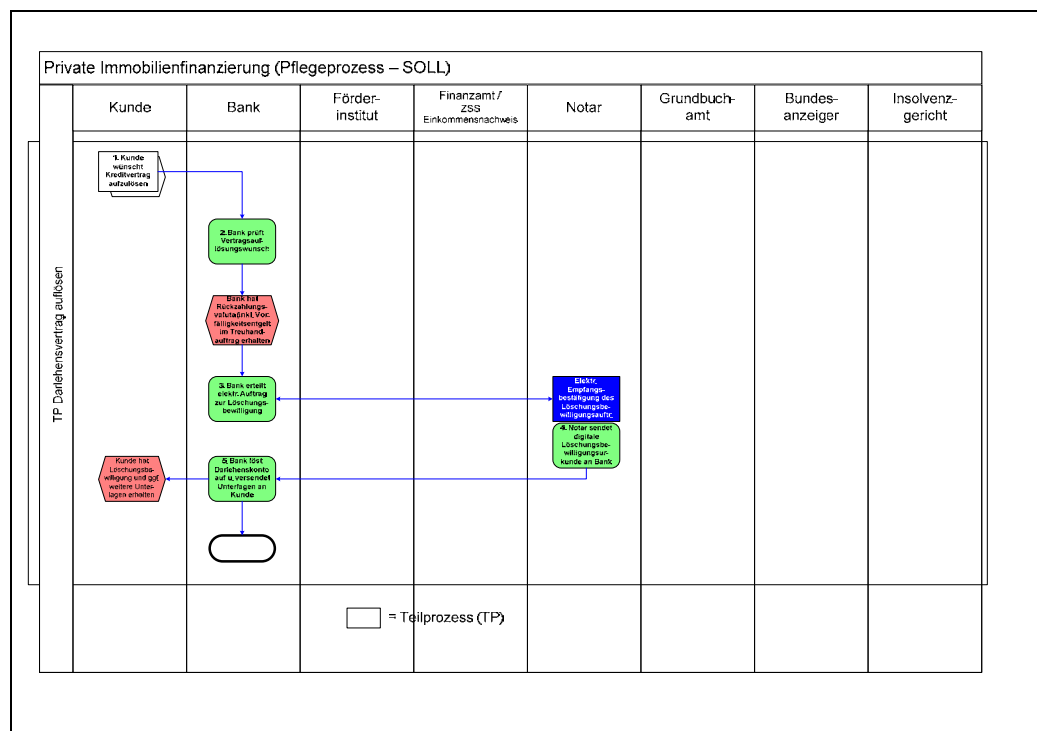


Abbildung 76: IMMO SOLL-Prozess Vertragsauflösung (Quelle: Eigene Darstellung)

Der Auftrag zur Erteilung der Löschungsbewilligung ergeht auf elektronischem Weg an das definierten Notariat. Die für die (elektronische) Ausstel-

lung des Auftrages zur Löschungsbewilligung notwendigen Daten werden dem operativen Bankverfahren entnommen.

Der Empfang des Löschungsbewilligungsauftrages werden durch Notare elektronisch quittiert.

Nach Erstellung der Löschungsbewilligungsurkunde (im Notarverfahren) wird diese in digitaler Form an das Kreditinstitut versandt.

Nach Prüfung durch das Kreditinstitut erhält der Kunde die Löschungsbewilligungsurkunde (in digitaler Form) und ggf. weitere Unterlagen, die aufgrund des aufgelösten Darlehensvertrages von der Bank nicht mehr benötigt werden.

Die vorangegangenen Beschreibungen der Teilprozesse haben den angestrebten SOLL-Zustand für die Prozesskette private Immobilienfinanzierung aufgezeigt. Ergänzend zu dieser fachlichen Beschreibung, werden in den folgenden Abschnitten auf die IT-Architekturen sowie auf Aspekte zur IT-Sicherheit und rechtliche Rahmenbedingungen fokussiert.

7.3.2 IT-architektonische Beschreibung und Analyse

Die IT-architektonische Perspektive beschreibt die zuvor dargestellte Prozesskette aufgrund einer IT-bezogenen Sichtweise. Die Ausführungen zeigen das Zusammenspiel der unterschiedlichen Systeme und Anwendungen dar, die bei den Prozessbeteiligten im Einsatz sind. Entsprechend den Ausführungen zur IST-Prozesskette, werden auch an dieser Stelle wieder die beiden Beispielprozessketten Förderinstitut sowie Grundbuchamt beschrieben.

Das Förderinstitut

Das SOLL kann grob wie in Abbildung 77 dargestellt werden. Statt papierne Dokumente werden strukturierte maschinenlesbare XML-Dokumente ausgetauscht. Falls eine Institution bereits eine Schnittstelle über PDF-Formulare bereitstellt, kann diese natürlich genutzt werden.

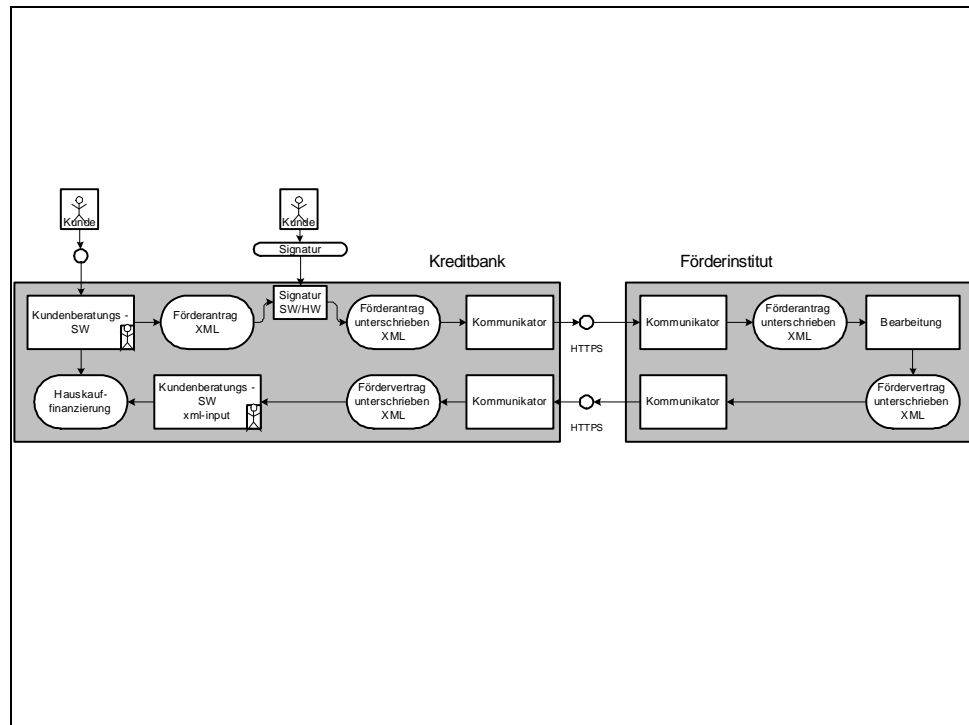


Abbildung 77: IMMO SOLL-Architektur Förderinstitut (Quelle: Eigene Darstellung)

Voraussetzung dafür ist erstens, dass die Antrags- und Vertragsdaten strukturiert werden können, was aber schon durch die interne elektronische Verarbeitung gegeben ist. Ggf. müssen die Datenformate bei der Kommunikation Semantik erhaltend transformiert werden. Möglicherweise wird im Kommunikator eine zusätzliche Komponente benötigt, um die Daten aus PDF-Formularen zu extrahieren. Mit Kommunikator werden hier ganz allgemein die Komponenten zusammenfassend bezeichnet, die neu geschaffen werden müssen, um die Kommunikation elektronisch zu ermöglichen. In dem Architekturmuster in der Abbildung 78 sind sie Client und Webservice genannt.

Die zweite Voraussetzung ist die Rechtssicherheit der Dokumente. Dazu muss die Identität aller Beteiligten feststellbar und dokumentierbar sein. Die Dokumente bzw. Teile daraus müssen elektronisch signiert werden können und der Inhalt muss unveränderbar sein. Technisch kann dazu der Standard XML-Signature verwendet werden. Wenn in der Umgebung des Systems schon der Standard PKCS 7 verwendet wird, so kann auch dieser hier eingesetzt werden. Benötigt wird eine qualifizierte elektronische Signatur nach SigG, wenn Verträge elektronisch ausgetauscht werden sollen, sonst reicht möglicherweise auch eine fortgeschrittene Signatur.

Für die Signatur gibt es zukünftig verschiedene Möglichkeiten:

- Smartcards der Banken (oder anderer akkreditierter Anbieter),
- der elektronische Personalausweis (ePA),
- die elektronische Gesundheitskarte,

Nicht alle aufgeführten Möglichkeiten enthalten die Signatur obligatorisch. Die Verbreitung und Akzeptanz ist ebenfalls offen. Die Smartcards der Banken dürften aber durchsetzbar sein.

Auf jeden Fall wird für die allgemeine Nutzung der Signatur eine dritte Partei, die nicht mit eingezeichnet ist, benötigt. Ein Trust Center muss mit eingebunden werden, zur Überprüfung der Gültigkeit der Zertifikate und der Abfrage der öffentlichen Schlüssel von Kundinnen oder Kunden.

Unter der Vorgabe, dass die internen Netze der Kreditbank und des Förderinstituts als sicher zu betrachten sind, ist weiterhin eine Transportverschlüsselung notwendig. Hier reicht keine einfache HTTPS-Verbindung aus, sondern im Rahmen des dazu notwendigen Identity-Managements ist eine zertifikatsbasierte Client-Authentifizierung notwendig.

Die Komponente "Kundenberatungs-SW xml-input" ist eine neu einzubindende Komponente, die mehr oder weniger automatisch arbeiten könnte. Eine analoge Komponente beim Förderinstitut ist für die bessere Lesbarkeit nicht eingezeichnet worden.

Die Kommunikatoren sollten nach dem SAGA-Standard für die öffentliche Verwaltung als Client / Server Webservices ausgeführt werden (siehe Abbildung 78). Sie können synchron und asynchron arbeiten. In dem Fall, dass Anträge wirklich noch fachlich bearbeitet werden, wird sicher eine asynchrone Schnittstelle gewählt werden müssen (siehe Abbildung 78).

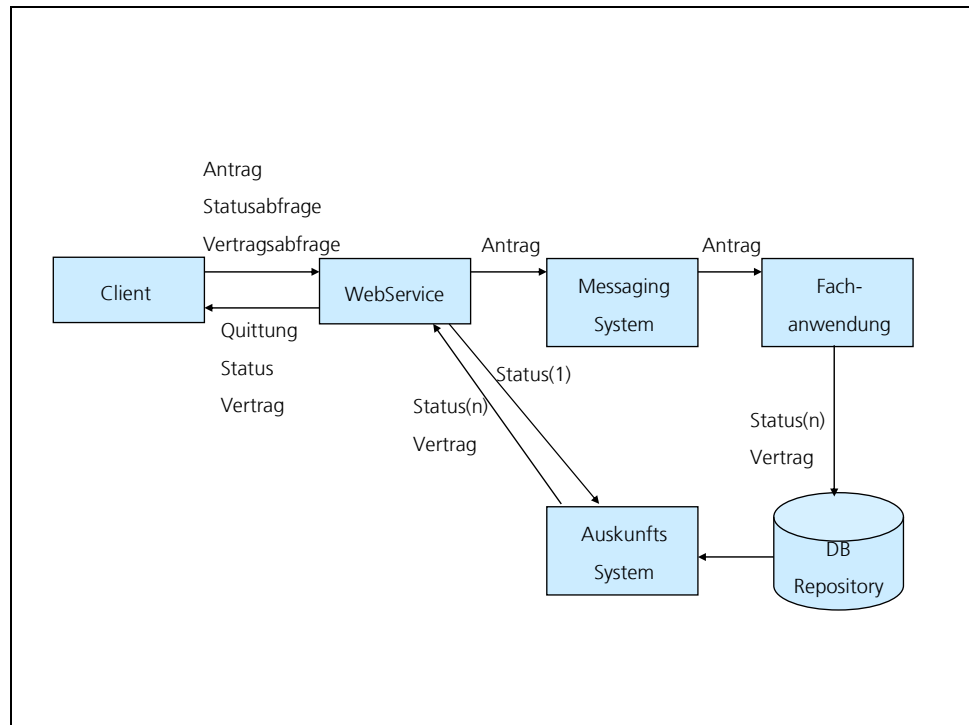


Abbildung 78: IMMO Das Architekturmuster für die Kommunikation mit dem Förderinstitut (Quelle: Eigene Darstellung)

Im asynchronen Fall muss man entscheiden, ob auf beiden Seiten Webservices eingerichtet werden und damit beide Seiten aktiv werden können oder ob die Kreditbank den Vertrag regelmäßig versucht abzuholen (möglicherweise auch nach einer entsprechenden Information).

Für die Schnittstelle des Webservice kommen die folgenden Varianten in Frage.

Erstens ein Server mit der Funktionalität:

- rechtsverbindlichen Antrag stellen (einschließlich einer rechtsverbindlichen Empfangsbestätigung)
- Status des Antrags abfragen
- rechtsverbindlichen Vertrag, Auskunft, Urkunde abholen (eventuell nach einer Information über einen anderen Kanal)

Im zweiten Fall, wird auch auf der ursprünglichen Client-Seite ein Server bereitgestellt. Beim ersten Server entfällt dann das Abholen des Vertrags. Der zweite Server bekommt bei Bedarf eine erweiterte Schnittstelle:

- Rückfrage einstellen
- Rechnung einstellen
- rechtsverbindlichen Vertrag, Auskunft, Urkunde einstellen

Für den Fall, dass kleinere Institutionen bzw. Bürgerinnen und Bürger, die verständlicherweise keine eigene Webservices bereitstellen können, mit Institutionen kommunizieren müssen, die ihrerseits kein Web-Portal dafür bereitstellen, könnten auch elektronische Postfächer oder "Dokumentensafes", wie z. B. das Bürgerportal oder ähnliche Dienste der Banken, zum Einsatz kommen. Diese könnten analog wie die elektronischen Postfächer der Justiz und der Handelsregister genutzt werden und bieten ähnliche Sicherheitsstandards.

Für die Webservices gibt es bereits verschiedene Lösungen (bzw. sind geplant), die ähnlich aussehen (siehe Tabelle 18) aber sehr unterschiedlich realisiert worden sind, besonders bzgl. Identity- und Access-Management. Hier sollte nach dem Vorschlag aus dem Projekt SAFE (siehe Kap. 4.2.3) ein einheitlicher Standard eingeführt werden. Wie weit die Lösungen intern dem vorgeschlagenen Muster entsprechen ist nicht für alle bekannt. Es ist möglich, dass es sich teilweise nur um intelligentere File System Repositories handelt und der Arbeitsablauf zzt. noch durch organisatorische Vorschriften statt durch ein Messaging System oder Vorgangsbearbeitungssystem gesteuert wird.

	BB ExtraNet	BaFin MVP	Grundbuchamt	Justiz (elektronisches Gerichtspostfach EGPV)	eVA
Zulassung	Sichere Authentisierung und Authentifizierung für Zulassung zum Verfahren zum Verfahren notwendig (einmalig, Erteilung des Account)	Sichere Authentisierung und Authentifizierung für Zulassung zum Verfahren notwendig (einmalig, Erteilung des Account)	Sichere Authentisierung und Authentifizierung für Zulassung zum Verfahren notwendig (einmalig, Erteilung des Account)	Registrierung und qualifizierte elektronische Signatur für Zulassung zum Verfahren notwendig	Kanal 1: keine Kanal 2: ja je FDL ein Nutzer
Anmeldung	user / password	user / password smartcard	user / password / Bearbeiterkennzeichen	smartcard	User / Password
Sicherheit (Kommunikation)	HTTPS, SSL, Server-Zertifikat	HTTPS, SSL, Client- und Server-Zertifikat	HTTPS, Server-Zertifikat	HTTPS, SOAP, OSCI	Kanal 1: HTTPS Kanal 2: HTTPS / SOAP
Client	Webbrowser oder Fachanwendung mit spezieller Schnittstelle	Webbrowser oder Fachanwendung mit spezieller Schnittstelle	Spezieller Client oder Webbrowser	Spezieller Client	Kanal 1: Webbrowser Kanal 2: Fachanwendung mit spezieller Schnittstelle
Kommunikationsart	Daten (XML Dokument) einstellen und abholen	Daten (XML Dokument) einstellen und abholen	Daten ansehen und drucken kein Messaging-System	Daten (XML Dokument) einstellen und abholen	Daten (XML Dokument) einstellen (und abholen)
Repository	Filesystem	Filesystem	SolumSTAR (Siemens)	Mailsystem, Filesystem	Filesystem, VBS, DB
Messaging System	Unbekannt	Unbekannt	Nicht enthalten	Nicht enthalten	VBS

Tabelle 18: Empirische Varianten der Kommunikation in Prozessketten

Weitere Varianten sind möglich, wenn statt XML-Dokumente signierte PDF-Dokumente ausgetauscht werden. Dann hätte man aber den Nachteil, dass eine automatische Übernahme und Verarbeitung der Daten nicht oder nur über weitere extrahierende Komponenten möglich ist. Damit bliebe nur der Vorteil der schnellen Kommunikation und des papierlosen Büros.

Grundbuchamt

Für die SOLL-Architektur wird der gleiche Lösungsansatz wie für das Förderinstitut verfolgt (siehe vorangegangenen Abschnitt). Das Architekturmuster für die Kommunikation mit dem Grundbuchamt ist in Abbildung 79 dargestellt.

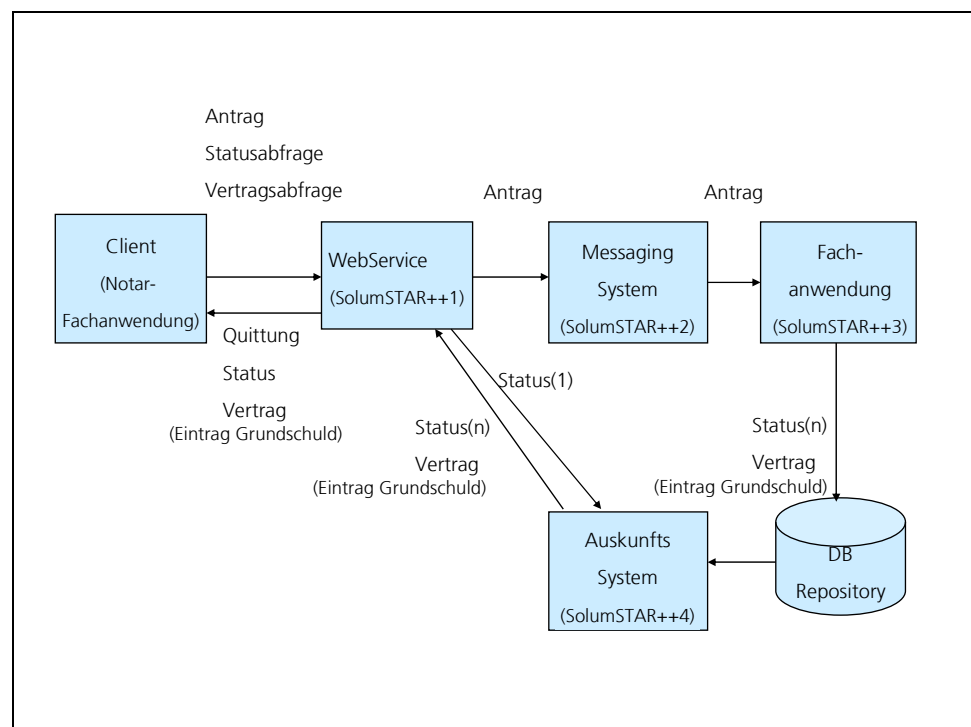


Abbildung 79: IMMO Das Architekturmuster für die Kommunikation mit dem Grundbuchamt (Quelle: Eigene Darstellung)

Man kann diese Vorgänge durch Umstellung auf Webservices, die XML-Dokumente akzeptieren und ausliefern, automatisieren (siehe Abbildung 80).

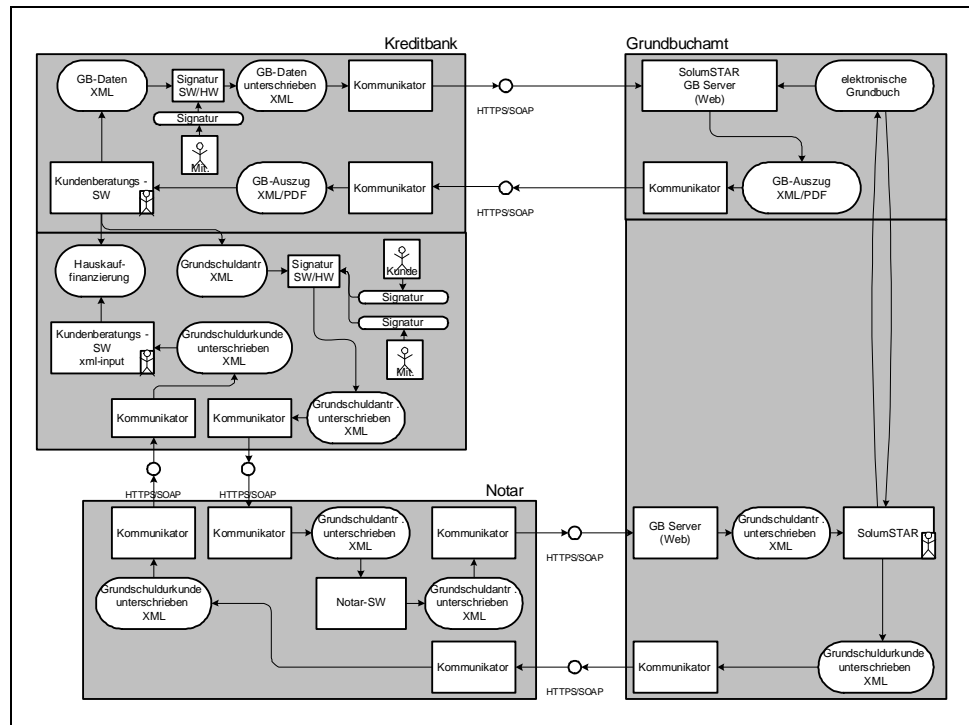


Abbildung 80: IMMO SOLL-Architektur Grundbuchamt (Quelle: Eigene Darstellung)

Wie auch schon in den anderen Architekturabbildungen fehlt hier die Infrastruktur für die Sicherheit (Zertifikat-, Identity-Management). Neue Sicherheitsmechanismen müssen zwischen den Kommunikatoren bzw. zwischen Kommunikator und Server eingeführt werden. Innerhalb der Institutionen werden Schutzanalyse und Sicherheitsvorkehrungen vorausgesetzt.

Die Zertifikate werden für die Unterschriften bzw. für die Authentifizierung benötigt.

Wie gezeigt, spielen in diesen Prozessketten Sicherheitsaspekte eine wichtige Rolle. Aus diesem Grund adressiert der folgende Abschnitt die wesentlichen Aspekte zur IT-Sicherheit, welche im Rahmen der dargestellten Prozessketten zu berücksichtigen sind.

7.3.3 Sicherheitstechnische Beschreibung und Analyse

Datenaustausch Förderinstitut

Der Datenaustausch findet über eine verschlüsselte Verbindung statt. Hierzu sollen neben dem obligatorischem HTTPS Client-Zertifikate zur sicheren Authentifizierung der Kommunikationspartner verwendet werden. Dazu können die heute verfügbaren Smartcards zur Signatur (fortgeschrittene oder qualifizierte Signatur) oder in Zukunft auch der ePA verwendet werden. Auch für die SOA-Kommunikation sollen mindestens softwarebasierte Zertifikate auf Clientseite verwendet werden.

Es ist zu beachten, dass angemessene Verfahren zur Verschlüsselung und Signatur verwendet werden. Es sollte also im Rahmen der gesetzlichen Möglichkeiten die fortgeschrittene elektronische Signatur verwendet werden, um den Aufwand gering zu halten. Sollte ein Kommunikationspartner ein Token zur qualifizierten Signatur (wie z. B. der ePA) zur Verfügung haben, müssen dieses auch verwendbar sein. Bei der Verwendung von XML-Dokumenten sollte der Standard XML-Signature verwendet werden.

Datenaustausch elektronisches Grundbuch

Der Datenaustausch mit dem Grundbuchamt besteht nicht mehr aus den zwei Teilprozessen, die Einsicht in das Grundbuch und das Bestellen einer Grundschuld, sondern wird zu einer Prozesskette zusammengefasst, wobei den Notariaten in ihren Rollen entsprechend berücksichtigt werden. Für die Kommunikation zwischen Grundbuchamt und Notariat ist, abgesehen von der Grundbuch-Einsicht, die qualifizierte Signatur notwendig. Es sind auch dementsprechende Verschlüsselungsverfahren zu verwenden – für die Transport-Verschlüsselung müssen Client-Zertifikate eingesetzt werden. Alle Teilprozessketten im Umfeld der Grundschuldbestellung sollten nach IT-Grundschutz zertifiziert werden.

7.3.4 Juristische Beschreibung und Analyse

Die verpflichtende Schriftform beim Verbraucherdarlehensvertrag (§ 492 BGB) macht eine Nutzung auf webbasierten Plattformen unflexibel.

Vergleichbare und zum Teil höhere Rechtssicherheit zur Nutzung sowohl im Internet als auch in der Bankfiliale brächte die flächendeckende Einführung der elektronischen Signatur. Die elektronische Signatur kann mit elektronisch vorliegenden Daten bzw. Informationen verknüpft werden und ermög-

licht, die Identifikation von Aussteller der Daten sowie die Prüfung der Integrität der Daten. Die elektronische Signatur in Bezug auf Daten entspricht damit technisch der handschriftlichen Unterschrift unter ein papierenes Dokument.

Der Bundesgesetzgeber hat in den letzten Jahren die erforderlichen Rechtsgrundlagen dafür geschaffen, neben der Schriftform eine elektronische Form einzusetzen.

Die Rechtsgrundlage für die elektronische Signatur wurde 1997 (damals noch unter dem Begriff digitale statt elektronische Signatur) mit dem luKDG geschaffen: Gesetz zur Regelung der Rahmenbedingungen für Informations- und Kommunikationsdienste (Informations- und Kommunikationsdienste-Gesetz - luKDG), gültig ab 01.08.1997 (BGBl I 1997, 1870). Das luKDG setzte in seinem Artikel 3 das "Gesetz zur digitalen Signatur" (SigG) in Kraft. Nach "§ 4 SigG Genehmigung von Zertifizierungsstellen" bedurfte der Betrieb einer Zertifizierungsstelle einer Genehmigung der zuständigen Behörde. Die Massenverbreitung von elektronischen Signaturen blieb aus.

Das Signaturgesetz (SigG) wurde 2001 (Signaturgesetz vom 16. Mai 2001) u. a. in Hinblick auf Einführung von genehmigungsfreien Zertifizierungsstellen geändert. Es führte in § 2 SigG (Begriffsbestimmungen) drei Formen von Signaturen ein:

Nr. 1 "elektronische Signaturen"

Nr. 2 "fortgeschrittene elektronische Signaturen"

Nr. 3 "qualifizierte elektronische Signaturen"

Die "qualifizierte elektronische Signatur" ist dabei eine "fortgeschrittene elektronische Signatur", die auf einem zum Zeitpunkt ihrer Erzeugung gültigen qualifizierten Zertifikat beruhen und mit einer sicheren Signaturerstellungseinheit erzeugt wurde.

Siehe dazu auch die Signaturverordnung (SigV) vom 16. November 2001.

Für die Nutzung der elektronischen Signatur im juristischen Umfeld stellt der Gesetzgeber im SigG und SigV bestimmte Anforderungen. Die Ersetzung der gesetzlich vorgeschriebenen Schriftform durch die elektronische Form ermöglicht nur der Einsatz einer qualifizierten elektronischen Signatur (§§ 126, 126a BGB).

§ 126 BGB Schriftform

(1) IST durch Gesetz schriftliche Form vorgeschrieben, so muss die Urkunde von dem Aussteller eigenhändig durch Namensunterschrift oder mittels notariell beglaubigten Handzeichens unterzeichnet werden.

(2) ¹Bei einem Vertrag muss die Unterzeichnung der Parteien auf derselben Urkunde erfolgen. ²Werden über den Vertrag mehrere gleichlautende Urkunden aufgenommen, so genügt

es, wenn jede Partei die für die andere Partei bestimmte Urkunde unterzeichnet.

(3) Die schriftliche Form kann durch die elektronische Form ersetzt werden, wenn sich nicht aus dem Gesetz ein anderes ergibt.

(4) Die schriftliche Form wird durch die notarielle Beurkundung ersetzt.

§ 126a BGB Elektronische Form

(1) SOLL die gesetzlich vorgeschriebene schriftliche Form durch die elektronische Form ersetzt werden, so muss der Aussteller der Erklärung dieser seinen Namen hinzufügen und das elektronische Dokument mit einer qualifizierten elektronischen Signatur nach dem Signaturgesetz versehen.

(2) Bei einem Vertrag müssen die Parteien jeweils ein gleichlautendes Dokument in der in Absatz 1 bezeichneten Weise elektronisch signieren.

Die Verbreitung insbesondere der juristisch interessanten qualifizierten elektronischen Signatur zum "Massenmedium" hat sich bislang nicht ergeben. Aktuell nutzen Kreditinstitute den regelmäßigen Tausch ihrer EC-Karten dazu, für die neu auszugebenden EC-Karten die Möglichkeit der Nutzung mit einer qualifizierten elektronischen Signatur anzubieten. Auch das BMI wird mit seinem neuen ePA eine entsprechende optionale Möglichkeit schaffen.

Kunde – Persönliche Vertragsunterzeichnung

Verbraucherdarlehensverträge sind gemäß § 492 Absatz 1 Satz 1 BGB, "soweit nicht eine strengere Form vorgeschrieben ist, schriftlich abzuschließen."

Das bisherige schriftliche Verfahren mit allgemeinen Geschäftsbedingungen sowie diverse weitere Formulare (z. B. Einsichtnahme in die Grundbuchblätter des zuständigen Grundbuchamts) könnte durch ein IT-Verfahren mit elektronischem Personalausweis und elektronischer Signatur abgelöst werden. Die Identifikation von Antragstellenden könnte damit "am Schalter" und via Web-Portal einheitlich gelöst werden. Der elektronische Vertragsschluss bietet eine juristische sichere Variante und könnte den Finanzinstituten ermöglichen, entsprechende webbasierte Verfahren anzubieten.

Bei Verbraucherkreditverträgen verbietet § 492 BGB Absatz 1 Satz 2 bisher bei Darlehensverträgen ihren Abschluss in elektronischer Form: "Der Abschluss des Vertrags in elektronischer Form ist ausgeschlossen."

Die "Richtlinie 2008 / 48 / EG des Europäischen Parlaments und des Rates vom 23. April 2008 über Verbraucherkreditverträge und zur Aufhebung der Richtlinie 87 / 102 / EWG des Rates" (**Verbraucherkreditrichtlinie** - ABl. EU Nr. L 133 S. 66) ist bis zum 12. Mai 2010 in deutsches Recht umgesetzt-

zen. Gemäß Erwägungsgrund 14 sollten zwar durch Grundpfandrechte gesicherte Kreditverträge vom Geltungsbereich dieser Richtlinie ausgeschlossen sein.

Die "Richtlinie 2000 / 31 / EG des Europäischen Parlaments und des Rates vom 8. Juni 2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt ("Richtlinie über den elektronischen Geschäftsverkehr")" - **E-Commerce-Richtlinie** - verpflichtet die Mitgliedstaaten sicherzustellen, dass das Rechtssystem den Abschluss von Verträgen im elektronischen Verkehr ermöglicht:

Artikel 9 Absatz 1 - Behandlung von Verträgen

(1) Die Mitgliedstaaten stellen sicher, daß ihr Rechtssystem den Abschluß von Verträgen auf elektronischem Wege ermöglicht. Die Mitgliedstaaten stellen insbesondere sicher, daß ihre für den Vertragsabschluß geltenden Rechtsvorschriften weder Hindernisse für die Verwendung elektronischer Verträge bilden noch dazu führen, daß diese Verträge aufgrund des Umstandes, daß sie auf elektronischem Wege zustande gekommen sind, keine rechtliche Wirksamkeit oder Gültigkeit haben...

Im Gesetzentwurf der Bundesregierung "Entwurf eines Gesetzes zur Umsetzung der Verbraucherkreditrichtlinie, des zivilrechtlichen Teils der Zahlungsdiensterichtlinie sowie zur Neuordnung der Vorschriften über das Widerrufs- und Rückgaberecht" vom 05.11.2008 (www.bmj.bund.de/files/-/3370/RegE_Verbraucherkreditrichtlinie.pdf)

wird demnach gemäß Ziffer "22. § 492 wird wie folgt geändert: a) Absatz 1 Satz 2 und 5 wird aufgehoben."

§ 492 BGB Absatz 1 Satz 2 lautet in aktueller Fassung: "Der Abschluss des Vertrags in elektronischer Form ist ausgeschlossen."

Mit Inkrafttreten des Gesetzentwurfs wird daher der Vertragsschluss elektronischem Weg möglich.

"Bisher lag der Ausschluss der elektronischen Form darin begründet, dass die Verbraucherkreditrichtlinie 87 / 102 / EWG in Artikel 4 Abs. 1 selbst Schriftform vorsah. Da die neue Verbraucherkreditrichtlinie am Schriftformerfordernis nicht festgehalten hat, ist wegen des Artikels 9 Abs. 1 der E-Commerce-Richtlinie auch der Ausschluss der elektronischen Form im innerstaatlichen Recht nicht mehr zulässig. Folglich kann ein Verbraucherdarlehensvertrag künftig statt durch Unterschrift auch durch qualifizierte elektronische Signatur (§§ 126 Abs. 3, 126a), nicht aber in Textform abgeschlossen werden." (Gesetzentwurf, S. 123)

Wird der Regierungsentwurf Gesetz, bietet der Vertragsschluss via qualifizierte elektronische Signatur (§§ 126 Absatz 3, 126a BGB), eine juristische sichere Variante und könnte den Finanzinstituten ermöglichen, entsprechende internet-basierte Verfahren anzubieten.

Die elektronische Signatur soll es ermöglichen, Urheber und Integrität von Daten zuverlässig festzustellen. Sie hat als qualifizierte elektronische Signatur Rechtswirkungen wie die handschriftliche Unterschrift (§§ 126, 126a BGB). Zu prüfen bleibt, ob es in allen Fällen wirklich erforderlich ist, die qualifizierte elektronische Signatur einzusetzen, möglicherweise führt der Einsatz der fortgeschrittenen elektronischen Signatur sicherheitstechnisch ebenfalls zu befriedigenden Ergebnissen. Nach Auskunft der beteiligten Banken reicht eine fortgeschrittene elektronische Signatur aus; sie würde bereits eingesetzt.

Fördermittelberatung und -beantragung, Beratung und Beantragung von Produkten der Vertriebspartner (Verbund, Konzern, etc.)

Einsatz der qualifizierten elektronischen Signatur wie oben.

Anforderung des Einkommensteuerbescheid und Einkommensnachweises

Einsatz der qualifizierten elektronischen Signatur wie oben. Die einmalige elektronische Abfrage der letzten Einkommensteuerbescheide beim zuständigen Finanzamt (siehe Verfahren Elster) muss dabei datenschutzkonform erfolgen: Die Mitarbeiterin oder der Mitarbeiter des Kreditinstituts weist sich gegenüber dem Finanzamt mit der qualifizierten elektronischen Signatur aus und beantragt Zugriff auf entsprechende Steuerbescheide, der Kunde genehmigt mit der qualifizierten elektronischen Signatur gegenüber dem Finanzamt.

Siehe auch die geplante bundesweite Einführung der Einkommensdatenbank ELENA (früher Jobcard).

Grundbuchamt

Grundbuchauskunft

Im derzeitigen IST muss das Kreditinstitut auch im Rahmen der Internet-Grundbucheinsicht nur mitteilen, dass es ein berechtigtes Interesse hat, nicht mehr. Die Bank muss hinterlegen, warum sie das Internet-Grundbuch abgefragt. Zunächst wird nicht geprüft, ob der Kunde der Grundbuchauskunft zugestimmt hat.

Im SOLL-Verfahren müssten die von der Eigentümerin oder dem Eigentümer des Grundstücks signierten Zustimmungserklärungen zur Grundbuchauskunft elektronisch an das Grundbuchamt weitergeleitet werden. Damit wäre das berechtigte Interesse im Rahmen jeder Grundbuchabfrage "rechtssicher" gewährt; Missbrauch wäre ausgeschlossen.

Grundschuldbestellung

Im Rahmen der Initiative Finanzstandort Deutschland (IFD) wurde das Projekt die "elektronische" Grundschuld - Kommunikation zwischen Banken und Notaren über NotarMail initiiert. Mehrere Kreditinstitute und die Bundesnotarkammer haben sich zum Ziel gesetzt die Prozesse der Grundschuldbestellung mit Unterstützung durch elektronische Medien abzubilden ohne sinnvolle rechtliche Strukturen des Verfahrens aufzugeben.

Die rechtlichen Voraussetzungen zur notariellen Beglaubigung in elektronischer Form sind geschaffen (§ 39a BeurkG). Nach § 39a BeurkG können "Beglaubigungen und sonstige Zeugnisse i. S. d. § 39 können elektronisch errichtet werden. Das hierzu erstellte Dokument muss mit einer qualifizierten elektronischen Signatur nach dem Signaturgesetz versehen werden."

Der Notar wird nicht ersetzt werden können.

Pfandfreigabe, Grundschuldlöschung

Die Speicherung der elektronischen Daten orientiert sich an den Aufbewahrungsverpflichtungen für entsprechende Akten.

An dieser Stelle ist die Darstellung und Beschreibung einer möglichen SOLL Prozesskette abgeschlossen. Die Darstellung der unterschiedlichen Sichten auf die Prozesskette zeigt, dass im Rahmen dieser noch eine Vielzahl von Optimierungspotenzialen vorhanden ist. Im nachfolgenden Abschnitt wird versucht diese Potenziale entsprechend den zugrunde gelegten Sichten nochmals kurz zusammen zu fassen und darzustellen.

Nutzenabschätzung bezüglich Wirtschaftlichkeitspotenzialen der SOLL-Prozesskette "private Immobilienfinanzierung"

Die nachfolgenden Ausführungen skizzieren, soweit möglich, nochmals einige Wirtschaftlichkeitsabschätzungen bezogen auf die SOLL-Prozesskette.

Grundsätzlich muss an dieser Stelle festgehalten werden, dass diese nur in einem allgemeinen Rahmen möglich ist. Dabei wird vor allem auf zeitliche und technische Aspekte fokussiert. Eine Kostenabschätzung ist an dieser Stelle nicht vorgenommen worden.

Der Musterprozess zur Standardvariante der privaten Immobilienfinanzierung (Neugeschäftsprozess) weist in den einzelnen Prozessphasen folgende Bearbeitungszeiten und Durchlaufzeiten aus:

Prozessphase	Bearbeitungszeit (BZ) in Minuten	Durchlaufzeit (DZ) in Minuten	Prozesseffizienz (BZ / DZ)
Beratung	20	140	0,14
Antrag / Genehmigung	82	1.869	0,04
Vertrag	22	9.452	0,002

Tabelle 19: Prozesszeiten für die Prozesskette "Private Immobilienfinanzierung"
(Quelle: BVR Projekt "VR-Process")

Die Kenngröße "Prozesseffizienz" (Quotient aus Bearbeitungszeit und Durchlaufzeit) verdeutlicht das noch vorhandene Potential an Wertschöpfung in einem (Teil-)Prozess. Die Wertschöpfung in einem (Teil-)Prozess ist dann optimal, wenn die Kenngröße gleich 1 ist. Die Angaben sind dem BVR-Projekt "VR-Process" entnommen.

Das wesentliche Optimierungspotential liegt in den unternehmensübergreifenden Schnittstellen zu den Institutionen der öffentlichen Verwaltung und in deren Geschäftsprozessen.

Bezogen auf die technischen Sichtweisen, kann die Umsetzung der SOLL-Prozesskette aufgrund der durchgehenden Automatisierung mit elektronischer Kommunikation ohne Medienbrüche mit standardisierten Formaten und Protokollen zu folgenden Nutzen für alle Beteiligten führen:

- mehr Sicherheit (sogar mehr Rechtssicherheit ist möglich)
- weniger menschliche Fehlerquellen an den Schnittstellen
- zu einem stabileren Prozess

- zu einem schnelleren Durchlauf (siehe Tabelle 19) und damit möglicherweise zu weniger notwendigen Mitarbeiterinnen oder Mitarbeitern, zu (einem Wettbewerbsvorteil durch) mehr Kundenzufriedenheit

Die dargestellten Nutzen sowie die Beschreibung der SOLL-Prozesskette zeigen die großen Potenziale, welche sich mit der zukünftigen Umsetzung verbunden sein können. Die Ausführungen zur Prozesskette private Immobilienfinanzierung zeigen jedoch auch noch eine Vielzahl von möglichen Handlungsfeldern auf, die sowohl von Seite der Banken als auch von Seite der öffentlichen Verwaltung von hoher Relevanz sind.

7.4 Handlungsempfehlungen

Auf Basis der bisherigen Erkenntnisse können folgende Handlungsempfehlungen adressiert werden:

Handlungsempfehlung Nr. 1: Prozessmanagement in den Banken und Verwaltungen weiter ausbauen

Die Ausführungen zeigen die große Relevanz des Themas Geschäftsprozessmanagement bei allen Beteiligten. Studien des Fraunhofer IAO zeigen, dass eine große Anzahl von Banken derzeit im Begriff ist, ihr Prozessmanagement zu professionalisieren. Auch auf Seiten der öffentlichen Verwaltungen muss dieses geschehen, um Level-1 Prozessketten realisieren zu können. Dazu muss neben den organisatorischen und technischen Voraussetzungen auch eine entsprechende Weiterbildung von den betroffenen Mitarbeiterinnen und Mitarbeitern stattfinden, um die Prozessketten und damit verbundenen Rollen in den unterschiedlichen Organisationen etablieren und deren Wirken entsprechend synchronisieren zu können.

Des Weiteren sind sowohl Banken als auch öffentliche Verwaltungen auf Grundlage eines professionellen Prozesskettenmanagement in der Lage die jeweiligen Prozessketten hinsichtlich ihres Wertschöpfungsbeitrages und unter Risikoaspekten bewerten zu können. Darüber hinaus ermöglichen diese Maßnahmen entsprechende Prioritäten bei der Umsetzung und Optimierung vornehmen zu können.

Handlungsempfehlung 1 adressiert die Ziele [IMMO 1], [IMMO 2], [IMMO 3].

Handlungsempfehlung Nr. 2: Schnittstellen bzw. PRK zwischen Banken und Verwaltungen automatisieren (z. T. schon erfolgt) und dafür allgemeingültige Standards etablieren

Für die Kommunikation zwischen den IT-Komponenten der Prozesskette sollten Kommunikatoren (Fassaden) entwickelt werden, die die benötigten Dienste mit definierten Schnittstellen zur Verfügung stellen. Die Kommunikatoren sollten nach dem SAGA-Standard für die öffentliche Verwaltung als Client / Server Webservices ausgeführt werden.

Handlungsempfehlung 2 adressiert das Ziel einer durchgehenden medienbruchfreien Automatisierung der Prozesskette über die Grenzen der Institutionen hinaus. [IMMO 4]

Handlungsempfehlung Nr. 3: Einführung und angemessene Nutzung fortgeschrittener und qualifizierter elektronischer Signaturen

Elektronische Signaturen unterstützen die Sicherheitsziele Integrität, Authentizität, Verbindlichkeit und Nicht-Abstreitbarkeit. Dabei müssen die Benutzbarkeit und die Kosten berücksichtigt werden. In den meisten Fällen in der Prozesskette zur Kreditvergabe ist die fortgeschrittene Signatur völlig ausreichend; Beispiele sind die Verfahren Elster und E-Vergabe. Qualifizierte elektronische Signaturen sollten nur dort zum Einsatz kommen müssen, wo dies auch rechtlich zwingend erforderlich ist. Chipkartenbasierte Anwendungen wie der ePA, die einen Container zur Unterbringung entsprechender Zertifikate bereitstellen, können in diesen Fällen die Anwendung der elektronischen Fachverfahren erleichtern.

Bei Neuentwicklungen zur elektronischen Authentisierung und qualifizierten Signatur muss das eCard-API-Framework (BSI TR-03112) des BSI berücksichtigt werden.

Handlungsempfehlung 3 adressiert die Ziele [IMMO 7] und [IMMO 8].

Handlungsempfehlung Nr. 4: Einführung einer elektronischen Vernetzung ohne Medienbrüche mit standardisierten Datenschemata zwischen allen Institutionen (XML-basierte Webservices, möglichst nach XÖV-Standards)

Es sollten nur noch strukturierte maschinenlesbare XML-Dokumente ausgetauscht werden. Falls eine Institution bereits eine Schnittstelle über PDF-Formulare bereitstellt, kann diese natürlich weiterhin genutzt werden.

Die Spezifikation der Datenmodelle sollte sich an den XÖV-Standards orientieren.

Die Dienste zur Übertragung der Daten sollten als Webservices realisiert werden.

Handlungsempfehlung 4 adressiert das Ziel einer durchgehenden medienbruchfreien Automatisierung der Prozesskette über die Grenzen der Institutionen hinaus und der Etablierung einheitlicher Standards für den Datenaustausch. [IMMO 4]

Handlungsempfehlung Nr. 5: Einführung einer auf Trusted Domains basierenden standardisierten Sicherheitsinfrastruktur mit einem flexiblen verteilten Identity-Management

Die Infrastruktur sollte sich am Deutschland-Online Projekt "Einheitliche Kommunikationsinfrastruktur für den elektronischen Rechtsverkehr" (SAFE / DIM) orientieren. Das SAFE Grobkonzept (siehe www.deutschland-online.de/DOL_Internet/broker.jsp?uMen=404209ab-8d40-9114-fb1-b1ac0c2f214a) zeigt den Weg dorthin (siehe Kap. 4.2.3). Wenn jede der beteiligten Parteien eine Trust-Domain im Sinne von SAFE in der für sie notwendigen Ausbaustufe darstellt, können die verschiedenen Nutzerverwaltungen besser aufeinander abgestimmt werden, der Umgang mit verschiedenen Sicherheitslevel wird leichter konfigurierbar. Die nach SAFE geforderten Identity-Provider und Attributservices ermöglichen rollenbasierte digitale Signaturen für Dokumente und Pseudonymisierung. Die XML-basierte Datenübertragung zwischen den Webservices beseitigt Medienbrüche und ermöglicht die elektronische Weiterverarbeitung.

Handlungsempfehlung 5 adressiert das Ziel einer durchgehenden medienbruchfreien Automatisierung der Prozesskette über die Grenzen der Institutionen hinaus. [IMMO 5], [IMMO 6]

Handlungsempfehlung Nr. 6: IT-Grundschutz etablieren und professionalisieren

Die Vertrauenswürdigkeit einer Prozesskette verlangt ein sicheres Umfeld. Die Orientierung an anerkannten Informationssicherheitsmanagement-Standards trägt dazu bei, dieser Anforderung zu entsprechen. Alle Prozessschritte und Teilprozesse der Kreditvergabe müssen daher den Anforderungen des BSI-Standards 100-2 genügen. Dabei ist der jeweilige Schutzbedarf zu berücksichtigen.

Zertifizierung bedeutet überprüfte Sicherheit und trägt damit zur Vertrauenswürdigkeit bei. Es ist deshalb insbesondere für (Teil-)Prozessketten mit hohem und sehr hohem Schadenspotenzial notwendig, eine Möglichkeit zu schaffen, die Sicherheitsmaßnahmen nach IT-Grundschutz zu zertifizieren.

Handlungsempfehlung 6 adressiert die Ziele zur Realisierung einer sichereren IT-Infrastruktur und entsprechende Verfahren zur Realisierung des IT-Grundschutzes. [IMMO 7], [IMMO 8]

Handlungsempfehlung Nr. 7: Juristische Handlungsempfehlungen zu Datenschutz und rechtsverbindlicher Signatur

Die vorhandenen Normen reichen zur Absicherung eines effektiven Handlungsempfehlungen aus juristischer Sicht:

- Die vorhandenen Normen reichen zur Absicherung eines effektiven Datenschutzes aus. Es ist darauf hinzuwirken, dass alle Beteiligten datenschutz-rechtliche Bestimmungen einhalten. Die qualifizierte elektronische Signatur ist das A und O jedes datenschutzrechtlich korrekten Informationsaustausches.
- Dringend erforderlich ist neben dem bereits beschlossenen ePA die bundesweite Einführung einer qualifizierten elektronischen Signatur des Datenübermittelnden bzw. -Abrufenden. Beides ist für die Rechtssicherheit absolut notwendig. Zu verifizieren bleibt, ob es in allen Fällen wirklich geboten ist, die qualifizierte elektronische Signatur einzusetzen; möglicherweise führt der Einsatz der fortgeschrittenen elektronischen Signatur sicherheitstechnisch ebenfalls zu befriedigenden Ergebnissen. Gleichzeitig ist darauf hinzuwirken, Verfahrensmethoden einzusetzen, die einen Zugriff unbefugter Dritter (Hacker) ausschließen.

Handlungsempfehlung 7 adressiert die juristischen Zielsetzungen [IMMO 9].

7.5 Ansätze zur Gestaltung neuer Geschäfts- und Betreibermodelle

Die zuvor dargestellten Handlungsempfehlungen geben Hinweise, welche bei der Gestaltung zukünftiger Geschäfts- und Betreibermodelle für Prozessketten im Bereich der privaten Immobilienfinanzierung grundsätzlich möglich sind.

Wie dargestellt ist eine zentrale **Voraussetzung** zur Realisierung dieser Ansätze die **Bereitstellung des ePA** mit Zertifikaten durch Bund, um eine sichere Authentifizierung zu ermöglichen.

Mittel des in Submodul E dargestellten Schemas können folgende, ausgewählte Betreibermodelle skizziert werden, welche sinnvoll in der Praxis genutzt werden können.

Betreibermodell 1:

Bund stellt sichere Datenräume für Bürgerinnen und Bürger bereit, die darin ihre notwendigen Dokumente sicher deponieren können (Betrieb durch Bund, PPP oder beauftragte Service Gesellschaft – Preismodell: kostenlos, fixer Grundbetrag pro Jahr, Fixpreis mit Transaktionskomponente).

Betreibermodell 2:

Aufbau eines integrierten Grundbuchs (bundesweit und einheitlich), i.S. e. Metaportals, um Banken den Zugriff auf notwendige Informationen zu erleichtern (Betrieb durch Bund, PPP oder beauftragte Service Gesellschaft – Preismodell: kostenlos, fixer Grundbetrag pro Jahr, Fixpreis mit Transaktionskomponente).

Betreibermodell 3:

Betrieb einer autorisierten Zertifizierungsstelle für personengebundene Zertifikate, wie ePA, Bankkarte etc. zur sicheren Personenidentifikation und -authentifizierung (Betrieb durch Bund, PPP oder beauftragte Service Gesellschaft – Preismodell: kostenlos, fixer Grundbetrag pro Jahr, Fixpreis mit Transaktionskomponente).

8 Prozesskettenanalyse II: Geldwäscheverdachts-Anzeige (GVA)

8.1 Die IST-Prozesskette

Geldwäsche ist nach dem deutschen Strafrecht ein Straftatbestand. Strafbar ist nach § 261 Strafgesetzbuch, wer einen rechtswidrig erlangten Gegenstand (z. B. Vermögenswerte aus dem Drogenhandel, Waffenhandel, Betrug oder Steuerhinterziehung) verschleiert, die Ermittlung oder Sicherstellung der Herkunft solcher unrechtmäßig erlangten Vermögenswerte gefährdet oder vereitelt. Dieser unrechtmäßig erlangte Vermögenswert ist somit entweder Ergebnis einer solchen Tätigkeit oder soll der Finanzierung illegaler Tätigkeiten (z. B. Terrorismus) dienen

www.bundesfinanzministerium.de/nr_2352/DE/BMF_Startseite/Service/Glossar/G/001_Geldwaesche.html.

Zur **Relevanz des Themas Geldwäsche**: Es gab gemäß Bundeskriminalamt (BKA) im Jahr 2007 9.080 Verdachtsanzeigen nach dem Geldwäschegesetz (GwG) (BKA 2008a: 8). 64 dieser Verdachtsmeldungen lagen laut FIU, der Financial Intelligence Unit des BKA, Transaktionen in Höhe von über drei Millionen Euro pro Anzeige zugrunde (BKA 2008a: 23).

Neben den traditionellen Bereichen der Kredit- und Finanzdienstleistungsbranche als Adressaten des GwG sind auch folgende Berufsgruppen in den Fällen des § 2 GwG den Pflichten des GwG unterworfen:

- Rechtsanwälte, Rechtsbeistände, Patentanwälte und Notare
- Wirtschaftsprüfer, vereidigte Buchprüfer, Steuerberater und Steuerbevollmächtigte
- Immobilienmakler
- Spielbanken
- sonstige Gewerbetreibende sowie Personen, die entgeltlich fremdes Vermögen verwalten

In diesem Kapitel werden Banken und Kreditinstitute als Absender von **Geldwäscheverdachts-Anzeige (GVA)** näher betrachtet.

Empfänger der GVA sind die Landeskriminalämter (LKA), das BKA sowie die Staatsanwaltschaften, und auf spezielle Fälle begrenzt auch die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin).

Das folgende Schaubild zeigt die Verfahrensübersicht im IST auf einen Blick (siehe Abbildung 81).

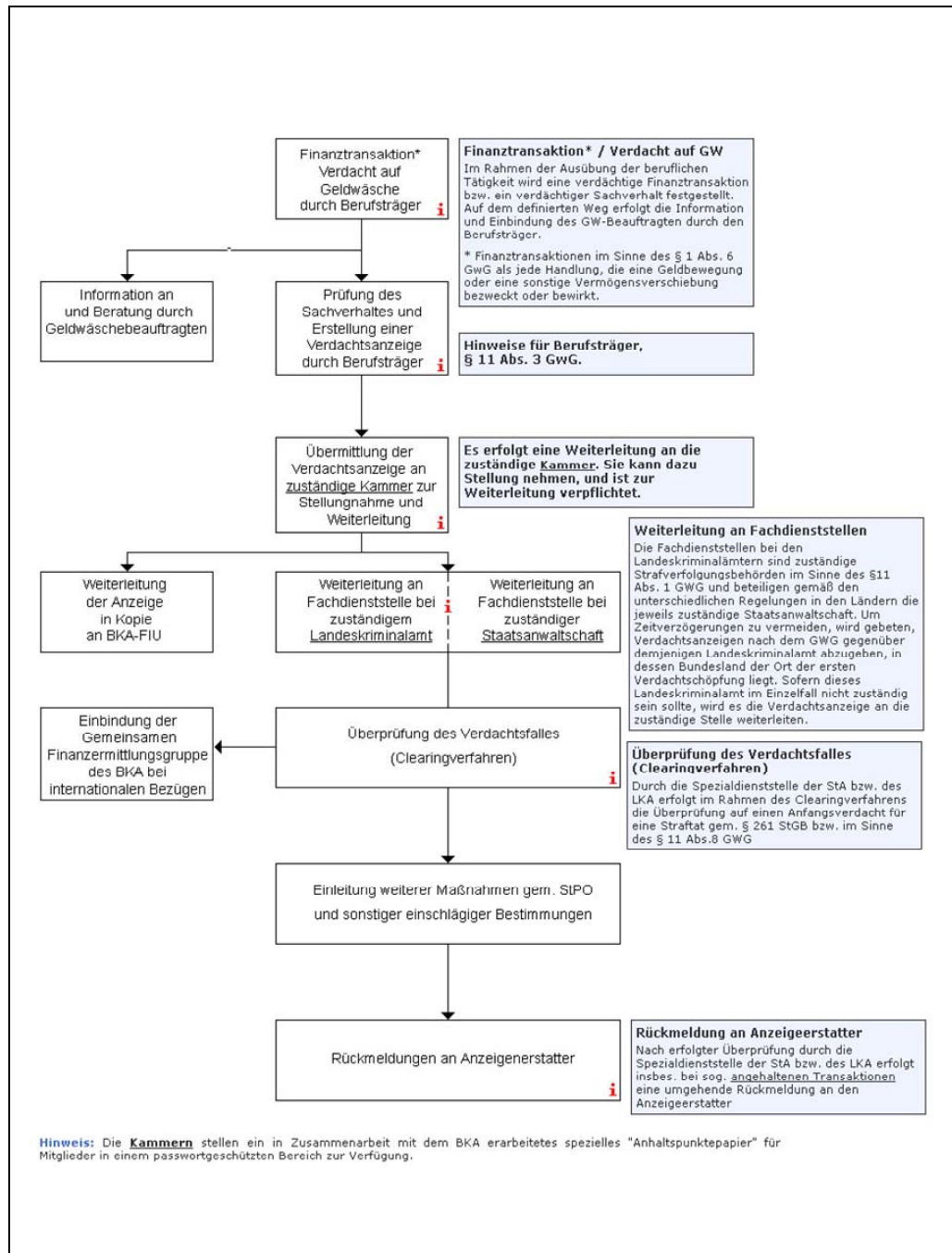


Abbildung 81: GVA IST-Verfahrensübersicht (Quelle: BKA 2008b)

8.1.1 Wirtschaftliche, prozessuale und organisatorische Beschreibung und Analyse

Die nachfolgende "Ereignisgesteuerte Prozesskette" (EPK) zeigt die Prozesskette im IST (siehe Abbildung 82).¹⁴

¹⁴ Es wird in Abbildung 82 im Rahmen der empfohlenen Prozessmodellierungsregeln des BMI im "Leitfaden für Entwickler von Prozess- und Datenmodellen" (BMI 2007) eine EPK-Notation mit Funktionen (Rechtecken), Ereignissen (Sechsecken) und Konnektoren ("und", "einschließendes oder", "ausschließendes oder") verwandt; es wird eine vereinfachte Semantik gewählt, bei der Funktionen auf Funktionen folgen können und Ereignisse relative Endpunkte modellieren (Frösche / Götz 2007: 33 ff.).

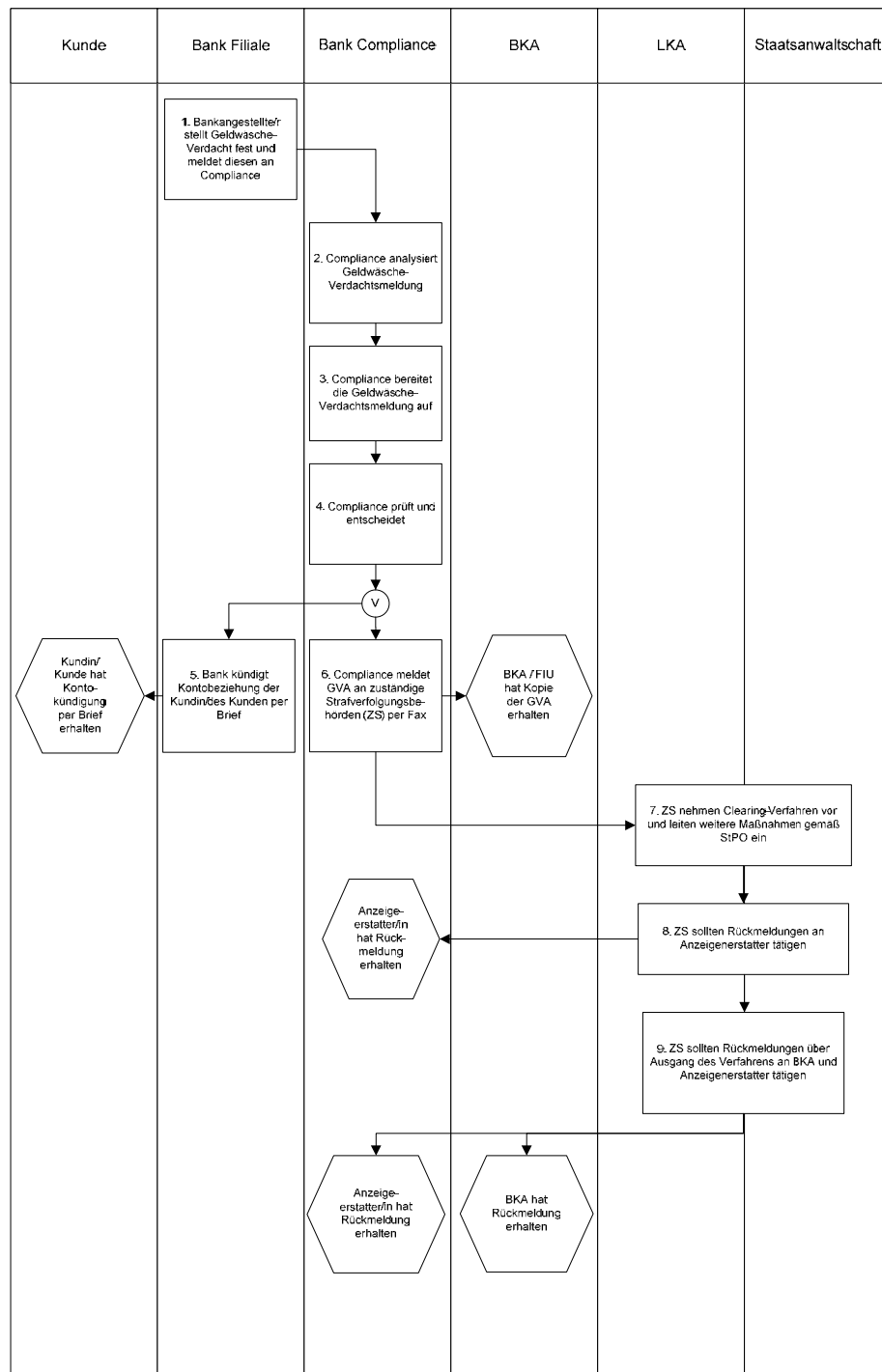


Abbildung 82: GVA IST-Prozesskette (EPK) (Quelle: Eigene Darstellung)

1. Die Bankangestellte oder der Bankangestellter stellt Geldwäsche-Verdacht fest und meldet diesen an die Compliance

Transaktionen i. S. d. Geldwäschegesetz ist jede Handlung, die eine Geldbewegung oder sonstige Vermögensverschiebung bezweckt oder bewirkt (§ 1 Abs. 4 GwG). Ein solcher Verdacht (verdächtige Finanztransaktion) wird z. T. durch den Berufsträger (z. B. Bankangestellten in einer Filiale) selbst oder durch sonstige Hinweise an die zuständige Abteilung Compliance bzw. den / die Geldwäschebeauftragte(n) gemeldet. Eine solche Verpflichtung zur Meldung einer verdächtigen Transaktion ergibt sich aus § 11 GwG in Verbindung mit § 261 StGB. Die eingegangene Meldung wird dann von der Compliance weiter bearbeitet. Die Bearbeitung einer solchen Verdachtsmeldung beinhaltet u. a. die Einstufung der Dringlichkeit des Vorgangs, den Abgleich der Kundendaten und der Transaktionen anhand bestehender Datenbanken. Des Weiteren wird zu jedem Vorgang eine Akte diesbezüglich angelegt. Somit ist es noch ein papierbasiertes Verfahren, welches zukünftig jedoch durch ein Case-Management auf elektronischen Wege abgewickelt werden soll.

2. Die Compliance analysiert die Geldwäsche-Verdachtsmeldung

Der Sachverhalt ist nach Priorisierung vollständig zu überprüfen, ob der Sachverhalt sich weiter erhärten lässt. Hierfür sind insbesondere fehlende Unterlagen, z. B. Kunden- / Kontoführungsdaten, Legitimationsdokumente und / oder Legitimationsdaten, nach dem KYC-Prinzip (Know-Your-Customer) i. S. d. § 1 GwG in Verbindung mit § 154 Abgabenordnung (AO) und / oder weitere Unterlagen zur Detaillierung der verdächtigen Finanztransaktion anzufordern und auszuwerten. Die Art der Analyse bzw. Identifizierung (Feststellung und Überprüfung der Identität i. S. d. § 1 GwG) richtet sich auch danach, ob es sich bei dem geführten Konto um ein Privat- oder Geschäftskonto handelt. Die Analyse der Geldwäscheverdachtsmeldung ist gerade in dieser Phase sehr gründlich vorzunehmen. Zum einen, ist die Grenze der Beihilfe zur Geldwäsche (§§ 27, 261 StGB) zu Lasten der Banken problematisch, aber auch gemäß § 17 GwG handelt die Verpflichtende oder der Verpflichtende ordnungswidrig, wenn dieser der Pflicht zur Anzeige eines Verdachtsfalls nach § 11 GwG nicht nachkommt. Eine solche Ordnungswidrigkeit kann mit einem Bußgeld bis zu hunderttausend Euro geahndet werden (§ 17 Abs. 3 GwG).

3. Die Compliance bereitet die Geldwäsche-Verdachtsmeldung auf

Die Compliance bereitet die Entscheidung zur Verdachtsanzeige vor, oder aber der Sachverhalt lässt sich aufklären, so dass eine Erstellung der Verdachtsanzeige nicht notwendig ist. Im Falle der Meldung einer Verdachts-

meldung von Seiten der Bankmitarbeiterinnen und Bankmitarbeiter bekommt die Filiale eine Rückmeldung der Fachabteilung mit weiteren Vorgehensweisen (Handlungsempfehlungen). Sofern es zu der Entscheidung einer Verdachtsanzeige kommt, werden ebenfalls Handlungsempfehlungen an die zuständige Sachbearbeitung, Filialeitung oder Betriebsleitung weitergegeben. Die aufbereitete Entscheidung (noch papierbasiert s. o.) geht dann an die Leitung der Abteilung Compliance zur endgültigen Entscheidung.

4. Die Compliance prüft und entscheidet

In dieser Phase wird die aufbereitete Entscheidung der zuständigen Abteilung noch einmal nach dem sogenannten "Vier-Augen-Prinzip" überprüft. Die Leitung der Abteilung Compliance entscheidet dann entweder, ob es zu einer Abgabe der Verdachtsanzeige an die zuständigen Strafverfolgungsbehörden kommt oder bei einer Negativentscheidung (keine Anzeige des Verdachts) mit entsprechender Begründung an die jeweiligen Beteiligten zurück geht. Eine solche Verdachtsanzeige durch den Berufsträger kann gemäß § 11 Abs. 2 GwG mündlich oder telefonisch gestellt werden, diese ist dann aber schriftlich, fernschriftlich oder durch elektronische Datenübermittlung zu wiederholen.

5. Bank kündigt Kontobeziehung der Kundin oder des Kunden per Brief

Mit der Abgabe der Verdachtsanzeige geht die Anweisung an die zuständige Kundenbetreuerin oder dem zuständigen Kundenbetreuer bzw. der Vorgesetzten oder dem Vorgesetzten, das jeweilige Konto aufzulösen und zu kündigen. Dies kann anhand von AGB durchaus geregelt werden, dass auch ohne Nennung eines bestimmten Grundes das Konto seitens des Kreditinstitut gekündigt werden kann. Der Verdachtsanzeiger (Kredit- / Finanzdienstleistungsinstitute) soll dann von der zuständigen Strafverfolgungsbehörde eine Empfangsbestätigung per Fax erhalten, dass die Anzeige eingegangen ist. Problematisch ist, dass das Kreditinstitut nun für die Strafverfolgungsbehörde die Daten für evtl. Nachfragen bereithalten muss. Es ist an der Stelle darauf hinzuweisen, dass zwischen Kundinnen oder Kunden und Kreditinstituten ein Geschäftsbesorgungsvertrag vereinbart wurde, nach dem weitere Finanztransaktionen getätigt werden "müssen". Es ist folglich eine rasche Anweisung der Strafverfolgungsbehörden gewünscht, um ggf. möglichen Schäden wirtschaftlicher Art rechtzeitig zu begegnen. Dennoch können Verpflichtete ungeachtet solcher vertraglichen Bestimmungen die Geschäftsbeziehung gemäß § 3 Abs. 6 GwG z. B. durch Kontokündigung beenden.

6. Die Compliance meldet Geldwäscheverdachts-Anzeige (GVA) an zuständige Strafverfolgungsbehörden per Fax

Zum jetzigen Zeitpunkt wird eine solche Verdachtsanzeige per Fax an die zuständigen Strafverfolgungsbehörden (zuständige LKA, zuständige Staatsanwaltschaft und je nach Bundesland besondere Fachdienststellen) und eine Kopie an die Zentralstelle für Verdachtsanzeigen BKA FIU i. S. d. § 10 GwG weitergeleitet. Somit erfolgt die gesamte Verdachtsanzeige auf papierbasierten Verfahren.

Die Compliance führt ggf. Nachmeldungen an zuständige Strafverfolgungsbehörden durch. Falls erforderlich werden Nachtragsverdachtsanzeigen bis zur Kontokündigung mit dem selben Formular an die zuständigen Behörden weitergeleitet (z. B. relevante Kontoumsätze).

7. Zuständige Strafverfolgungsbehörden nehmen Clearing-Verfahren vor und leiten weitere Maßnahmen gemäß StPO ein

Der detaillierte Gang des Strafverfahrens ist hierzu in Kap. 8.1.4 geschildert.

8. Zuständige Strafverfolgungsbehörden sollten Rückmeldungen an Anzeigenerstatter tätigen

Nach erfolgter Überprüfung wird das Ergebnis auch an den Polizeibehörden gemäß § 482 StPO in Verbindung mit § 11 Abs. 9 GwG mitgeteilt. Dennoch ist anzumerken, dass diese Rückmeldungen der Staatsanwaltschaft von Bundesland zu Bundesland unterschiedlich gehandhabt werden. So stellte die BKA FIU fest, dass z. B. aus Hamburg und Schleswig-Holstein kaum Rückmeldungen eingehen, wobei z. B. aus den Bundesländern Baden-Württemberg, Bayern, Berlin und Hessen sehr hohe Rückmeldungen zu verzeichnen sind (BKA 2008a: 27).

9. Zuständige Strafverfolgungsbehörden sollten Rückmeldungen über Ausgang des Verfahrens an BKA und Anzeigenerstatter tätigen

Ermittlungsbehörden sollten die Anzeige erstattende Bank nach Erledigung automatisch vom Ausgang des Verfahrens benachrichtigen.

Es bedarf keiner Begründung, welche Entscheidung der Beendigung zugrunde liegt. Die Bank muss jedoch bei Erledigung des Verfahrens die Daten zu diesem Fall löschen. Die Speicherung der Daten ist dann nicht mehr zur Aufgabenerfüllung erforderlich. Sonst droht ein Konflikt mit dem BDSG, sofern solche Daten gespeichert sind.

8.1.2 IT-architektonische Beschreibung und Analyse

Die allgemeinen **IT-Architektur der GVA** ist in der nächsten Abbildung dargestellt (siehe Abbildung 83).

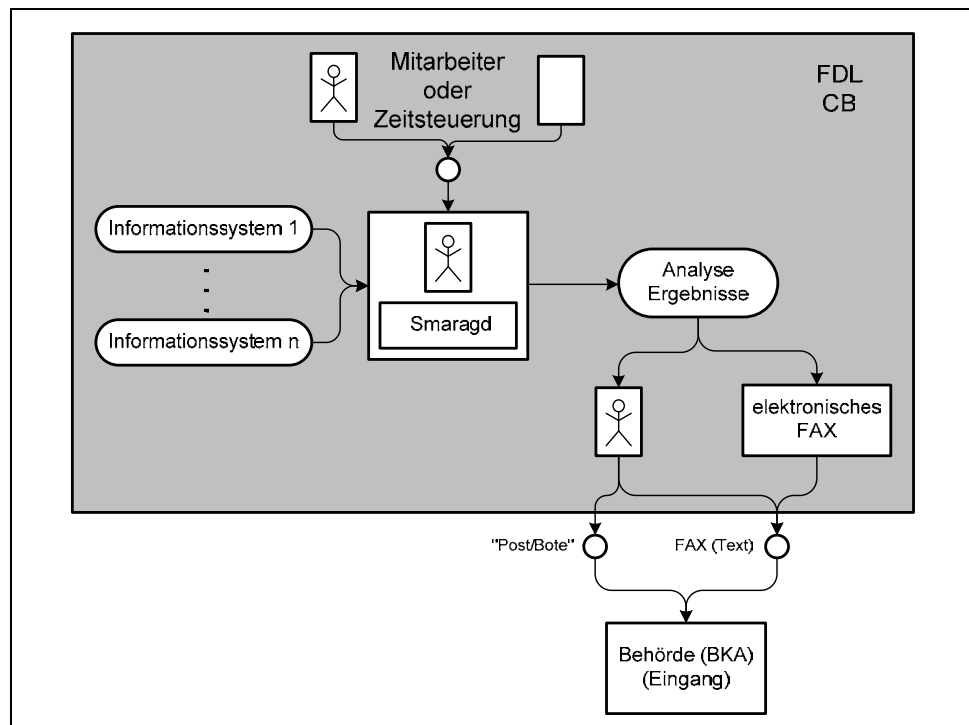


Abbildung 83: GVA IST-Architektur (FMC) (Quelle: Eigene Darstellung)

Der Prozess Verdachtsanzeige wird in der Regel nach einem Hinweis von Filialmitarbeiterinnen und Filialmitarbeitern oder dem Auftreten von Verdachtsindizien aus laufenden Monitoring-Anwendungen angestoßen und durchläuft den geschilderten Analyse- und Entscheidungs-Prozess (siehe Kap. 8.1.1). Die Verdachtsfälle werden in einer **Fachanwendung (Fallakte, Vorgangsbearbeitung)**¹⁵ dokumentiert. Die Verdachtsanzeige wird per Papierfax oder elektronischem Fax (Druckertreiber , Faxserver) an die zustän-

¹⁵ In der Commerzbank wird z. B. die Anwendung Smaragd verwendet.

dige Behörde (BKA) geschickt. Dazu gehören auch die möglichen Beweismittel aus der Analyse. In besonderen Fällen werden weitere Unterlagen per Bote überbracht.

Besonders großer Wert wird hier auf die Vertraulichkeit und Sicherheit der Dokumente gelegt, da jede Art von Öffentlichkeit das Ansehen der Kundin oder des Kunden und der Bank dauerhaft schädigen könnte bzw. im Fall eines bestehenden Rechtsverstoßes die Ermittlungen behindern oder unmöglich machen würden.

Weiterhin wäre es für die Bank von großem Nutzen, wenn sie eine **Rückmeldung zum Verlauf des Verfahrens** (Weiterführungswunsch des Kontos seitens des LKA, Verurteilung) bekommen würde, um ihre Vorgehensweise zu optimieren und den Fall abschließen zu können.

8.1.3 Sicherheitstechnische Beschreibung und Analyse

Die in Kap. 8.1.2 genannten Kommunikationswege sind sicherheitstechnisch wie folgt zu analysieren und einzuschätzen.

Kommunikation per Post / Bote

Diese Kommunikationswege werden betrachtet, weil diese häufig in kritischen Fällen bevorzugt verwendet werden und somit Teil der Prozesskette sind. Dennoch sind sie aber keineswegs als sicher zu betrachten. Übliche Gefährdungen sind hier in den menschlichen Fehlhandlungen der beteiligten Personen zu suchen, wie Sorglosigkeit, Korruption oder "Social Engineering", d. h. das illegale "Erarbeiten" von Informationen durch persönliche Manipulation der am Vorgang beteiligten Personen.

Kommunikation per FAX

Ein großer Teil der Kommunikation wird **per Fax** ausgeführt. Daraus ergeben sich eine Reihe von Gefährdungen.

Die Sicherheit von Faxgeräten ist im **Baustein B 3.402** Faxgerät der IT-Grundschutzkataloge des BSI beschrieben. Neben organisatorischen Mängeln, menschlichen Fehlhandlungen und technischem Versagen sind hier besonders die vorsätzlichen Handlungen von Bedeutung. Hierzu gehören insbesondere folgende Gefährdungen für den Betrieb von Faxgeräten:

- **G 5.7** Abhören von Leitungen

Das Abhören wird als nicht zu vernachlässigende Gefährdung angesehen. Dazu findet man in den Grundschutzkatalogen: "Grundsätzlich gibt es keine abhörsicheren Kabel. Lediglich der erforderliche Aufwand zum Abhören unterscheidet die Kabel. Ob eine Leitung tatsächlich abgehört wird, ist nur mit hohem messtechnischen Aufwand feststellbar.

Der Entschluss, eine Leitung abzuhören, wird im wesentlichen durch die Frage bestimmt, ob die Informationen den technischen bzw. den finanziellen Aufwand und das Risiko der Entdeckung wert sind. Die Beantwortung dieser Frage ist sehr von den individuellen Möglichkeiten und Interessen des Angreifers abhängig. Somit ist eine sichere Festlegung, welche Informationen und damit Leitungen ggf. abgehört werden, nicht möglich."

Die weiteren unten stehenden Gefährdungen sind im Detail unter www.bsi.de/gshb/deutsch/baust/b03402.htm (BSI 2008b), nachzulesen.

- **G 5.30** Unbefugte Nutzung eines Faxgeräts oder eines Faxservers
- **G 5.31** Unbefugtes Lesen von Faxsendungen
- **G 5.32** Auswertung von Restinformationen in Faxgeräten und Faxservern
- **G 5.33** Vortäuschen eines falschen Absenders bei Faxsendungen
- **G 5.34** Absichtliches Umprogrammieren der Zieltasten eines Faxgeräts
- **G 5.35** Absichtliche Überlastung durch Faxsendungen

Die oben stehenden Gefährdungen verdeutlichen, dass Faxgeräte ohne die Verwendung von Kryptographie nicht als sicheres Transportmedium angesehen werden können. Die Problematik ist ähnlich einzuschätzen wie bei unverschlüsselten E-Mails – man versendet quasi eine Postkarte. Deshalb sollte sobald wie möglich auf die Kommunikation per Fax verzichtet werden, sofern nicht zusätzliche Verschlüsselungsverfahren verwendet werden (z. B. mit Hilfe kryptographischer Faxgeräte).

8.1.4 Juristische Beschreibung und Analyse

Im folgenden werden Anfangsverdacht, Verdachtsverdichtung und Verfahrensgang juristisch diskutiert und anschließend der Gang des Strafverfahrens erläutert.

Der Anfangsverdacht

Ein solcher Verdacht entsteht zuerst dort, wo Geld wie eine Ware eingesetzt wird. Also zuerst bei Banken, aber auch überall dort, wo mit Geld gehandelt wird (Wechselstuben bis hin zu den Brokern); siehe die Verpflichteten i. S. d. § 2 GwG.

Der § 261 StGB (Geldwäsche, Verschleierung unrechtmäßig erlangter Vermögenswerte) hat in Deutschland dem einen ganz klaren "Riegel" vorgegeben. Daraus folgt: Alle Verpflichteten (§ 2 GwG) haben einen solchen Verdacht an die Strafverfolgungsbehörden (Polizei, Staatsanwaltschaft, LKA) und in Kopie an das BKA - Zentralstelle für Verdachtsanzeigen - zu melden, § 11 GwG. Weiter ist an §§ 27 ff. StGB Beihilfe zu denken bzw. an eine Ordnungswidrigkeit i.S. des § 17 GwG bzw. sogar an eine Straftat nach § 261 Abs. 5 StGB (bei leichtfertiger Unterlassung der Anzeige).

Banken müssen insofern alle Transaktionen anzeigen, die Ihnen i.S. des § 261 StGB verdächtig erscheinen. Mit der Höhe der Geldtransaktion hat dies nur zweitrangig zu tun. "Ungewöhnliche" Geldübermittlungen sind per se verdächtig.

Informationsrechtlich - und auch von Seiten des Datenschutzes - ist gegen eine solche Meldung nichts einzuwenden. Solange das Kreditinstitut seinen Verdacht meldet, ob nun über Schreiben, über Telefon, über Fax, über E-Mail oder sonst wie elektronisch, immer geht es nur darum, dem GwG und dem § 261 StGB zu entsprechen. Vom Datenschutz her ist indessen noch zu prüfen, ob das BKA solche Daten bei den Banken selbst abrufen kann. Das Abrufsrecht ist eine andere Kategorie des Datenaustauschs (siehe Ringwald 1983). Evtl. ist ein Bereithalten zum Abruf bei ausreichenden Sicherungsmaßnahmen hinsichtlich anderer Daten zulässig.

Die Verdachtsverdichtung

Oftmals kann die Bank nicht wissen, ob ein einzelnes Vorkommnis zu einem Verdacht im Sinne einer Geldwäsche führen wird. Doch das Vorkommnis muss bei der Bank festgehalten werden dürfen. Ob nun elektronisch oder per Akte macht keinen Unterschied. Zunächst ist die Nichtanzeige eines Verdachts in § 17 Abs.1 Nr. 1 GwG mit Bußgeld bewehrt. Und § 261 Abs. 5

StGB stellt unter Strafe, "wer leichtfertig nicht erkennt, dass der Gegenstand aus einer in Abs. 1 genannten rechtswidrigen Tat herrührt" (also aus einer Geldwäsche). Unter leichtfertig ist eine gesteigerte Form der Fahrlässigkeit zu verstehen, aber eben nicht Vorsatz.

Innerhalb der gleichen Institutsgruppe in anderen EU-Ländern ist dies normiert (Datenaustausch zulässig, siehe § 12 Absatz 1 Nr. 2 GwG). Zu fremden Instituten ist dies nach dem Gedanken des Datenschutzrechts per IT nicht zulässig. Keinesfalls darf eine Benachrichtigung gleich welcher Art (auch nur telefonisch oder gesprächsweise) an die "Schutzgemeinschaft für allgemeine Kreditsicherung" (SCHUFA Holding AG) und dergleichen erfolgen. Ob von dort Informationen bezogen werden, bleibt dem Verpflichteten unbenommen.

Wichtig ist aus Gründen der Nachvollziehbarkeit, dass solche Vorkommnisse im Rahmen einer internen Verwaltung gespeichert sind (Zweigstelle, Name der eingebenden Mitarbeiterinnen oder Mitarbeiter etc.).

Keinesfalls dürfen solche Vorkommnisse bereits weitergemeldet werden (an Polizei, Staatsanwaltschaft, LKA oder BKA). Hat das einzelne Vorkommnis den Verdacht noch nicht ergeben, wäre die Anzeige wider besseren Wissens für die Anzeigerstellerin oder den Anzeigersteller sehr gefährlich. Es gibt den § 164 StGB (Falsche Verdächtigung). Aber was setzt einen Verdacht tatsächlich voraus? IST ein hinreichender Tatverdacht i. S. d. Strafprozessordnung (StPO) gemeint? Sicherlich nein; die StPO ist Strafverfahrensrecht, Normadressat ist nicht der Private! Gilt hier die Rechtsformel vom objektiven Beobachter (also ähnlich wie im Bürgerlichen Recht, BGB)? Dies alles ist ein Gebiet, das mit Normen wohl nicht zu regeln ist. Auch ist es juristisch bislang noch nicht hinreichend durchdacht.

Der Verfahrensgang

Ist ein Verdacht an das BKA gemeldet worden, ist seitens der Bank folgendes zu beachten:

1. Kündigung des Kontos. Eine einseitige Auflösung der Kontoverbindung ist rechtlich nicht zu beanstanden, sofern solches in die Vertragsbedingungen aufgenommen wurde (reines Privatrecht). Nach § 3 Abs. 6 GwG besteht sogar die Pflicht, bestehende Geschäftsbeziehungen zu beenden.
2. Reagieren bei Rückfragen. Hier gelten nicht die Regeln der StPO für Zeugen. Diese gelten nur in einem formellen Strafverfahren. Daraus folgt: Auf Anfrage einer ermittelnden Behörde muss man nichts aussa-

gen. Auf keinen Fall dürfen Tatsachen und auch Vermutungen, die mit der Anzeige nicht verbunden waren, einfach so weitergegeben werden. Meist spielt sich das alles am Telefon ab – und letztlich weiß niemand mehr, wer was gesagt hat. In diesem Fall ist ganz einfach darauf zu verweisen, dass die Verdachtsanzeige mit geänderter Begründung nochmals übermittelt wird.

3. Erledigungsrückmeldung. Ganz wichtig ist, dass die Anzeigerstellerinnen und Anzeigersteller darüber informiert werden, wann und wie das Verfahren strafrechtlich abgeschlossen wurde. Er hat dann die Daten über diesen Fall zu löschen (die Daten sind nicht mehr "zur Zweckbestimmung eines Vertragsverhältnisses oder vertragsähnlichen Vertrauensverhältnisses" notwendig (§ 28 Abs. 1 Nr. 1 BDSG)).

Übersicht des Strafverfahrens nach der StPO – Gang des Strafverfahrens

Das Strafverfahren unterteilt sich im Wesentlichen in drei Abschnitte: dem Vorverfahren, auch Ermittlungsverfahren genannt, dem Zwischenverfahren und dem Hauptverfahren (Eisenberg 2007: 1 ff.). Im Anschluss an das Hauptverfahren gibt es noch Rechtsmittelverfahren und Vollstreckungsverfahren (siehe Abbildung 84).

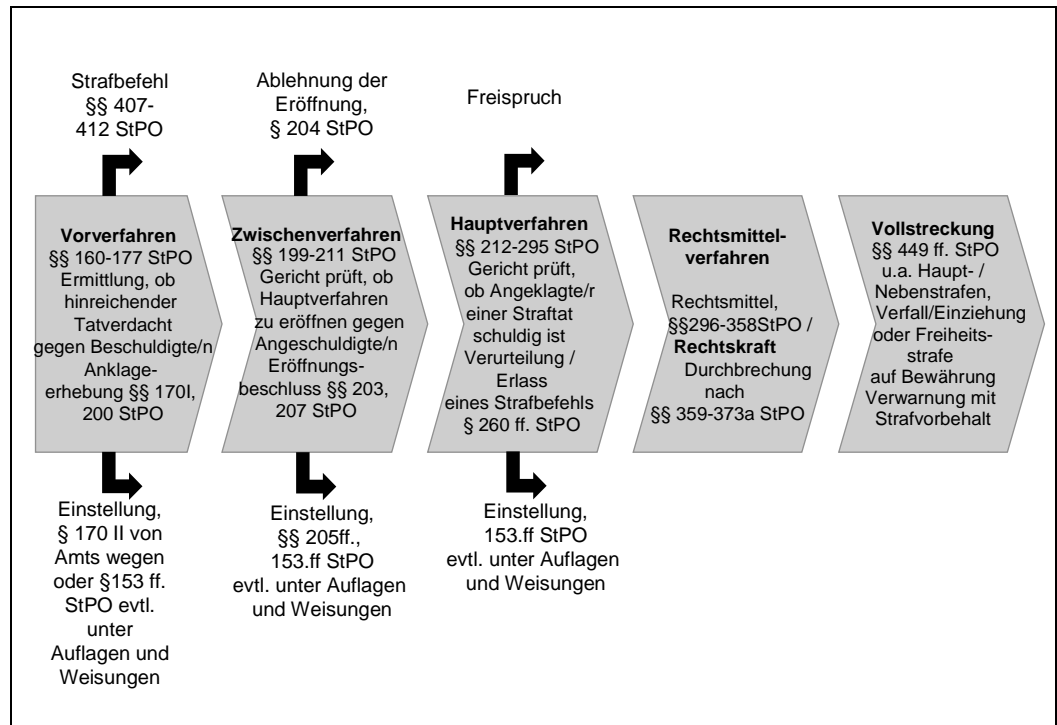


Abbildung 84: GVA Gang des Strafverfahrens – Kenntniserlangung der Strafverfolgungsorgane (Quelle: Eigene Darstellung)

Durch die Kenntniserlangung der Strafverfolgungsorgane aufgrund einer Anzeige gemäß 158 Abs. 1 und 160 Abs. 1 1. Alt. StPO wird das Strafverfahren in Gang gesetzt. Die Abbildungen beschreiben zum einen die einzelnen Stufen des gesamten Verfahrens und zum anderen, dass das Verfahren in jeder Stufe, z. B. durch Einstellung beendet werden kann oder es dann letztlich auf der letzten Stufe zum Ende des Hauptverfahrens, z. B. durch ein Urteil, kommen kann.

Vorverfahren

Das Vorverfahren, welches auch das Ermittlungsverfahren genannt wird, bestimmt sich nach den Vorschriften der Strafprozessordnung. Im Ermittlungsverfahren haben die Strafverfolgungsbehörden, im vorliegenden Fall die LKA und Staatsanwaltschaft, durch die Anzeige der Verpflichtenden i. S. d. § 2 GwG eine Anzeige auf Verdacht der Geldwäsche erhalten. So dass dieser Auslöser, das besagte Verfahren in Gang setzt. Aufgrund des sogenannten Legalitätsprinzips sind die Strafverfolgungsbehörden verpflichtet jeder An-

zeige nachzugehen gemäß § 163 StPO ff. Des Weiteren ist die Staatsanwaltschaft Herrin des Vorverfahrens.

Im Vorverfahren wird aufgrund der Anzeige und der Verpflichtung aufgrund des Amtsermittlungsgrundsatzes (§ 155 Abs. 2 StPO) ermittelt, ob tatsächlich ein Anfangsverdacht besteht. Besteht kein Anfangsverdacht, ist das Verfahren von Amtswegen nach § 152 Abs. 2 StPO einzustellen.

Nach dem Jahresbericht der BKA FIU (BKA 2008a: 20 f.) lassen sich die Ergebnisse der Clearingstellen der Geldwäsche (LKA) gerade im Hinblick auf das Vorverfahren folgendermaßen zusammenfassen: "Im Jahr 2007 wurden von den 9.080 Verdachtsanzeigen nach dem GwG in ca. 6 Prozent der Fälle die polizeilichen Ermittlungen (Clearing) ohne Restverdacht abgeschlossen. In rund 20 Prozent der Fälle erfolgte der Abschluss der Ermittlungen, ohne dass aus polizeilicher Sicht ein Restverdacht ausgeräumt werden konnte. In ca. 36 Prozent der Vorgänge war die Bearbeitung bei den Clearingstellen am Jahresende noch nicht abgeschlossen. Bei ca. 36 Prozent der Vorgänge hatte sich im Clearingprozess der Verdacht der Geldwäsche bzw. einer sonstigen Straftat so weit erhärtet, dass die Verfahren zur weiteren Bearbeitung an eine entsprechende polizeiliche Fachdienststelle abgegeben wurden. In weiteren ca. 2 Prozent der Fälle erhärtete sich der Verdacht einer Steuerstraftat, so dass die Verfahren an Finanzbehörden abgegeben wurden. Damit hat sich bei 38 Prozent der Anzeigen der Verdacht einer Straftat erhärtet (2006: 34 Prozent).

Besteht ein Anfangsverdacht, d. h. ein zureichend tatsächlicher Anhaltspunkt (§ 155 Abs. 2 StPO), ist von den Staatsanwaltschaften, die sich auch der Ermittlungspersonen der Polizei "bedienen" (§ 161 Abs. 1 StPO; 152 GVG), der Sachverhalt zu erforschen, ob ein hinreichender Tatverdacht vorliegt.

Ist dies nicht der Fall, wird das Verfahren nach § 170 Abs. 2 StPO durch die Staatsanwaltschaft eingestellt (Opportunitätsprinzip). Besteht ein hinreichender Tatverdacht und handelt es sich aber um eine "Bagatelle" (geringe Schuld), kann das Verfahren nach § 153 ff. StPO unter Auflagen und Weisungen (z. B. gegen Geldauflagen) eingestellt werden.

Besteht ein hinreichender Tatverdacht und kann dieser nicht nach §§ 153 ff. StPO eingestellt werden, hat die Staatsanwaltschaft die Erhebung der Anklage nach § 170 Abs. 1 StPO bzw. den Antrag auf Erlass eines Strafbefehls § 407 ff. StPO (welches nicht das Zwischenverfahren durchläuft) beim zuständigen Gericht zu beantragen.

Die Staatsanwaltschaft teilt das Ergebnis des Vorverfahrens in der Regel der Tatverdächtigen oder dem Tatverdächtigen bzw. der Beschuldigten oder

dem Beschuldigten (z. B. nach §170 Abs. 2 StPO), den Anzeigerstatten-
den und den Polizeibehörden (§ 482 StPO) mit.

Zwischenverfahren

Das Zwischenverfahren wird somit aufgrund des Antrags der Staatsanwalt-
schaft (Anklageerhebung § 170 Abs. 1 StPO) gemäß § 199 ff. StPO eingelei-
tet. Im Zwischenverfahren prüft das Gericht dann den Antrag der Staatsan-
waltschaft, ob ein solcher hinreichender Tatverdacht vorliegt, der zur Eröff-
nung des Hauptverfahrens gegeben sein muss. Des weiteren bekommen
Angeschuldigte i.S. des § 157 StPO in diesem Verfahrensabschnitt die Mit-
teilung über die Anklageschrift, so dass diese Beweisanträge und / oder
Einwände vorbringen kann (§ 201 StPO). Das Zwischenverfahren endet in-
dem das Gericht dem Antrag der Staatsanwaltschaft zustimmt (sog. Eröff-
nungsbeschluss nach §§ 203, 207 ff. StPO), den Antrag ablehnt (Nichteröff-
nungsbeschluss §§ 204 StPO) oder aber das Verfahren nach §§ 153 ff.
StPO gegen Auflagen und Weisungen einstellt.

Gegen den Nichteröffnungsbeschluss kann die Staatsanwaltschaft sofortige
Beschwerde gemäß § 210 Abs. 2 1. Var. StPO einlegen.

Das Ergebnis des Zwischenverfahrens wird in der Regel den Angeschuldig-
ten z. B. nach § 204 Abs. 2 StPO oder §153 ff. StPO, den Anzeigerstatten-
den als auch den Polizeibehörden (jeweils durch die Staatsanwaltschaft) §
482 StPO bekanntgegeben.

Gerade im Bereich der Wirtschaftskriminalität ist die Einstellungsquote recht
hoch, dies zeigt sich auch in der Statistik des Berichts der BKA FIU. Von den
insgesamt 4.107 eingegangenen Rückmeldungen der Staatsanwaltschaft wer-
den 3.749 Fälle anhand einer solchen Verfügung eingestellt.¹⁶ Das BKA be-
richterstattet (BKA 2008a: 29): "Damit liegt die Einstellungsquote bei rund 91
Prozent. Die Einstellungsverfügungen teilen sich nach der Art der Entschei-
dung wie folgt auf:

- gemäß § 170 Abs. 2 StPO 3563 Fälle

¹⁶ beachte hierbei die Problematik der unterschiedlichen Praxis der Rückmeldungen
einzelner Bundesländer, siehe Kap. 8.1.1

- gemäß § 153 Abs. 1 StPO 129 Fälle
- gemäß § 154 Abs. 1 StPO 35 Fälle (In den Fällen wird meistens begründet, dass zu erwarten ist, dass die Tatverdächtige oder der Tatverdächtige bzw. die Beschuldigte oder der Beschuldigte wegen eines anderen Tatbestandes verurteilt wird, so dass die Geldwäsche nicht ins Gewicht fällt.)
- gemäß § 205 StPO 20 Fälle (hierbei handelt es sich um eine vorläufige Einstellung, gerade bei dauernde Abwesenheit des Angeschuldigten)
- gemäß § 152 StPO 2 Fälle

Das heißt rund 95 Prozent der Einstellungen erfolgt nach § 170 Abs. 2 StPO."

Hauptverfahren

Im Hauptverfahren, welches sich nach den §§ 212-295 StPO richtet, prüft das Gericht (Ermittlungsgrundsatz), ob Angeklagte i. S. d. § 157 StPO einer Straftat schuldig ist.

Das Hauptverfahren endet mit dem Freispruch, einer Verurteilung bzw. dem Erlass eines Strafbefehls oder der Einstellung des Verfahrens, evtl. unter Auflagen und Weisungen (§ 153a StPO).

Im sog. Rechtsmittelverfahren stehen dann die Rechtsmittel der Berufung §§ 312 ff. und der Revision §§ 333 ff. StPO zur Verfügung.

Im Rahmen der Strafvollstreckung richtet sich das Verfahren nach dem sog. Vollstreckungsverfahren, §§ 449 ff. StPO. Vollstreckungsbehörde ist die Staatsanwaltschaft § 451 Abs. 1 StPO. Die Sanktion kann Strafe (Freiheitsstrafe - auf Bewährung oder Strafvollzug - oder Geldstrafe) und / oder Maßregel der Besserung und Sicherung sein.

8.2 Ziele und Anforderungen an die Prozesskette Level-1

Übergeordnete Ziele auf Seiten der Bank ist zum einen die **Einhaltung der gesetzlichen Verpflichtung** und zum anderen die **Abwendung von Reputationsschaden** für die Bank.

Übergeordnetes Ziel des Staats und seiner Organe ist, wie das GwG schon in seiner Überschrift bezeichnet, "**das Aufspüren von Gewinnen aus schweren Straftaten**".

In einem **PRK-Scoping** wurden im Projekt die Ziele und Anforderungen an die Prozesskette Level-1 erhoben. Für die Bankenseite wurden diese in einer Primärerhebung erhoben (Expertinnen- und Experteninterview am 16.10.2008 mit der Abteilung Compliance einer deutschen Universalbank); für die Seite der öffentlichen Verwaltung erfolgte eine Primär- und Sekundäranalyse (Gespräch mit BKA und veröffentlichte Dokumente zum Projekt "Elektronische Verdachtsanzeige (eVA)").

Ziele der Bank

Ziele der Bank sind gemäß der Expertinnen- und Experteninterviews:

1. Die Prozesskette Level-1 muss zu aller erst **rechtsverbindlich** sein, d. h. dass die Bank befähigt wird, die Geldwäscheverdachts-Anzeige als Organisation autorisiert ("**Firmenstempel**") und ohne Nennung von Mitarbeiterangabe ("**Mitarbeiter-Datenschutz**") vornehmen zu können. Sicherheit und Stabilität der Datenverbindung und -übertragung ist die damit verbundene Anforderung, Beispiel hierfür ist die Datenübermittlung über eine sicher Verbindung, ohne 8 MB-Upload-Mengen- oder Time-Out-Probleme etc. [GVA 1]
2. Die Bank braucht eine **aktive Rückmeldung von Seiten der öffentlichen Verwaltung zum Verlauf des Verfahrens** mit seinen unterschiedlichen Status im Rückkanal. Die Status wurden im Kap. 8.1.1 im einzelnen beschrieben. [GVA 2]
3. Die Bank braucht einen **rollengerechten Zugang zum Informationsstand des Verfahrensverlaufs** mit seinen unterschiedlichen Status, z. B. über ein Tracking- oder Trouble Ticket System. [GVA 3]

Der Unterschied zwischen Ziel 2 und Ziel 3 ist, dass bei erstem die öffentliche Verwaltung von sich aus aktiv informiert ("Information Push"), beim zweiten die Bank sich on-demand Abfragen zum Stand einer Anzeige erstellen kann ("Information Pull"). Wichtig über allem ist die Beschränkung der Zugangs-, Lese- und Schreibrechte gemäß der rechtlichen Rahmenbedingungen.

Ziele BKA und Projektkonsortium im Projekt eVA

Das BKA und das Projektkonsortium verfolgen im Projekt eVA folgende Ziele (siehe E-Government 2.0 Umsetzungsplan 2009, im Erscheinen):

1. Die Realisierung der elektronischen Verdachtsanzeige soll eine **qualitativ bessere, schnellere und sichere Übermittlung der Verdachtsanzeigen an das BKA** sowie die zentralen Fachdienststellen der Landeskriminalämter ermöglichen. [GVA 4]
2. Die elektronische Datenübermittlung **entlastet die Behörden, optimiert die Verfügbarkeit der Daten sowie deren Auswertung.** [GVA 5]
3. Weiterhin wird eine **Reduzierung des Kommunikationsaufwands** für die meldepflichtigen Finanzdienstleister und damit die **Erhöhung des Meldeaufkommens** durch medienbruchfreie, optimierte elektronische Verfahren angestrebt. [GVA 6]

Weitere Ziele sind:

- Beseitigung von Medienbrüchen, um eine (teil-)automatisierte Erfassung im polizeilichen Fachverfahren zu erreichen [GVA 7]
- Qualitätssteigerung durch Vermeidung von Erfassungsfehlern [GVA 8]
- Reduzierung eines Mehrbedarfs an Erfassungspersonal, der durch den weiteren zahlenmäßigen Anstieg von Verdachtsanzeigen bereits aktuell besteht [GVA 9]
- Verbesserung des Schutzes der übermittelten Daten hinsichtlich Vertraulichkeit, Integrität, Authentizität sowie schneller und umfassender Verfügbarkeit [GVA 10]
- Einhaltung der datenschutzrechtlichen Vorgaben [GVA 11]
- hohe Akzeptanz auf Seiten aller Meldeverpflichteten [GVA 12]
- Gewährleistung der Revisionssicherheit des gesamten Systems [GVA 13]
- Nutzung anerkannter Standards und Verfahren, welche sich bereits im Einsatz bewährt haben und über die somit ein breites Wissen auf Seiten aller Beteiligten herrscht, um diese ohne aufwändige Prüfungen übernehmen zu können [GVA 14]

8.3 Die Prozesskette Level-1

Die Meldung verdächtiger Transaktionen auf der Grundlage des Geldwäschegesetzes (GwG) wird auf ein elektronisches Verfahren umgestellt. Damit kommt das Bundeskriminalamt einer Forderung der Verpflichteten nach dem GwG nach, die derzeit beim Vorliegen des Verdachts der Geldwäsche oder der Finanzierung des Terrorismus eine in der Praxis papiergebundene Verdachtsanzeige abgeben müssen. Gemeinsam mit der Wirtschaft soll ein Verfahren entwickelt werden, das sowohl die Belange klein- und mittelständischer Unternehmen wie auch die Möglichkeiten von Großbanken und großen Finanzdienstleistern mit entsprechender IT-Ausstattung berücksichtigt und auf bestehenden IT-Systemen im Banken- und Finanzdienstleistungssektor aufbaut. Beim weiteren Ausbau der Prozesskette ist die Beteiligung weiterer Bundes- und Landesbehörden geplant (siehe E-Government 2.0 Umsetzungsplan 2009, im Erscheinen).

Die folgende Abbildung zeigt das Projekt eVA schematisch im Überblick (siehe Abbildung 85):

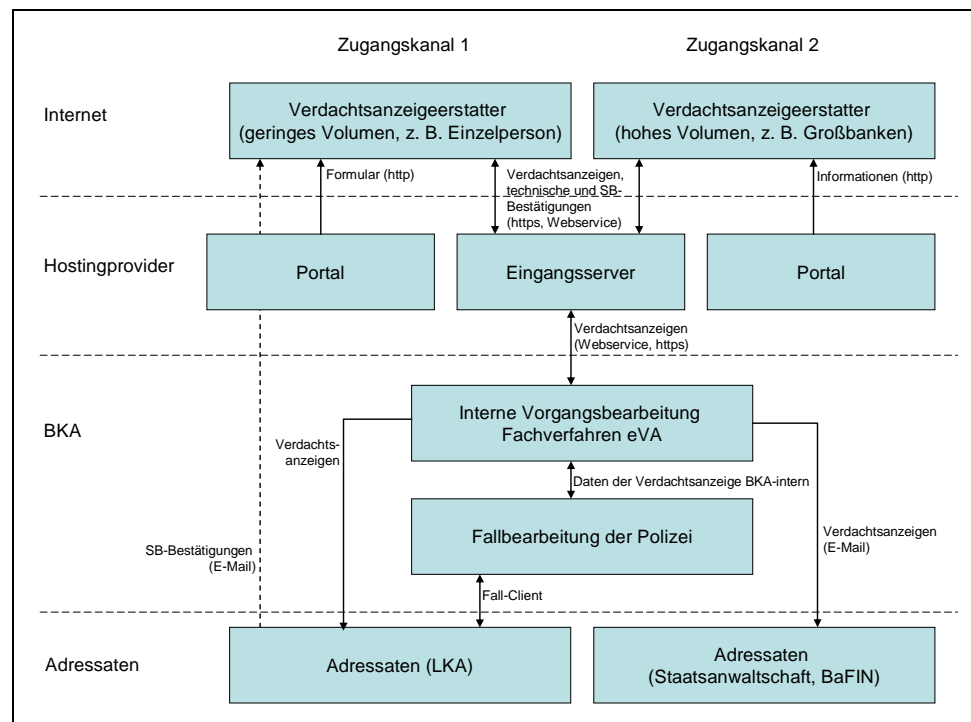


Abbildung 85: GVA SOLL-Verfahrensübersicht nach Projekt eVA (Quelle: Eigene Darstellung)

Es gibt zwei Zugangskanäle.

Kanal 1 segmentiert und adressiert Nutzerinnen und Nutzer mit einem geringen Anzeigenaufkommen, also z. B. Einzelpersonen, Gewerbetreibende und kleine Institute wie z. B. Sparkassen. Um Anzeige zu erstatten, können sich einzelne Anzeigenerstatterinnen und Anzeigenerstatter von den Portalen des BKA, der LKA oder anderen Portalen im Internet ein PDF-Formular zur Verdachtsanzeige herunterladen und das ausgefüllte PDF-Formular auf den Eingangsserver hochladen.

Kanal 2 richtet sich an die Institutionen der Kredit- und Finanzdienstleistungsbranche, die ein hohes Volumen an Verdachtsanzeigen aufweisen, das sind z. B. große Banken und Finanzdienstleister. Aus ihren Enterprise-Ressource-Planning Systemen (ERP) können die Großbanken Verdachtsanzeigen generieren. Die Daten werden dann per Secure Socket Layer (HTTPS) übertragen, auf dem Eingangsserver wird dazu ein Webservice zur Verfügung gestellt.

Die interne Vorgangsbearbeitung Fachverfahren eVA empfängt die elektronischen Verdachtsanzeigen vom Eingangsserver, sowohl von Kanal 1 als auch von Kanal 2. Das PDF-Formular mit Daten und Anlagen wird als Eingangsnachricht abgespeichert; strukturierte Daten werden extrahiert und gespeichert. Pro Verdachtsanzeige wird ein Vorgang neu angelegt, dem die jeweilige Eingangsnachricht zugeordnet wird.

Die Daten der Verdachtsanzeige werden über die aufgezeigten Schnittstellen an die Adressaten weitergemeldet.

8.3.1 Wirtschaftliche, prozessuale und organisatorische Beschreibung und Analyse

Die nachfolgende Abbildung zeigt die Prozesskette im SOLL, auf Basis der allgemeinen Ziele und Anforderungen an Level-1 und Generation 3 Prozessketten (Kap. 4) und der erhobenen spezifischen "PRK-Scoping" Ziele und Anforderungen in Kap. 8.2 (siehe Abbildung 86).

Es wird darauf hingewiesen, dass das Autorenteam der Studie im folgenden von einem "Hochleistungsportal zum Management von Geldwäschever-

dachts-Anzeigen" (HMG) sprechen.¹⁷ Auf dieses beziehen sich die Beschreibung, Analyse und Handlungsempfehlungen in den folgenden Kapiteln. Dort, wo verzeichnet, beziehen sich Informationen auf das Projekt eVA. Die Projektmitglieder der Studie sind nicht Mitglieder des Projektes eVA.

¹⁷ siehe zu Hochleistungsportalen und Business Communities, die diese Hochleistungsportale nutzen, die Standardwerke Lucke, v. 2008 und Bullinger et al. 2002

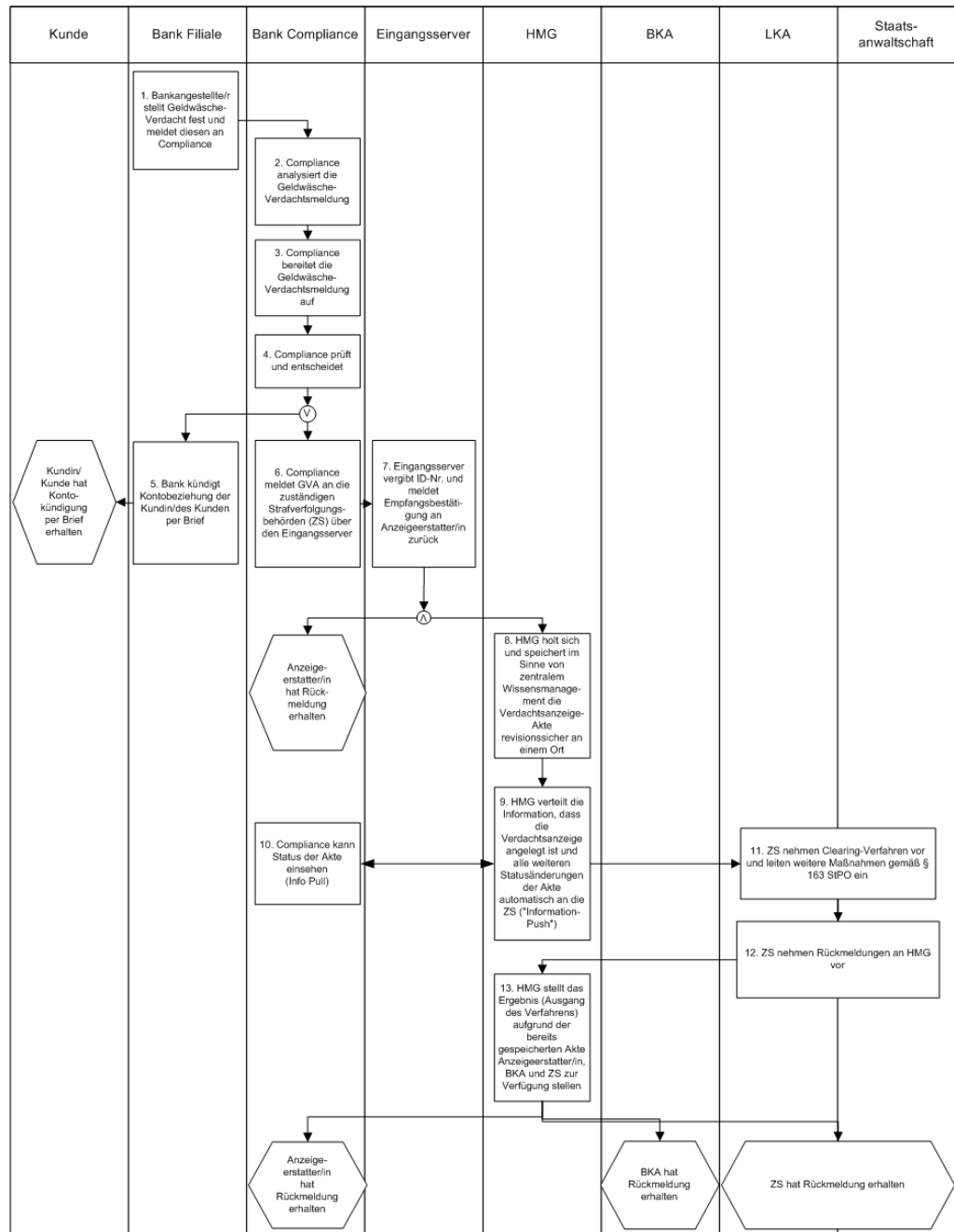


Abbildung 86: GVA Prozesskette Level-1 (EPK) (Quelle: Eigene Darstellung)

1. Die Bankangestellte oder der Bankangestellte stellen Geldwäsche-Verdacht fest und melden diesen an die Compliance¹⁸

Ein solcher Verdacht (verdächtige Finanztransaktion) wird z. T. durch den Berufsträger (z. B. Bankangestellten in einer Filiale) selbst, oder durch sonstige Hinweise an die zuständige Abteilung Compliance bzw. den Geldwäschebeauftragten gemeldet.

2. Die Compliance analysiert die Geldwäsche-Verdachtsmeldung

Der Sachverhalt ist nach Priorisierung vollständig zu überprüfen, ob sich dieser Verdacht weiter erhärten lässt.

3. Die Compliance bereitet die Geldwäsche-Verdachtsmeldung auf

Die Compliance bereitet die Entscheidung zur Verdachtsanzeige vor, oder aber der Sachverhalt lässt sich aufklären, so dass eine Erstellung der Verdachtsanzeige nicht notwendig ist.

4. Die Compliance prüft und entscheidet

In dieser Phase wird die aufbereitete Entscheidung der zuständigen Abteilung noch einmal nach dem sogenannten "Vier-Augen-Prinzip" überprüft und entscheidet, ob es zur Abgabe der Verdachtsmeldung kommt oder ob eine Negativentscheidung (keine Anzeige des Verdachts) ergeht.

5. Die Bank kündigt die Kontobeziehung per Brief

Mit der Abgabe der Verdachtsanzeige geht die Anweisung an die zuständige Kundenbetreuung bzw. den Vorgesetzten, das jeweilige Konto aufzulösen und zu kündigen.

¹⁸ im weiteren wird in der Beschreibung und Analyse auf diejenigen Teile des SOLL-Prozesses verstärkt eingegangen, in denen er sich vom IST-Prozess unterscheidet

6. Die Compliance meldet die Geldwäscheverdachts-Anzeige (GVA) an die zuständigen Strafverfolgungsbehörden über den Eingangsserver

Die Verpflichtende oder der Verpflichtende (Anzeigerstatter) kann im SOLL-Prozess im Unterschied zum IST-Prozess die Verdachtsanzeige online abgeben. Der Eingangsserver kann Teil des Hochleistungsportals zum Management von Geldwäscheverdachts-Anzeigen (HMG) sein, oder als reiner Empfangsserver dem Workflow des HMG vorgeschaltet.

Die Verdachtsanzeige wird als XML-Datenstrom abgegeben, es können Anhänge wie PDF, JPG etc. beigefügt werden, dabei handelt es sich z. B. um Kontoauszüge, Vertragskopien etc. Das inhaltlich bewährte Anzeigeformular (bisher PDF-Dokument bzw. Papier) ist zu verwenden.

Der Eingangsserver kann sowohl solche Anzeigerstatter mit hohem Anzeigevolumen (z. B. Banken) als auch solche mit geringem Anzeigevolumen (z. B. Einzelpersonen) bedienen und so zwei verschiedene kundensegmentierte Kanäle zur Verfügung stellen.

7. Der Eingangsserver vergibt automatisch eine ID-Nr. und meldet Empfangsbestätigung an die Anzeigerstatter zurück

Der Eingangsserver erstellt dann pro GVA eine ID-Nr. und meldet diese an die Anzeigerstatter zurück. Dadurch wird das bisherige papierbasierte Verfahren medienbruchfrei ersetzt. Gemäß § 11 Abs. 2 GwG ist eine Verdachtsanzeige auch durch elektronische Datenübermittlung möglich. In diesen Eingangsserver können dann, im Falle der Nachmeldungen (Anlagen), jeweils per Datenübermittlung an die ID-Nr. ebenfalls medienbruchfrei nachgereicht werden.

8. Das HMG holt sich und speichert im Sinne von zentralem Wissensmanagement die Verdachtsanzeige-Akte revisionssicher an einem Ort

Die in dem Eingangsserver abgelegten Daten (Anzeige, ggf. Anlagen), werden dann in einen "zentralen Datenpool" empfangen und gespeichert. Die Daten werden im Sinne eines zentralen Wissensmanagement revisionssicher abgelegt.

Technologisch können die Daten von dort aus als XML extrahiert werden. Dadurch ist es möglich, die folgenden weiteren Verfahrensschritte in dem Prozess medienbruchfrei und automatisiert fortzusetzen (Webservices). Es bestehen dedizierte Lese- und Schreibrechte entsprechend der Rollen der Beteiligten (Benutzerverwaltung).

Eine Möglichkeit einen solches HMG an einem (virtuellen) Ort zu verwalten, wäre durch das BKA als Betreiber gegeben – zumal es die zentrale Stelle für Verdachtsanzeigen im Bereich Geldwäsche darstellt.

9. Das HMG verteilt die Information, dass die Verdachtsanzeige angelegt ist und alle weiteren Statusänderungen der Akte automatisch an die zuständigen Strafverfolgungsbehörden ("Information-Push")

Die eingegangene GVA muss dann an die zuständigen Strafverfolgungsbehörden, d. h. an die jeweiligen zuständigen Landeskriminalämter und den zuständigen Staatsanwaltschaften, weitergeleitet werden.

Im modernsten Hol- und Bringsschuldmanagement der Beteiligten ist es möglich, die Daten zentral auf dem HMG zu speichern und zu pflegen und nur die Benachrichtigungsinformation, dass sich ein Status geändert hat, an die Beteiligten zu übermitteln. Dadurch werden redundante Daten, Versionskonflikte, Friktionen, Zuständigkeitsunklarheiten etc., mit allen verbundenen Management- und Datenschutzproblemen, de jure und de facto vermieden.

Regelbasierte Informations-Workflows sind über die event-getriggerten Informations-Workflows hinaus denkbar.

10. Die Compliance fragt bei Bedarf den Status der Akte ab ("Information-Pull")

In diesem Schritte der SOLL-Prozesskette kann die Bank unter bestimmten Voraussetzungen (s. o.) den Status der Akte einsehen.

Das HMG sollte insofern eine Tracking- und Trouble-Ticket-Funktionalität anbieten.

11. Die zuständigen Strafverfolgungsbehörden nehmen Clearing-Verfahren vor und leiten weitere Maßnahmen gemäß § 163 StPO ein

Durch die Kenntniserlangung der Strafverfolgungsorgane aufgrund der weitergeleiteten Anzeige wird das Strafverfahren in Gang gesetzt.

12. Die zuständigen Strafverfolgungsbehörden nehmen Rückmeldungen an die HMG vor

Die Staatsanwaltschaft unterrichtet die Polizeibehörden, vorliegend LKA, über den Ausgang des Verfahrens nach § 482 StPO. Gemäß § 11 Abs. 8 GwG teilt die zuständige Staatsanwaltschaft dem BKA, die Erhebung der öffentlichen Klage und den Ausgang des Verfahrens mit.

Um einen medienbruchfreien end-to-end Prozess zu ermöglichen, ist eine Rückmeldung an das zentrale System von erheblichem Vorteil.

13. Das HMG stellt das Ergebnis (Ausgang des Verfahrens) aufgrund der bereits gespeicherten Akte der Anzeigerstatterin oder dem Anzeigerstatter, BKA und zuständigen Strafverfolgungsbehörden zur Verfügung stellen.

Dies kann in Form eines Strafbefehls, Beschlusses oder Urteils erfolgen.

Die Bank hat nach § 11 Abs. 8 GwG einen Auskunftsanspruch. Das HMG muss das Ergebnis (Ausgang des Verfahrens) aufgrund der bereits gespeicherten Akte der Anzeigerstatterin oder dem Anzeigerstatter zur Verfügung stellen.

Es bedarf keiner Begründung, welche Entscheidung der Beendigung zugrunde liegt. Die Bank muss bei Erledigung des Verfahrens die Daten zu diesem Fall löschen. Die Speicherung ist dann nicht mehr zur Aufgabenerfüllung erforderlich. Sonst droht ein Konflikt mit dem BDSG, sofern solche Daten elektronisch gespeichert sind.

8.3.2 IT-architektonische Beschreibung und Analyse

Die allgemeinen Ziele für eine Prozesskette Level-1 sind in Kap. 4 beschrieben, die erhobenen spezifischen "PRK-Scoping" Ziele und Anforderungen in Kap. 8.2.

Für die IT-Architektur eines HMG besonders wichtig sind eine sichere, dem sehr hohen Schutzbedarf angepasste Kommunikation, Medienbruchfreiheit und Kompatibilität zu bestehenden und zu schaffenden Systemen in einem übergreifenden Gesamtsystem.

Das eVA-Verfahren und Level-1

Als Basis für die GVA Prozesskette im SOLL dient die Betrachtung des Projekts eVA. Hierauf aufbauend wird untersucht, wie die entsprechende Prozesskette auf Level-1 und in Generation 3 aussehen kann.

Das Projekt eVA läuft zur Zeit im internen Pilotbetrieb, der Wirkbetrieb ist für 2009 geplant. Die Projektmitglieder der Studie sind nicht Mitglieder des Projektes eVA.

Es ist geplant, das eVA-Verfahren über zwei Kanäle anzubieten. Kanal 1 für ein geringes Meldeaufkommen wird über ein Portal ein PDF-Formular bereitstellen, das sich selbst an den Eingangsserver sendet. Kanal 2 wird eine Webplattform sein, der direkt von den Fachanwendungen der Banken angesprochen werden kann. Es gibt nur einen Ansprechpartner, das BKA, das interne Bearbeitungssystem sorgt dafür, dass die GVA mit einigen Informationen angereichert an die in der GVA aufgeführten Adressaten weitergeleitet wird.

Datenschema

Das Datenschema von eVA folgt dem bekannten Meldeformular des BKA (PDF-Dokument, Papier). Anhänge bestimmter Typen sind möglich.

Laut Beschreibung können über den Kanal 2 mehrere GVA übermittelt werden. Das wird aber nur algorithmisch durch Versenden mehrerer GVA erfolgen, da als Quittung genau eine ID-Nr. zurückgegeben wird.

Folgende Entwicklungen sind in Bezug auf Level-1 für ein HMG denkbar:

- Die Datenstruktur für den Bereich Beweismittel kann weiter verfeinert werden; so ist in einer Transaktion kein Wert über die Höhe der Transaktion vorgesehen.
- Auf die Nutzung der XML-Sicherheitsmechanismen (Signatur und Verschlüsselung) wird zur Zeit noch verzichtet. Hier bestehen im Hinblick auf den hohen Schutzbedarf Entwicklungspotenziale (Beurkundung der Gleichheit eines Dokuments durch eine Mitarbeiterin oder einen Mitarbeiter und Schutz des Abbildes vor unbemerkter Veränderung gescannter Dokumente).
- Das Dokument sollte grundsätzlich zu keinem Zeitpunkt unverschlüsselt vorliegen (abgesehen von der Bearbeitung in einer sicheren Umgebung). Dazu ist ein Identity- und Access-Management notwendig, das den Zugang und Zugriff regelt.

Architektur und Schnittstellen

Die Architektur von eVA wird mit ihren Schnittstellen in der folgenden Abbildung grob beschrieben. Es wird darauf verzichtet, die bankinternen Datenbanken und Monitoring-Werkzeuge aufzuführen. Ausgeblendet wurde auch die Sicherheits- und Zertifikats-Infrastruktur. Weiterhin werden die nachgeordneten Institutionen pauschal zusammengefasst (siehe Abbildung 87).

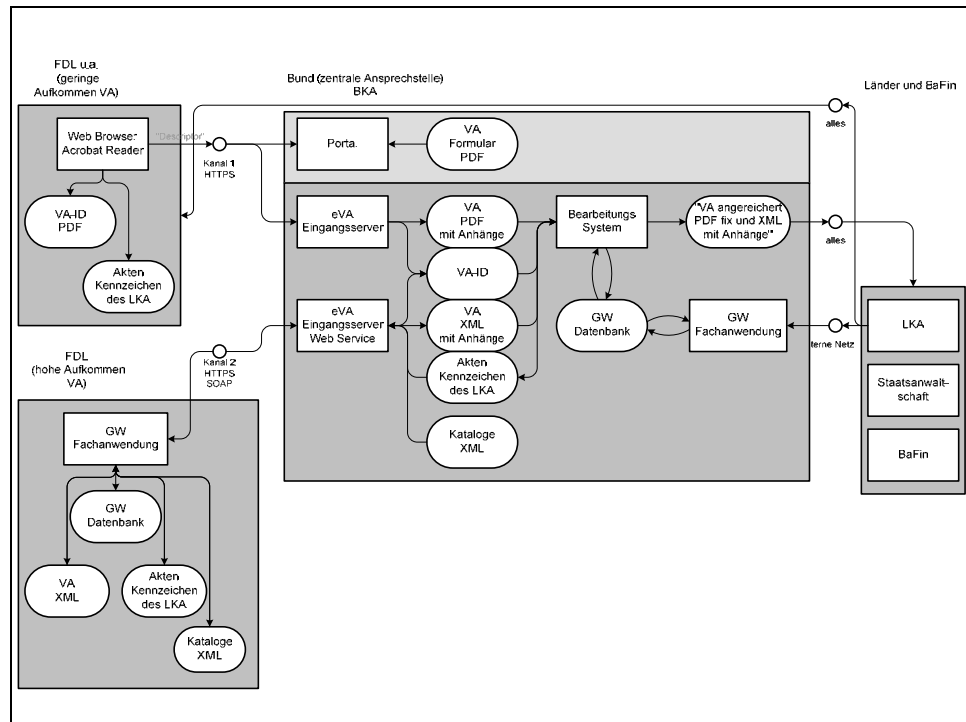


Abbildung 87: GVA Architektur Level-1 für Projekt eVA (FMC) (Quelle: Eigene Darstellung)

Schnittstelle Kanal 1

Aus dem Portal können sich verpflichtete Interessenten das Anzeigeformular beschaffen, ausfüllen und zurücksenden (PDF-Dokument). Als Quittung bekommen sie die vom Eingangsserver vergebene fortlaufende Nummer der GVA (PDF-Dokument), später kommt noch auf einem der angegebenen Kommunikationswege das Aktenkennzeichen des LKA hinzu.

Folgende Entwicklungen sind in Bezug auf Level-1 für ein HMG denkbar:

- Es ist zzt. keine elektronische Signatur vorgesehen. Dadurch kann ggf. nicht verhindert werden, dass eine Person eine fingierte GVA in fremden Namen macht. Durch Nutzung eines Trust Centers und der fortgeschrittenen oder qualifizierten elektronischen Signatur (z. B. der Smartcards der Banken oder anderer akkreditierter Anbieter oder des ePA mit Signatur) kann das Problem zukunftssicher gelöst werden.
- Die Passwortsicherung der PDF-Dokument kann verbessert werden. Mit angemessener Verschlüsselung, in Kombination mit der oben genannten Signatur ist deutlich mehr Sicherheit zu erreichen.

Schnittstelle Kanal 2

Die Fachanwendung Geldwäsche (GW) einer Bank kann, nach dem der interne Prozess der Bank für eine GVA durchlaufen ist, die GVA mit allen Beweismitteln zusammenstellen und als XML-Dokument versenden. Als Quittung kommt die vom Eingangsserver vergebene fortlaufende Nummer der GVA (XML-Dokument) zurück, später kann die Anwendung auch das Aktenkennzeichen des LKA abfragen. Es besteht auch die Möglichkeit, Kataloge der zulässigen Werte einiger Attribute vom Server zu holen.

Folgende Entwicklungen sind in Bezug auf Level-1 für ein HMG denkbar:

- Eine notwendige Rückmeldung, ob das Konto möglicherweise offen gehalten werden soll, kann integriert werden.
- Im XML-Dokument wird das Signieren und Verschlüsseln ermöglicht. Damit wird die zzt. verwendete Benutzerkennung als Sicherheit erweitert. Dadurch kann dann auch der sehr hohe Schutzbedarf abgedeckt werden.
- Z. B. kann sich die Abteilung Compliance einer Großbank wie die Commerzbank AG vorstellen, mit dem üblichen Meldeformular ein Zugriffstoken zu verschicken, der die Ermittlungsbehörden berechtigen würde auf die zugehörigen Daten ihrer Fachanwendung zu zugreifen. Das würde eine umfassende und zeitnahe Information ermöglichen. Das könnte weiter bis zu einer direkten Kopplung der beiden GW-Fachanwendungen auf Seite der Banken und auf Seite des BKA gehen. Dazu bedarf es aber sicher einer weitergehenden Standardisierung oder einer semantischen Transformation der Daten. Weiterhin müsste bei der Bank ein Webservice für die Kopplung geschaffen werden. Notwendige Voraussetzung ist die Schaffung einer föderierten Infrastruktur mit einem entsprechenden Identity- und Access-Management (siehe Kap. 4.2.3).

Schnittstelle vom BKA zu den Landesbehörden und BaFin

Sie bekommen sowohl eine PDF- als auch eine XML-Datei, die vorher mit weiteren Daten aus der Fachanwendung angereichert wurde. Die Dokumente sind auch nicht mehr veränderbar. Die Übertragung erfolgt für die LKA über die interne EPOST im internen Netz, Staatsanwaltschaft und BaFin werden per Fax oder verschlüsselter E-Mail versorgt. Für die Verschlüsselung gibt es wieder eine eigene Nutzer- und Schlüsselverwaltung.

Für die Arbeit an den GW-Daten haben die LKA über einen Client des Fachverfahrens im internen Netz direkten Zugriff auf die Daten beim BKA.

Folgende Entwicklungen sind in Bezug auf Level-1 für ein HMG denkbar:

- Es könnte die Kommunikation mit der BaFin über deren "Melde- und Veröffentlichungsplattform" (MVP) (BaFin 2008) erfolgen bzw. über föderierte Webservices zwischen eVA und MVP.
- Es ist anzudenken, inwieweit für die Kommunikation mit der Staatsanwaltschaft nicht das "Elektronisches Gerichts- und Verwaltungspostfach" (www.egvp.de) benutzt werden kann.

Sicherheitszonen

In Abbildung 87 oben sind keine Sicherheitszonen eingezeichnet, trotzdem ist jede IT-Infrastruktur, die am Internet angeschlossen ist, mit verschiedenen Sicherheitszonen auszustatten (BMI 2008, BSI 2005, Kuhlisch 2007, www.fallakte.de u. a.). In der Regel werden wenigstens drei Zonen benötigt:

- Die demilitarisierte Zone (DMZ, Informations- und Dienstzone, Portalzone), die direkt Daten über das Internet austauscht und relativ offen ist.
- Die Application-Zone (Anwendungszone), in der die Anwendungen laufen und zu der nur die Fachanwender Zutritt haben.
- Die Backend-Zone (Datenzone), in der die Daten lagern und zu der nur Administratoren zwecks Wartung und Backup Zutritt haben.

Zur letzten Zone gehört die "GW Datenbank" und zu der Fachanwendungszone die Anwendungen "Bearbeitungssystem", "GW Fachanwendung" und eventuell weitere Anwendungen, die in dem geschlossenen Netz der Polizei laufen.

Oft wird auch noch eine Authentisierungszone geschaffen mit ähnlichen Restriktionen wie sie die Backend-Zone kennzeichnen. Weiterhin kann eine Management-Zone eingerichtet werden, für die etwas andere Zugriffs- und Weiterleitungsrestriktionen gelten, als für andere Zonen.

8.3.3 Sicherheitstechnische Beschreibung und Analyse

Im Hinblick auf die allgemeinen Ziele und Anforderungen an Level-1 und Generation 3 Prozessketten (Kap. 4) und die erhobenen spezifischen "PRK-Scoping" Ziele und Anforderungen in Kap. 8.2 sind besonders folgende si-

cherheitstechnischen Punkte für die Prozesskette GVA im SOLL zu beleuchten.

Verschlüsselung der Transportwege

Die Übertragung des GVA-Formulars erfolgt über HTTPS auf den HMG. Client-Zertifikate wären für diesen Teilprozess nützlich, um z. B. "Man-in-the-middle"-Szenarien zu vermeiden. Für den Einsatz von Client-Zertifikaten gibt es Unterschiede zwischen Kanal 1 und Kanal 2:

- Für Kanal 1 ist die Verwendung von Client-Zertifikaten aufgrund der heterogenen Teilnehmergruppen praktisch schwer zu erzwingen. Ihre Verwendung sollte deshalb optional sein.
- Für Meldungen über Kanal 2 sind Client-Zertifikate vergleichsweise einfach zu implementieren. Da hier zwar ein hohes Aufkommen an Verdachtsanzeigen vorliegt, aber gleichzeitig die Kommunikationsbeziehungen (Partner, Übertragungswege) zwischen Finanzdienstleistern und dem HMG weitgehend festgelegt sind.

Eine Verwendung von Pseudonymen in den Zertifikaten ist unproblematisch, solange sichergestellt ist, dass die Pseudonyme im Bedarfsfall aufgelöst werden können. Dies setzt zum einen die Verwendung mindestens fortgeschrittener Zertifikate, zum anderen ein fixiertes Regelwerk über die Zulässigkeit der Auflösung von Pseudonymen und die dabei anzuwendenden Verfahrensweisen voraus.

Alle weiteren innerhalb der Prozesskette GVA notwendigen Daten-Transportwege müssen verschlüsselt (HTTPS oder VPN über IPsec) werden und müssen zur Verhinderung von Angriffen zusätzlich Client-Zertifikate verwenden. Dies gilt auch für "interne" Netze, so dass selbst bei einem Einbruch in ein solches Netz das Mitlesen der Datenströme vermieden wird. Teilprozessketten mit der Sicherheitsstufe "sehr hoch" dürfen beim Daten-Transport über öffentliche Netze nur VPN-Lösungen verwenden. Hierzu ist insbesondere die SINA-Lösung des BSI zu empfehlen (BSI 2008c), die auch strengen Geheimhaltungsanforderungen genügt und somit auch den hohen Sicherheitsansprüchen der FDL gerecht werden kann.

Verschlüsselung und Signatur der Dokumente

Wie unter Kap. 8.3.2 beschrieben, ist weder für Kanal 1 noch für Kanal 2 vorgesehen, dass das Verdachtsanzeige-Formular signiert werden muss. Der Beweiswert dieser Formulare ist damit im Zweifelsfall eher gering. Die Verwendung fortgeschrittener elektronischer Signaturen erhöht den Beweis-

wert. Zusätzlich ist zu berücksichtigen, dass die bei den FDL tätigen Personen einem u. U. hohem Risiko ausgesetzt sind, wenn ihnen konkrete Verdachtsanzeigen zugeordnet werden können. Deshalb ist bei GVA über Kanal 2 die Nutzung von Pseudonymen vorzusehen. Das Pseudonym kann dann z. B. auf Antrag eines Gerichts von der zuständigen CA aufgelöst werden.

Archivierung der Dokumente und der Signaturen

Zur Wahrung der Revisionssicherheit müssen alle im Zusammenhang mit der GVA erzeugten elektronischen Dokumente für lange Aufbewahrungsfristen gemäß den gesetzlichen Bestimmungen geeignet sein. Dazu sind entsprechende Archivierungs-Datenträger zu verwenden. Es muss sichergestellt werden, dass die Dokumente auch nach langen Zeiträumen noch entschlüsselt und die Signaturen überprüft werden können. Wurden Zertifikate akkreditierter Trustcenter verwendet, sollte i. d. R. die Entschlüsselung möglich sein, sofern ein Key-Recovery-Verfahren realisiert wurde. Gleiches gilt auch für die Überprüfung der Signaturen. Allerdings kommt es vor, dass selbst standardisierte Datenformate verändert werden, um diese an die jeweils aktuellen technischen Gegebenheiten anzupassen. Dann ist neben der Daten- oder Datenträgerkonvertierung auch eine rechtsichere Transformation der elektronisch signierten sowie ggf. verschlüsselten Dokumente notwendig. Lösungen hierzu findet man bei den Projekten ArchiSig und TransiDoc (TransiDoc 2007).

8.3.4 Juristische Beschreibung und Analyse

Generelle Textquellen zur juristische Beschreibung und Analyse der GVA im SOLL sind, neben dem **Bundesdatenschutzgesetz** (BDSG) und den jeweiligen Datenschutzgesetzen der Länder, vor allem das **Geldwäschegesetz** vom 13. August 2008 (BGBl. I S. 1690), Gesetz über das Aufspüren von Gewinnen aus schweren Straftaten (Geldwäschegesetz - GwG). Es ist gemäß Art. 11 Satz 1 dieses Gesetzes am 21.08.2008 in Kraft getreten. Bereits am 22.09.1992 wurde in das Strafgesetzbuch als § 261 StGB die Geldwäsche, Verschleierung unrechtmäßig erlangter Vermögenswerte, eingefügt (letzte Änderung mit GwG).

Die **Banken** waren dadurch verpflichtet, eine Arbeitsmethode zu entwickeln, die diesen Gesetzen Rechnung trug. Nach § 17 GwG Abs. 1 sind bei Vorsatz oder Leichtfertigkeit 100.000 Bußgeld Euro angedroht, nach Abs. 2 bei Vorsatz und Fahrlässigkeit 50.000 Euro. Die Strafbewehrung nach § 261 Abs. 3 StGB sieht eine Strafbarkeit vor, "[...] wer leichtfertig nicht erkennt, dass ein Gegenstand" aus einem dort genannten Delikt (Verbrechen, be-

stimmte schwere Straftat (siehe unten Gesetzestext zu § 261 StGB)) herührt, nämlich bis zu 2 Jahren oder Geldstrafe. Daneben ist auch Beihilfe nach § 27 StGB zu einer rechtswidrigen Tat eines Dritten möglich. Weiterhin ist zu beachten, dass die Datenschutzgesetze ihrerseits Sanktionen kennen, sofern unrechtmäßig Daten gespeichert, verarbeitet bzw. übermittelt werden oder auch zum Abruf bereitgehalten werden.

Es besteht für Banken also nach zwei Seiten hin eine Pflicht: Einerseits dem GwG bzw. § 261 StGB Genüge zu tun, andererseits den Schutz des Persönlichkeitsrechts zu wahren. Auch das BDSG ist mit Sanktionen bewehrt (§ 43 BDSG = Bußgeld bis zu 25.000 Euro, bzw. 250.000 Euro; § 44 BDSG bei Vorsatz und Bereicherungs- bzw. Schädigungsabsicht bis 2 Jahre oder Geldstrafe).

§ 17 GwG Bußgeldvorschriften

(1) Ordnungswidrig handelt, wer vorsätzlich oder leichtfertig

1. entgegen § 3 Abs. 1 Nr. 1 eine Identifizierung des Vertragspartners nicht vornimmt,
2. entgegen § 8 Abs. 1 erhobene Angaben oder eingeholte Informationen nicht, nicht richtig oder nicht vollständig aufzeichnet,
3. entgegen § 8 Abs. 3 Aufzeichnungen und sonstige Belege über Geschäftsbeziehungen und Transaktionen nicht aufbewahrt oder
4. entgegen § 11 Abs. 1 der Pflicht zur Anzeige eines Verdachtsfalls nicht nachkommt.

(2) Ordnungswidrig handelt, wer

1. entgegen § 3 Abs. 1 Nr. 3 das Vorhandensein eines wirtschaftlich Berechtigten nicht abklärt,
2. entgegen § 4 Abs. 5 Satz 1 den Namen des wirtschaftlich Berechtigten nicht erhebt,
3. entgegen § 6 Abs. 2 Nr. 2 die Identität des Vertragspartners nicht überprüft oder nicht sicherstellt, dass die erste Transaktion von einem auf den Namen des Vertragspartners eröffneten Konto erfolgt, oder
4. entgegen § 12 Abs. 1 den Auftraggeber oder eine andere als die in § 12 Abs. 1 Satz 2 genannten Stellen oder Personen in Kenntnis setzt.

(3) Die Ordnungswidrigkeit kann in den Fällen des Absatzes 1 mit einer Geldbuße bis zu hunderttausend Euro, in den Fällen des Absatzes 2 mit einer Geldbuße bis zu fünfzigtausend Euro geahndet werden

§ 261 Geldwäsche, Verschleierung unrechtmäßig erlangter Vermögenswerte StGB

(1) ¹Wer einen Gegenstand, der aus einer in Satz 2 genannten rechtswidrigen Tat herrührt, verbirgt, dessen Herkunft verschleiert oder die Ermittlung der Herkunft, das Auffinden, den Verfall, die Einziehung oder die Sicherstellung eines solchen Gegenstandes vereitelt oder gefährdet, wird mit Freiheitsstrafe von drei Monaten bis zu fünf Jahren bestraft. ²Rechtswidrige Taten im Sinne des Satzes 1 sind

1. Verbrechen,

2. Vergehen nach

a) § 332 Abs. 1, auch in Verbindung mit Abs. 3, und § 334,

b) § 29 Abs. 1 Satz 1 Nr. 1 des Betäubungsmittelgesetzes und § 19 Abs. 1 Nr. 1 des Grundstoffüberwachungsgesetzes,

3. Vergehen nach § 373 und nach § 374 Abs. 2 der Abgabenordnung, jeweils auch in Verbindung mit § 12 Abs. 1 des Gesetzes zur Durchführung der Gemeinsamen Marktorganisationen und der Direktzahlungen,

4. Vergehen

a) nach den §§ 152a, 181a, 232 Abs. 1 und 2, § 233 Abs. 1 und 2, §§ 233a, 242, 246, 253, 259, 263 bis 264, 266, 267, 269, 271, 284, 326 Abs. 1, 2 und 4, § 328 Abs. 1, 2 und 4 sowie § 348,

b) nach § 96 des Aufenthaltsgesetzes, § 84 des Asylverfahrensgesetzes und nach § 370 der Abgabenordnung, die gewerbsmäßig oder von einem Mitglied einer Bande, die sich zur fortgesetzten Begehung solcher Taten verbunden hat, begangen worden sind, und

5. Vergehen nach §§ 129 und 129a Abs. 3 und 5, jeweils auch in Verbindung mit § 129b Abs. 1, sowie von einem Mitglied einer kriminellen oder terroristischen Vereinigung (§§ 129, 129a, jeweils auch in Verbindung mit § 129b Abs. 1) begangene Vergehen.

³Satz 1 gilt in den Fällen der gewerbsmäßigen oder bandenmäßigen Steuerhinterziehung nach § 370 der Abgabenordnung für die durch die Steuerhinterziehung ersparten Aufwendungen und unrechtmäßig erlangten Steuererstattungen und -vergütungen sowie in den Fällen des Satzes 2 Nr. 3 auch für einen Gegenstand, hinsichtlich dessen Abgaben hinterzogen worden sind.

(2) Ebenso wird bestraft, wer einen in Absatz 1 bezeichneten Gegenstand

1. sich oder einem Dritten verschafft oder

2. verwahrt oder für sich oder einen Dritten verwendet, wenn er die Herkunft des Gegenstandes zu dem Zeitpunkt gekannt hat, zu dem er ihn erlangt hat.

(3) Der Versuch ist strafbar.

(4) ¹In besonders schweren Fällen ist die Strafe Freiheitsstrafe von sechs Monaten bis zu zehn Jahren. ²Ein besonders schwerer Fall liegt in der Regel vor, wenn der Täter gewerbsmäßig oder als Mitglied einer Bande handelt, die sich zur fortgesetzten Begehung einer Geldwäsche verbunden hat.

(5) Wer in den Fällen des Absatzes 1 oder 2 leichtfertig nicht erkennt, daß der Gegenstand aus einer in Absatz 1 genannten rechtswidrigen Tat herrührt, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.

(6) Die Tat ist nicht nach Absatz 2 strafbar, wenn zuvor ein Dritter den Gegenstand erlangt hat, ohne hierdurch eine Straftat zu begehen.

(7) ¹Gegenstände, auf die sich die Straftat bezieht, können eingezogen werden. 2§ 74a ist anzuwenden. 3§ 73d ist anzuwenden, wenn der Täter gewerbsmäßig oder als Mitglied einer Bande handelt, die sich zur fortgesetzten Begehung einer Geldwäsche verbunden hat.

(8) Den in den Absätzen 1, 2 und 5 bezeichneten Gegenständen stehen solche gleich, die aus einer im Ausland begangenen Tat der in Absatz 1 bezeichneten Art herrühren, wenn die Tat auch am Tatort mit Strafe bedroht ist.

(9) ¹Nach den Absätzen 1 bis 5 wird nicht bestraft, wer

1. die Tat freiwillig bei der zuständigen Behörde anzeigt oder freiwillig eine solche Anzeige veranlasst, wenn nicht die Tat in diesem Zeitpunkt ganz oder zum Teil bereits entdeckt war und der Täter dies wusste oder bei verständiger Würdigung der Sachlage damit rechnen musste, und
2. in den Fällen des Absatzes 1 oder 2 unter den in Nummer 1 genannten Voraussetzungen die Sicherstellung des Gegenstandes bewirkt, auf den sich die Straftat bezieht.

²Nach den Absätzen 1 bis 5 wird außerdem nicht bestraft, wer wegen Beteiligung an der Vortat strafbar ist.

(10) Das Gericht kann in den Fällen der Absätze 1 bis 5 die Strafe nach seinem Ermessen mildern (§ 49 Abs. 2) oder von Strafe nach diesen Vorschriften absehen, wenn der Täter durch die freiwillige Offenbarung seines Wissens wesentlich dazu beigetragen hat, dass die Tat über seinen eigenen Tatbeitrag hinaus oder eine in Absatz 1 genannte rechtswidrige Tat eines anderen aufgedeckt werden konnte.

Kundinnen und Kunden haben der Bank gegenüber ein Auskunftsrecht gemäß den datenschutzrechtlichen Bestimmungen (§ 34 Absatz 3 BDSG, Auskunft ist schriftlich zu erteilen) auch u. U. gegenüber sämtlichen Ermittlungsbehörden, auch BKA und LKA. Dieses Auskunftsrecht ist die Voraussetzung für die evtl. weitergehenden datenschutzrechtliche Schritte seitens

der Betroffenen. Dies umfasst ebenfalls das Auskunftsrecht des zuständigen Datenschutzbeauftragten.

Damit **Banken** rechtlich abgedeckt sind, lassen sie sich in aller Regel einen Revers hinsichtlich des Hinweises auf Speicherung und Weitergabe (Einverständniserklärung) unterschreiben in denen auch auf die AGB hingewiesen wird. Für die Verdachtsbearbeitung und Verdachtsübermittlung ist dies indessen nicht notwendig, siehe §§ 2 ff. GwG. Das GwG ist ein verdachtorientiertes Verfahren. Insofern ist das GwG die *lex specialis* zum BDSG. Zur Erfüllung ihrer Pflichten (Sorgfaltspflichten nach § 3 Abs. 1 Nr. 1 bis 3) kann die Bank auf Dritte zurückgreifen (§ 7 GwG). Die Verantwortung für die Erfüllung der Sorgfaltspflichten verbleibt indessen bei der Bank.

Ist an **Strafverfolgungsbehörden** bzw. an das **BKA** (§ 11 GwG, Zentralstelle für Verdachtsanzeigen) ein Verdacht gemeldet worden, verbleibt das Verfahren (technisch und organisatorisch) in deren Händen. Solange dort das Verfahren läuft, kann die Bank die Daten dieses Falles indessen gespeichert halten. Sie muss es sogar tun, sonst könnte sie zu diesem Fall keine weiteren verdächtigen Vorkommnisse melden.

Bei laufendem Verfahren kann die Ermittlungsbehörde jederzeit bei der anzeigenden Bank nachfragen. Allerdings wird die nachvollziehbare Übermittlung (Bank, Zweigstelle, Person) einer nur telefonischen Weitergabe vorzuziehen sein. Sonst besteht die Gefahr, dass hinterher niemand mehr weiß, wann, was und von wem weitergegeben wurde. Richtig deshalb § 11 Abs. 2 GwG: "Eine mündlich oder telefonisch gestellte Anzeige nach Abs. 1 ist schriftlich, fernschriftlich oder durch elektronische Datenübermittlung zu wiederholen".

Bestätigt sich der Verdacht als nicht hinreichend, hat die Bank den Vorgang zu löschen. Gleiches gilt bei Abschluss des Verfahrens durch Einstellung im Zwischenverfahren (§ 199 StPO) oder Hauptverfahren (§§ 153 ff. StPO) bzw. durch Urteil (§ 269 StPO). Die Bank hat nach § 11 Abs. 8 GwG einen Auskunftsanspruch (Verweis auf § 475 StPO, § 477 Abs. 3 StPO findet keine Anwendung). Bei den Ermittlungsbehörden bzw. dem BKA ist dort nach den allgemeinen Vorschriften zu handeln (z. B. INPOL, Verwahrvorschriften, BDSG). De lege ferenda sollte dies dahingehend geändert werden, dass die Anzeige erstattende Bank nach Erledigung automatisch vom Ausgang des Verfahrens benachrichtigt wird. Dazu bedarf es keiner Begründung, welche Entscheidung der Beendigung zugrunde liegt. Lediglich die Bank muss bei Erledigung des Verfahrens die Daten zu diesem Fall löschen. Die Speicherung ist dann nicht mehr zur Aufgabenerfüllung erforderlich. Sonst droht ein Konflikt mit dem BDSG, sofern solche Daten elektronisch gespeichert sind.

8.4 Handlungsempfehlungen

Es können zusammenfassend folgende sieben Handlungsempfehlungen abgeleitet werden.

Handlungsempfehlung Nr. 1: Das Hochleistungsportal zum Management von Geldwäscheverdachts-Anzeigen (HMG) soll unter Einsatz von modernen state-of-the-art Authentifizierungsmethoden und sicheren Datenzugriffs- und -verwendungstechniken ein integriertes verlässliches Identity- und Access-Management sicherstellen

Das HMG sollte in den großen Rahmen des Deutschland-Online Projekts "Einheitliche Kommunikationsinfrastruktur für den elektronischen Rechtsverkehr" (SAFE / DIM) eingepasst werden. Das SAFE Grobkonzept (siehe www.deutschland-online.de/DOL_Internet/broker.jsp?uMen=404209ab-8d40-9114-fb1-b1ac0c2f214a) zeigt den Weg dorthin (siehe Kap. 4.2.3). Wenn jede der beteiligten Parteien eine Trust-Domain im Sinne von SAFE in der für sie notwendigen Ausbaustufe darstellt, können die verschiedenen Nutzerverwaltungen besser aufeinander abgestimmt werden, der Umgang mit verschiedenen Sicherheitslevel wird leichter konfigurierbar.

Die Prozesskette Level-1 muss bzgl. Verschlüsselung, Signatur und Signatur-Infrastruktur angemessen überarbeitet und erweitert werden. Dazu sollen die Teilprozesse der Prozesskette nach ihrem Schutzbedarf ("normal", "hoch" oder "sehr hoch") klassifiziert werden, so dass jeder Teilprozess entsprechend seines Gefährdungspotentials mit entsprechenden Sicherheitsmaßnahmen ausgestattet werden kann. Das auf SAFE basierende Identity-Management der Prozesskette erfolgt zertifikatsbasiert und berücksichtigt die unterschiedlichen Sicherheitsstufen der Teilprozesse. Für besondere Sicherheitsansprüche, wie sie z. B. bei der Kommunikation über öffentliche Netze mit den FDL, dem BKA, den LKA und dem HMG gefordert sind, muss das HMG hochsichere VPN-Lösungen zur Verfügung stellen (siehe Kap. 8.3.3). Hier empfiehlt sich die Verwendung der BSI-Lösung SINA (BSI 2008c).

Die Handlungsempfehlung 1 adressiert die Ziele [GVA1], [GVA 6] und [GVA 9].

Handlungsempfehlung Nr. 2: Das HMG soll den unterschiedlichen Stakeholdern, die gesetzlich berechtigt und verpflichtet sind, ermöglichen, Zustandsänderungen allen Beteiligten sofort zu melden

Alle weiter verarbeitenden Parteien müssen allen berechtigten Parteien Zustandsänderungen in ihrem Zuständigkeitsbereich sicher kommunizieren ("Information-Push").

Das setzt einen empfangenden Webservice mit sicherer Authentifizierung für den Schreibvorgang bei allen Parteien voraus oder einen zentralen Informations-Webservice mit sicherer Authentifizierung, der von allen Parteien beschrieben werden kann oder die Informationen von den verteilten Informationsservern weiterleitet. Dies kann z. B. in Form eines geschlossenen Newsfeeds oder einer geschlossenen Mailingliste erfolgen.

Die Nachrichten der Zustandsänderungen können als "Trigger" in die Workflows der beteiligten Fachsysteme verwendet werden.

In diesem Kontext muss eine hohe bzw. bei laufenden Verfahren sehr hohe Informationssicherheit durchgängig gewährleistet sein. Da diese Handlungsempfehlung ausschließlich Kanal 2 (FDL mit hohem Aufkommen an GVA) betrifft (siehe Kap. 8.3.3), kann hier eine standardisierte VPN-Verbindung verwendet werden. Hierzu ist die Sichere Inter-Netzwerk Architektur (SINA) besonders gut geeignet (BSI 2008c).

Die Handlungsempfehlung 2 adressiert die Ziele [GVA 2], [GVA 6] und [GVA 9].

Handlungsempfehlung Nr. 3: Das HMG soll den unterschiedlichen Stakeholder, die gesetzlich berechtigt und verpflichtet sind, ermöglichen sich jederzeit über den Stand der Prozesskette vom Geldwäscheverdacht bis theoretisch zum gerichtlichen Ausgang zu informieren

Erstrebenswert ist, dass die Banken jederzeit den Bearbeitungsstand der Ermittlung beim BKA über das HMG abfragen können ("Information-Pull"). Hierzu ist ein HMG mit Tracking- und Trouble-Ticket-System Funktionalitäten erforderlich.

Für die Verwaltung der GVA setzen die Banken entsprechende Fallsysteme ein, in denen jederzeit der Bearbeitungsstand eingesehen werden kann. Für die Zukunft kann sich z. B. eine Großbank wie die Commerzbank AG durchaus vorstellen, über ein Identity- und Access-Management dem BKA partiell

Zugriff auf die Fälle zu erlauben, um so z. B. den Ermittlungsbehörden den Zugriff auf Umsatzzahlen zu erleichtern. Eine ähnliche innovative Lösung ist z. B. bei einer Prozesskette zu Meldepflichten bei geschlossenen Fonds durch die FDL an die BaFIN / Bundesbank z. T. realisiert.

Die Handlungsempfehlung 3 adressiert die Ziele [GVA 3], [GVA 6] und [GVA 9].

Handlungsempfehlung Nr. 4: Die Kommunikation zwischen Banken und den ÖV kann durch den Einsatz eines HMG qualitativ besser, schneller und sicherer erfolgen, indem das Fax als Referenzlösung abgelöst wird (Input Schnittstelle)

Faxlösungen bedeuten immer einen Medienbruch und beeinträchtigen die Effizienz einer Prozesskette negativ, da bei der Weiterverwertung der Faxsendung immer nur ein Bild und keine strukturierten Daten vorliegen. Die automatische Weiterverarbeitung z. B. durch OCR-Verfahren ist unflexibel, langsam und fehleranfällig. Hinzu kommen die Sicherheitsrisiken (siehe Kap. 8.1.3), die immer noch unterschätzt werden. Hierbei sei insbesondere auf die Möglichkeiten zum Abhören von Leitungen sowie die Fälschungsmöglichkeiten von Absendern und Unterschriften verwiesen.

Die Daten müssen im XML-Format zwischen Fachanwendungen und den Webservices ausgetauscht werden. Damit können über WS-Standards Vertraulichkeit, Integrität und Authentizität ermöglicht werden. Medienbrüche und die Mehrfacheingabe der Daten entfallen damit.

Wenn die Infrastruktur des EGVP eingesetzt werden soll, so müsste für die automatische Bedienung eine Implementierung der API für Fachanwendungen eingesetzt werden, um nicht über besondere Clients gehen zu müssen. (z. B. PC-WARE: OSCI[®] Add-In für Office, OSCI[®] Add-In für Notare, OSCI[®] Add-In für Applikationen).

Vor dem Hintergrund von Handlungsempfehlung Nr. 4 sei sich noch einmal der wirtschaftliche Impact der Prozesskette vor Augen geführt. Für die FDL ist nach Aussagen in Expertinnen- und Experteninterviews der Zeitaufwand für die GVA im IST beträchtlich: Er wird auf 15 Min. bis 4 Wochen Zeitaufwand pro GVA, bei einem ungefähren Durchschnitt von 0,5 bis 1,5 Tage Zeitaufwand pro GVA geschätzt.

Die Handlungsempfehlung 4 adressiert die Ziele [GVA 4], [GVA 8], [GVA 10] und [GVA 11].

Handlungsempfehlung Nr. 5: Das HMG soll das BKA und die zuständigen Strafverfolgungsbehörden befähigen durch abgestimmte XML-Schemata und maschinenverarbeitbare XML-Dokumente ausgetauscht über Webservices Daten weiterzuverarbeiten, dynamisch zu pflegen und auszuwerten (interne Schnittstelle)

In Bezug auf die interne Schnittstelle ist vor allem die Weiterverarbeitbarkeit der Daten erfolgskritisch. Z. B. die Kriminalstatistik, die die BKA FIU führt und als Jahresberichte publiziert (BKA 2008a), ist essentiell auf die Daten angewiesen.

Das HMG kann hier wertvolle Dienste leisten: Es stellt die Daten in real-time und maschinenverarbeitbar zur Pflege und Auswertung zur Verfügung. Durch das Austauschen dieser Daten und der Nutzung dieses HMG, ist eine schnelle und effektive Verarbeitung gewährleistet, auch und gerade im Zusammenspiel mit den dezentralen und föderalen LKA.

Die Handlungsempfehlung 5 adressiert die Ziele [GVA 5], [GVA 7] und [GVA 8].

Handlungsempfehlung Nr. 6: Das HMG muss revisionssicher sein

Die HMG muss per se die geschäftsmäßige Ordnung erfüllen.

Jede Partei muss empfangene Daten der Gegenstelle quittieren und jede Partei muss die Kommunikation selbst protokollieren. Da bei den FDL und der Verwaltung selbst alles revisionssicher behandelt werden muss, ist damit die gesamte Kette revisionssicher.

Die Revisionssicherheit kann u. a. durch ein geeignetes Archivierungssystem gewährleistet werden. Hierbei ist zu beachten, dass die vorgeschriebenen Aufbewahrungsfristen organisatorisch und technisch eingehalten werden können (siehe Kap. 8.3.3). Zur revisionssicheren Transformation von Dokumenten, deren Format (Datenträger oder Datenformat) veraltet ist, findet man Lösungsansätze in den Projekten ArchiSig und TransiDoc (TransiDoc 2007). Das dort beschriebene elektronische Transformationssiegel kann Probleme lösen, die sich aus zu erwartenden Veränderungen der zur Archivierung eingesetzten Hard- und Software sowie den verwendeten Datenformaten ergeben.

Die Handlungsempfehlung 6 adressiert das Ziel [GVA 13].

Handlungsempfehlung Nr. 7: Im Hinblick auf Change Management entscheidet die Akzeptanz und das Know-How der Stakeholder dass das HMG und seine Dienste nicht nur angeboten sondern auch genutzt wird

Die Lösung für das HMG sollte bereits in der Verwaltung eingesetzte Verfahren und offene Standards benutzen. Sie ermöglicht jeder Partei ihr eigenes Rollen- und Rechte-System zu betreiben und zu pflegen einschließlich der Verwaltung der Zugriffsrechte auf die eigenen Webservices. Das Datenmodell sollte zwischen Polizei und Compliance-Verantwortlichen der Banken regelmäßig diskutiert und evolutionär erweitert werden, falls sich dadurch inhaltliche Verbesserungen oder Effizienzsteigerungen erwarten lassen

Bei all dem bleibt klar: es können zwar Anreize für die Nutzung gesetzt werden. Die ausschließliche Nutzung der HMG für die GVA ist nur möglich, wenn der elektronische Workflow (B2G) und vice versa (G2B) verpflichtend gemacht wird. Nur dann lassen sich auch alle Potentiale bei den Stakeholdern heben.

Die Handlungsempfehlung 7 adressiert die Ziele [GVA 12] und [GVA 14].

8.5 Ansätze zur Gestaltung neuer Geschäfts- und Betreibermodelle

Die zuvor dargestellten Handlungsempfehlungen geben Hinweise, welche bei der Gestaltung zukünftiger Geschäfts- und Betreibermodelle für Prozessketten im Bereich der elektronische Verdachtsanzeige, grundsätzlich möglich sind.

Mittels des in Submodul E dargestellten Schemas können Betreibermodelle skizziert werden, welche sinnvoll in der Praxis genutzt werden können.

An dieser Stelle wird der Aufbau eines HMG zur Abwicklung der Prozessketten als eine praktikable und machbare Lösung dargestellt. Das Betreibermodell berücksichtigt dabei, dass der Schutzbedarf für Daten und für das benötigte Portal nach IT-Grundschutz "sehr hoch" ist. Es ist deshalb auch erforderlich, besondere Schutzmaßnahmen wie z. B. die SINA-Lösung des BSI zu implementieren.

Hinzu kommt, dass auf dem Portal Daten von **hoheitlichem Interesse** hinterlegt werden und der Datenschutz besondere Berücksichtigung finden muss.

Eine erste Einschätzung führt also zu dem Ergebnis, dass **als Betreiber nur Institutionen des Bundes (ggf. der Länder)** dafür geeignet sind, z. B. das BKA oder das Bundesverwaltungsamt.

9 Ausblick

Die vorangegangenen Ausführungen der Machbarkeitsstudie haben gezeigt, wie bedeutend die Gestaltung von organisationsübergreifenden Prozessketten sind.

Direkt an die Arbeit und die Ergebnisse der Studie schließen folgende drei Herausforderungen an.

1. Es ist die **Visualisierung von Prozessketten ("Prozesslandkarte")** und die **Zugänglichmachung des Wissens zu Prozessketten ("Prozessbibliothek")** erforderlich – für politische und wirtschaftliche Entscheidungsträgerinnen und Entscheidungsträgern, Anwenderinnen und Anwender, Kundinnen und Kunden sowie die interessierte Öffentlichkeit.
2. **Weitere Theoriebildung** ist notwendig, vor allem zum **Zusammenspiel der PRK auf Level-1** und zur **Umsetzung von PRK und deren Erfolgsfaktoren**. Es hat sich gezeigt, dass das Konzept der organisationsübergreifenden Prozessketten ein großes wirtschaftliches Potenzial, sowohl für Banken, Einrichtungen der öffentlichen Verwaltung und deren Kundinnen oder Kunden besitzen. Die branchenweite Umsetzung und barrierefreie Integration aller Partner wird jedoch noch einige Zeit in Anspruch nehmen. Nichtsdestotrotz können durch die Etablierung von Level-1 neue Möglichkeiten der Organisationsgestaltung erschlossen werden, welche allen Beteiligten eine Verbesserung im marktlichen Wettbewerb ermöglichen können.
3. Die **pilothafte Umsetzung von ausgewählten Verfahren, die als Blaupause für viele Verfahren geeignet sind (Level-1 und Generation G3)**. Z. B. müssen nach dem GwG die Banken bei Kundengeschäften, die mit der Einrichtung eines Kontos einhergehen (etwa Abschluss eines privaten Immobilienkredits; siehe Kap. 7 und 8) der Kundin oder des Kunden identifizieren – d. h. in der Praxis entweder durch das persönliche Erscheinen in der Bankfiliale oder die Beglaubigung durch das Postident-Verfahren, das für die Banken teuer und unzuverlässig ist. Verbandsmanagerin Ulrike Linde vom Bundesverband deutscher Banken (BdB) sagt: "Wenn wir den Prozess der Kontoeröffnung im Internet sicher abbilden können, dann wäre das die Blaupause für viele weitere Geschäftsprozesse." (heise c't vom 24.11.2008: 56)

In Bezug auf den zweiten Punkt, der über die Rahmensetzung dieser Studie hinaus geht, lautet die entscheidende Frage: **Wann und unter welchen Umständen sind Level-1 Prozessketten generell machbar, was sind die Erfolgsfaktoren und Lessons Learned bei der Umsetzung?**

Hypothesen für Erfolgsfaktoren sind:

- **Commitment der Partner für gemeinsame Leistungserstellung:**
Als eine grundlegende Voraussetzung zur Gestaltung einer Level-1 Prozesskette müssen sich alle beteiligten Partner auf die gemeinsamen Ziele einigen können sowie die notwendigen Voraussetzungen für die organisationsübergreifende Kooperation schaffen.
- **Professionelles Prozessmanagement:**
Ein funktionierendes Prozessmanagement innerhalb der beteiligten Organisationen ist eine weitere notwendige Voraussetzung für die erfolgreiche Umsetzung von Prozessketten. Studien und Untersuchungen des Fraunhofer IAO zeigen, dass sowohl auf Seite der Banken als auch bei öffentlichen Verwaltungen bezüglich des Reifegrades des Prozessmanagements noch ein erheblicher Optimierungsbedarf besteht.
- **Etablierung offener Schnittstellen (fachlich und IT):**
Um medienbruchfreie und automatisierte Prozesskette gestalten zu können, ist die Etablierung offener und standardisierter Schnittstellen, sowohl auf fachlicher als auch IT-bezogener Art, notwendig.
- **Klare Regelungen bezüglich Kompetenzen in der Prozesskette:**
Da sich Level-1 Prozessketten über mehrere rechtlich selbstständige Organisationen erstrecken, müssen zwischen diesen klare Regelungen und Kompetenzverteilungen für das Management der gesamten Prozesskette festgelegt werden, um eine Steuerung und Optimierung auch wirksam durchsetzen zu können.
- **Erfüllung rechtlichen Anforderungen:**
Da die beteiligten Partner einer Level-1 Prozesskette zum Teil unterschiedlichen gesetzlichen und regulatorischen Verpflichtungen unterliegen, müssen Level-1 Prozessketten diese unterschiedlichen Gegebenheiten berücksichtigen. Ein Möglichkeit dazu wäre die Gestaltung von Prozesskettenbezogenen AGB welche die rechtlichen Pflichten und Besonderheiten in der Form abdecken, dass alle beteiligte Partner ihren rechtlichen Verpflichtungen entsprechen können.

Darüber hinaus zeigt die Machbarkeitsstudie auch zahlreiche Ansätze für einen weitergehenden Forschungs- und praktischen Umsetzungsbedarf:

- **Forschungsbedarf zur Organisationsgestaltung:**
Im Bereich der Organisation zeigt sich noch ein großer Bedarf an der Erforschung und Erprobung von Ansätzen von verteilten Organisationsformen unter der Berücksichtigung der durchgängigen Prozessorientierung.
- **Prozessorientierung in der öffentlichen Verwaltung:**
Die Etablierung eines durchgängigen und professionellen Geschäftsprozessmanagements in der öffentlichen Verwaltung. Dabei sind Ansätze und Modelle zu entwickeln, welche auf die Besonderheiten der öffentlichen Verwaltung abzielen.
- **Steuerungskonzepte für organisationsübergreifende Prozesskettenmanagement:**
Eng mit den organisatorischen Bedarf ist es notwendig neue bzw. angepasste Managementansätze zu entwickeln, welche auf die organisationsübergreifende Planung, Steuerung und das Controlling von Prozessketten abzielen.
- **Notwendigkeit zur Definition tragfähiger Geschäfts- und Betreibermodelle für neue Prozessketten (Klasse I und III)**
die Machbarkeitsstudie bezüglich neuer Prozessketten zwischen Wirtschaft und Verwaltung hat gezeigt, dass aufgrund der Gestaltung von Prozessketten, auch neue Geschäfts- und Betreibermodelle ermöglicht werden. In diesem Bereich gibt es einen sehr großen Bedarf bei der Entwicklung tragfähiger und nachhaltiger Modelle und Konzepte, welche das Management von Prozessketten unterstützen können.
- **Kompetenzmanagement zwischen rechtlich selbstständigen Organisationen:**
Ein bedeutender Forschungsbedarf besteht auch bezüglich Konzepten und Methoden für ein Kompetenzmanagement, welches sich über mehrere, rechtlich selbstständig Organisationen erstrecken. Welche Befugnisse und Pflichten werden neu zu schaffenden Rollen (z. B. Process Owner einer Level-1 PRK) eingeräumt und wie werden diese in der Praxis realisiert.
- **Performance- und Qualitätsmanagement für Prozessketten Level-1:**
Entsprechendes gilt für die zukünftige Gestaltung von Managementansätzen für ein organisationsübergreifendes und integriertes Performance- und Qualitätsmanagement für Level-1 Prozessketten.
- **Erweiterung der Prozesskette zwischen Finanzdienstleister, öffentlicher Verwaltung und der Realwirtschaft**
Finanzströme sind in der gesamten Wirtschaft omnipräsent. Aus diesem

Grund ist es sinnvoll das Konzept der Level-1 Prozessketten nicht nur auf den FDL Sektor zu beschränken, sondern diese auch auf die anderen Wirtschaftsbereiche auszudehnen.

- **Ansätze zum Management der Komplexität der Prozessketten**
Mit der Integration zahlreicher Partner innerhalb einer Prozesskette besteht für die beteiligten Organisationen ebenfalls ein großer Handlungsdruck bezüglich der Beherrschung der damit verbundenen Komplexität bei der Steuerung und Abstimmung mit den Partnern. Aus diesem Grund sind entsprechende Methoden und Konzepte notwendig, um geeignete Lösungen adressatengerecht entwickeln zu können.
- **Bedarf für Sichere Prozessketten**
Entsprechendes gilt für den Bereich der IT-Sicherheit. Aufgrund zum Teil sehr hohen Sicherheitsanforderungen in den Prozessen zwischen Wirtschaft und der öffentlichen Verwaltung müssen auch hier entsprechende Standards und Verfahren (weiter-)entwickelt und etabliert werden.
- **Integration und Nutzung neuer Technologien (z. B. ePA etc.) im Rahmen neu zu gestaltender Prozessketten**
Ein wichtiger Aspekt im Rahmen der Weiterentwicklung von branchenübergreifenden Prozessketten besteht in der Integration neuer Technologien, welche beispielsweise in Kooperation zwischen Organisationen unterschiedlicher Branchen entwickelt werden, um einer möglichst umfassende Anforderungsabdeckung gewährleisten zu können und damit auch tendenziell schnell in der Praxis eingesetzt werden können. Dafür müssen entsprechende multidisziplinäre Konzepte und Vorgehensweisen entwickelt werden, um diese Entwicklung unterstützen zu können.
- **Föderierte Systeme**
Eine der größten Herausforderungen für die Entwicklung von Level-1 Prozessketten ist, und hier besteht auch noch großer Forschungsbedarf, eine standardisierte einheitliche IuK-Infrastruktur zu schaffen, die flexibel erweiterbar ist, die föderalen Strukturen der politischen und Verwaltungslandschaft widerspiegelt und in Richtung der Sicherheitsanforderungen skalierbar ist. Alle Partner (FDL und Behörden) müssen die Verantwortung über ihre IT behalten und diese unabhängig entwickeln können. Die Schaffung föderierter Infrastrukturen und die Nutzung internationaler Standards ist daher eine notwendige Bedingung, um die in der Studie beschriebenen Ziele zu erreichen. Projekte wie SAFE zeigen in die richtige Richtung, sind aber nur der Anfang. Föderiertes Identity- und Access-Management wird daher in den nächsten Jahren eine wesentliche Rolle spielen beim Aufbau sicherer und vertrauenswürdiger IuK-Infrastrukturen und Prozessketten. Nur wenn man es schafft, die sich ak-

tuell bildenden SOA-Inseln in den Banken und Behörden gefördert zu vernetzen, können die Ziele erreicht werden.

- **Elektronische Signaturen**

Auch die Einführung und angemessene Nutzung fortgeschrittener und qualifizierter elektronischer Signaturen muss eines der Ziele beim Aufbau von Level-1 Prozessketten sein. Chipkartenbasierte Anwendungen wie der ePA können hier zum Katalysator werden und sollten unbedingt in die Planungen einbezogen werden.

- **Technische und semantische Interoperabilität**

Neben der technischen Interoperabilität zwischen Anwendungen der Prozessketten wird zukünftig auch die semantische Interoperabilität nicht mehr zu vernachlässigen sein, gerade auch im Kontext pan-europäischer Prozessketten. Prozessketten-Projekte sollten daher auf Ergebnisse bestehender Projekte aus dem Kontext Deutschland-Online Standardisierung oder aus dem europäischen Kontext von IDABC zurückgreifen. Nicht an allen Stellen macht eine Standardisierung von Datenaustauschformaten Sinn. Oft ist auch die Harmonisierung von Datenaustauschformaten zwischen Prozessbausteinen ausreichend und wirtschaftlicher als ein langwieriger Standardisierungsprozess. Großer Forschungsbedarf besteht z. B. bei Definition von Semantik bewahrenden Abbildungen zwischen Informationsmodellen aus dem Bereich der XML-Modellierung ebenso wie aus dem Bereich der konzeptuellen Modellierung z. B. mit UML unter dem Einsatz semantischer Strukturen wie Taxonomien und Ontologien.

10 Referenzen

Bibliographie und Hyperlinks

Alemann, U. von 1995: Politikwissenschaftliche Methoden. Grundriss für Studium und Forschung, Westdeutscher Verlag, Opladen

Beauftragter der Bundesregierung für Informationstechnik,
www.cio.bund.de/cln_102/sid_9130FA044B6A5C2FA9750E368A73D56E/DE/Standards/SAGA/saga_node.html, Standards und Architekturen für E-Government (SAGA) und SAGA 4.0, aufgerufen am 10.12.2008

Brunzel, M. / Fröschle, N. / Kraft, R. / Mambrey, P. / Nentwig, L. / Steffens, P. / Stöwer, M. / Tschichholz, M. / Wehner, J. 2007: Eckpunktepapier zur inhaltlichen Vorbereitung des Umsetzungsplans 2008 / Workshop "Evaluation E-Government 2.0", nichtöffentliche Studie Fraunhofer eGovernment Zentrum für BMI, 146 S.

Brunzel, M. / Fröschle, N. / Kraft, R. / Nentwig, L. / Nordbrock, G. / Steffens, P. / Tschichholz, M. / Wehner, J. 2007: Aktuelle Trends im E-Government und Vorschläge zum Programm "E-Government 2.0", Studienkurzzusammenfassung Fraunhofer eGovernment Zentrum für BMI, 5 S.

Bullinger, H.-J. / Baumann, T. / Fröschle, N. / Mack, O. / Trunzer, T. / Waltert, J. 2002: Business Communities. Professionelles Beziehungsmanagement von Kunden, Mitarbeitern und B2B-Partnern im Internet, Galileo Press, Bonn

Bundesamt für Sicherheit in der Informationstechnik (BSI) (Hrsg.) 2005: Modul: Sicherer Internet-Auftritt im E-Government, 2002-2005, www.bsi.de/fachthem/egov/download/4_IntAuf.pdf, aus E-Government-Handbuch, www.e-government-handbuch.de, aufgerufen am 01.12.2008

Bundesamt für Sicherheit in der Informationstechnik (BSI) (Hrsg.) 2008a: BSI-Standard 100-1, 100-2, 100-3, www.bsi.bund.de/literat/bsi_standard/index.htm, aufgerufen am 28.11.2008

Bundesamt für Sicherheit in der Informationstechnik (BSI) (Hrsg.) 2008b:

IT-Grundschutz-Kataloge, www.bsi.de/gshb/index.htm und www.bsi.de/gshb/deutsch/baust/b03402.htm, aufgerufen am 28.11.2008

Bundesamt für Sicherheit in der Informationstechnik (BSI) (Hrsg.) 2008c: Sichere Inter-Netzwerk Architektur (SINA), www.bsi.de/fachthem/sina/index.htm, aufgerufen am 28.11.2008

Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) (Hrsg.) 2008: Melde- und Veröffentlichungsplattform – MVP, Benutzerhandbuch für die Meldeplattform, Benutzerhandbuch zur Zugangsverwaltung, www.bafin.de, aufgerufen 19.11.2008

Bundesfinanzministerium (BMF) (Hrsg.) 2008: Glossar. Geldwäsche, www.bundesfinanzministerium.de/nr_2352/DE/BMF_Startseite/Service/Glossar/G/001_Geldwaesche.html, aufgerufen am 11.11.2008

Bundeskriminalamt (BKA) (Hrsg.) 2008a: Jahresbericht 2007 Financial Intelligence Unit (FIU) für Deutschland, www.bka.de, aufgerufen am 01.10.2008

Bundeskriminalamt (BKA) (Hrsg.) 2008b: Verdachtsanzeige Workflow, Financial Intelligence Unit (FIU), www.bka.de/profil/zentralstellen/geldwaesche/neuverpflichtete/fiu4.html, aufgerufen am 01.10.2008

Bundesministerium des Innern (BMI) (Hrsg.) 2007a: Handlungsfeld Prozessketten im Programm E-Government 2.0. Kurzfassung, Version 2.0

Bundesministerium des Innern (BMI) (Hrsg.) 2007b: Leitfaden für Entwickler von Prozess- und Datenmodellen, Praxisorientiertes Vorgehen zur Modellierung von Prozessen und Daten in der Bundesverwaltung, Version 1.0, Publikation der KBSt, www.kbst.bund.de/modellierungsleitfaden, aufgerufen am 23.06.2008

Bundesministerium des Innern (BMI) (Hrsg.) 2007c: Umsetzungsplan 2007, E-Government 2.0 - Das Programm des Bundes

Bundesministerium des Innern (BMI) (Hrsg.) 2008a: Standards und Architekturen für E-Government-Anwendungen, Version 4.0, März 2008, www.kbst.bund.de/saga und http://gsb.download.bva.bund.de/KBSt/SAGA/SAGA_v4.0.pdf, aufgerufen 19.11.2008

Bundesministerium des Innern (BMI) (Hrsg.) 2008b: Umsetzungsplan 2008, Fortschrittsbericht zum Regierungsprogramm Zukunftsorientierte

Verwaltung durch Innovationen einschließlich Programm E-Government 2.0

Bundesministerium des Innern (BMI) (Hrsg.), E-Government-Forschung für Deutschland, Rede von Bundesminister Dr. Wolfgang Schäuble bei der Konferenz "Zukunft gestalten – E-Government-Forschung für Deutschland" am 17. Juli 2007 in Berlin, www.bmi.bund.de/cln_028/nn_122688/sid_C2BEF6417C3D710F37AC23C0956F4D20/nsc_true/Internet/Content/Nachrichten/Reden/2007/07/BM_E_Government_Forschung.html, aufgerufen am 10.12.2008

Bundesministerium des Innern (BMI) (Hrsg.), Migrationsleitfaden Version 3.0, April 2008

Bundesministerium für Wirtschaft und Technologie (BMWi) (Hrsg.) 2007: TransiDoc. Rechtssichere Transformation signierter Dokumente, 2004-2007, www.transidoc.de, aufgerufen am 28.11.2008

Bundesverwaltungsamt – Bundesstelle für Büroorganisation und Bürotechnik (BVA BBB) (Hrsg.) 2002: Sprachliche Gleichbehandlung von Frauen und Männern, BBB-Merkblatt M 19, 2. Auflage, www.bundesverwaltungsamt.de, aufgerufen am 13.03.2009

Clements, P. / Kazman, R. / Klein, M. 2001. Evaluating Software Architectures: Methods and Case Studies. Addison-Wesley Professional. Part of the SEI Series in Software Engineering series, Oktober 2001, ISBN-10: 0-201-70482-X, ISBN-13: 978-0-201-70482-2

Deutsche Bundesbank (Hrsg.) 2008: Bundesbank ExtraNet Dokumentation für Kunden, Version 2.4, www.bundesbank.de/extranet, aufgerufen am 19.11.2008

Deutsche Verwaltungsdienstverzeichnis (DVDV), www.dvdv.de und www.bit.bund.de/BIT/DE/Zentrale_Dienste/DVDV/node.html?_nnn=true, aufgerufen am 19.08.2008

Deutschland-Online (Hrsg.) 2007: SAFE Grobkonzept 1.0, Stand 31.12.2007, in IT-Umsetzung der Europäischen Dienstleistungsrichtlinie, Projektbericht, Stand: 24.09.2008, www.deutschland-online.de, aufgerufen am 27.11.2008

Deutschland-Online (Hrsg.) 2008a: IT-Umsetzung der Europäischen Dienstleistungsrichtlinie, Projektbericht, Stand: 24.09.2008,

www.deutschland-online.de, aufgerufen 27.11.2008

Deutschland-Online (Hrsg.) 2008b: S.A.F.E. (Secure Access to Federated e-Justice / e-Government) D.I.M. (Distributed Identity-Management), Dataport und BLK-AG "IT-Standards in der Justiz", www.justiz.de/ERV/Grob-und_Feinkonzept/index.php, aufgerufen am 19.11.2008

Deutschland-Online (Hrsg.), Secure Access to Federated E-Justice / E-Government (S.A.F.E.) - einheitliche Verfahren für den elektronischen Rechtsverkehr, www.deutschland-online.de/DOL_Internet/broker.jsp?uMen=404209ab-8d40-9114-fbf1-b1ac0c2f214a, aufgerufen am 01.12.2008

Deutschland-Online (Hrsg.), www.standardisierung.deutschland-online.de, aufgerufen am 10.12.2008

Doppler, K. / Lauterburg, C. 2002: Change Management. Den Unternehmenswandel gestalten, Campus Verlag, Frankfurt a. M., 10. Auflage

EGVP Elektronischen Gerichts- und Verwaltungspostfach, www.egvp.de, aufgerufen am 19.11.2008

Eisenberg, U. 2007: Fälle zum Schwerpunkt Strafrecht. Strafprozess, Kriminologie, Jugendstrafrecht, Strafvollzug, Verlag C. H. Beck, München, 8. Auflage

Engstler, M. / Makram, L. / Vocke, C. 2004: Industrialisierung der Finanzbranche, Whitepaper, Fraunhofer IAO, Stuttgart

Ernst, A. M. / Lankes, J. / Matthes, F. / Wittenburg, A. 2007: Software Cartography Models and methods for documenting, planning, and evaluating application landscapes; 2007-01-21, www.softwarekartographie.de, aufgerufen am 19.11.2008

FMC Consortium (Hrsg.) 2008: Fundamental Modeling Concepts (FMC), www.fmc-modeling.org, aufgerufen am 20.11.2008

Fraunhofer ISST (Hrsg.) 2008: Elektronische Fallakte (eFA), Spezifikation 1.2, www.fallakte.de, aufgerufen 19.11.2008

Fröschle, N. / Götz, A. / Klocke, I. 2007: eGOV-Rechner in der Landeshauptstadt Stuttgart, in: Zechner, A. (Hrsg.) 2007: Handbuch E-Government. Strategien, Lösungen und Wirtschaftlichkeit, IRB-Verlag,

Stuttgart, 253-261

Fröschle, N. / Gölz, A. 2007: Guideline eGOV-Rechner Version 0.9beta, Wirtschaftlichkeitsanalyse im eGovernment, www.egov-rechner.org, aufgerufen am 01.12.2008

Gabler (Hrsg.) 2000: Gablers Wirtschaftslexikon, Wiesbaden, Gabler Verlag, 15. vollständig überarbeitete und aktualisierte Auflage

heise c't 23 / 2001: Erfinden nach Plan. TRIZ-Methode hilft dem Aha-Effekt auf die Sprünge, 96-105

heise c't 25 / 2008: Ausweistechnik 4.0. Bundesdruckerei bietet ID-Management künftig als Dienstleistung an, 56

Initiative Finanzstandort Deutschland (IFD), www.finanzstandort.de, aufgerufen am 12.12.2008

Interoperable Delivery of European eGovernment Services to public Administrations, Businesses and Citizens (IDABC), European Commission Directorate-General for Informatics DIGIT / 01 - European eGovernment services (IDABC) (Hrsg.) 2004: EIF - European Interoperability Framework for Pan European eGovernment Services Version 1.0, <http://europa.eu.int/idabc>, aufgerufen am 20.11.2008

KBSt (Hrsg.), IT-Architekturkonzept für die Bundesverwaltung Version 1.0, Juli 2007

Knöpfel, A. / Gröne, B. / Tabeling, P. 2005: Fundamental Modelling Concepts Effective Communication of IT Systems, John Wiley & Sons Ltd, Hoboken, NJ

Koordinierungs- und Beratungsstelle der Bundesregierung für Informationstechnik in der Bundesverwaltung (KBSt) (Hrsg.) 2007, IT-Architekturkonzept für die Bundesverwaltung Version 1.0, Juli 2007

Kostka, C. / Mönch, A. 2002: Change Management. 7 Methoden für die Gestaltung von Veränderungsprozessen, Hanser, München, 2. Auflage

KPMG (Hrsg.) 2001: Meldepflichten, Aufsichtsrechtliche Meldungen nach Kreditwesengesetz, Bankenstatistik, Außenwirtschaftsgesetz, Wertpapierhandelsgesetz und Geldwäschegesetz, www.kpmg.de, aufgerufen am 10.09.2008

Krcmar, H. 2003: Informationsmanagement, Springer, Berlin / Heidelberg / New York / Hongkong / London / Mailand / Paris / Tokio, 3. Auflage

Kuhlisch, R. 2007: Realisierung komplexer Sicherheitsdienste unter Verwendung der Standards WS-Trust und SAML am Beispiel der elektronischen Fallakte, Diplomarbeit an der Fachhochschule für Technik und Wirtschaft Berlin

Kunz, G. 2003: Führen durch Zielvereinbarungen Im Change Management Mitarbeiter erfolgreich motivieren, C.H. Beck Wirtschaftsverlag, München

Kussmaul, A. 2006: Wirtschaftliche Internetkommunikation am Beispiel des E-Government, Dissertation, Universität der Künste Berlin, Logos Verlag, Berlin

Lankes, J. / Matthes, F. / Wittenburg, A. 2005: Softwarekartographie: Systematische Darstellung von Anwendungslandschaften. In: 7. Internationale Tagung Wirtschaftsinformatik 2005, Bamberg, www.softwarekartographie.de, aufgerufen am 19.11.2008

Lucke, J. v. 2008: Hochleistungsportale für die öffentliche Verwaltung. Habilitation, Deutsche Hochschule für Verwaltungswissenschaft Speyer, Eul-Verlag, Köln

Morrmann, J. / Hillesheimer, M. / Metzler, C. / Zahn, C. 2006: Wertschöpfungsmanagement in Banken, Bankakademie Verlag GmbH, Frankfurt a. M.

Nationaler Normenkontrollrat (NKR) (Hrsg.) 2008: Der Nationale Normenkontrollrat nimmt Stellung zum Bericht der Bundesregierung und bescheinigt ihr gute Fortschritte beim Bürokratieabbau www.normenkontrollrat.bund.de/nn_252070/Webs/NKR/Content/DE/Artikel/2008-12-10-presseerklaerung-nkr-nimmt-stellung-zum-bericht-der-bundesregierung.html, aufgerufen am 10.12.2008

OSCI-Leitstelle (Hrsg.) 2008: Online Services Computer Interface (OSCI), www.osci.de und www.osci.de, Navigationspunkte "XÖV-Koordination" > "XÖV-Projekte", aufgerufen am 19.11.2008

OSCI-Leitstelle (Hrsg.), Online Services Computer Interface (OSCI), www.osci.de oder www.osci.de, Navigationspunkte "XÖV-Koordination" > "XÖV-Projekte", aufgerufen am 19.11.2008

Porter, M. E., 2000: Wettbewerbsvorteile, Spitzenleistungen erreichen und

behaupten, Campus Verlag, Frankfurt a. M., 6. Auflage

Pracht, A. 2008: Zukunftschance Performance Contracting: Vermarktung industrieller Leistungen über Betreibermodelle, www.b2bnewsblog.com/2006/06/zukunftschance-performance-contracting.html, abgerufen am 14.01.2009

Praeg, C.-P. 2007: An Assessment Tool for Bank Industrialisation - Challenges and Opportunities for Business Process Management, in: Proceeding of 18th Australasian Conference of Information Systems (ACIS) 2007, Toowoomba, Queensland, Australien

Praeg, C.-P. 2008a: Facetten der Bankenindustrialisierung in: Spath, D. / Bauer, W. / Engstler, M. (Hrsg.) 2008: Innovationen und Konzepte für die Bank der Zukunft. Mit modernen Vertriebslösungen und optimierten Wertschöpfungsprozessen künftige Herausforderungen begegnen, Gabler, Wiesbaden

Praeg, C.-P. 2008b: Strukturmodelle industrialisierter Banken, Whitepaper, Stuttgart

Praeg, C.-P. 2008c: Der Industrialisierungs-Quick-Check, in: Spath, D. / Bauer, W. / Engstler, M. (Hrsg.) 2008: Innovationen und Konzepte für die Bank der Zukunft. Mit modernen Vertriebslösungen und optimierten Wertschöpfungsprozessen künftige Herausforderungen begegnen, Gabler, Wiesbaden

Ringwald, G. 1983: Der Datenabruf und das Bundesdatenschutzgesetz, JZ 1983, 291-297

Ringwald, G. 1984: INPOL und StA: zum Abrufrecht der Staatsanwaltschaften aus polizeilichen Datenspeichern, Schweitzer Verlag, München

Schmelzer, H. J. / Sesselmann, W. 2003: Geschäftsprozessmanagement in der Praxis, Kunden zufrieden stellen - Produktivität steigern - Wert erhöhen, München, Hanser Verlag

Schmidt, M. G. 1995: Wörterbuch zur Politik, Alfred Kröner Verlag, Stuttgart

Schnell, R. / Hill, P. / Esser, E. 1989: Methoden der empirischen Sozialforschung, Oldenbourg, München / Wien, 2. Auflage

Schulz, V.; Resch, A.; Uebornickel, F.; Brenner, W. (2008): Shared Service-Organisationen als Möglichkeit wertorientierter Steuerung des IT-

Bereichs; in Fröschle, H-P.; Zarnekow, R. (2008): Wertorientiertes IT-Servicemanagement, HMD Praxis der Wirtschaftsinformatik, Heft 264, dpunkt.verlag, Heidelberg 2008.

Schwarzer, B. 1994: Prozessorientiertes Informationsmanagement in multinationalen Unternehmen: eine empirische Untersuchung in der Pharmaindustrie, Dissertation, Universität Hohenheim

Spath, D. (Hrsg.) / Bauer, W. / Engstler, M / Praeg, C.-P. / Vocke, C. 2008: Marktstudie Bank & Zukunft 2008, IRB Verlag, Stuttgart

Spath, D. (Hrsg.) / Bauer, W. / Engstler, M / Praeg, C.-P. / Vocke, C. 2007: Marktstudie Bank & Zukunft 2007, IRB Verlag, Stuttgart

Spath, D. / Bauer, W. / Engstler, M. (Hrsg.) 2008: Innovationen und Konzepte für die Bank der Zukunft. Mit modernen Vertriebslösungen und optimierten Wertschöpfungsprozessen künftige Herausforderungen begegnen, Gabler, Wiesbaden

SPIEGEL ONLINE vom 13.11.2008, Merkel will Hedgefonds an die Leine nehmen. Issing-Plan für Weltfinanzgipfel, www.spiegel.de/wirtschaft/0,1518,590262,00.html, aufgerufen am 13.11.2008

Standard Anwendung Meldewesen Banken (SAMBA), www.logicacmg.com und www.logica.com/meldewesen+samba/350235831, aufgerufen am 19.11.2008

Standards und Architekturen für E-Government-Anwendungen Version 4.0, Bundesministerium des Innern, März 2008, www.kbst.bund.de/saga oder http://gsb.download.bva.bund.de/KBSt/SAGA/SAGA_v4.0.pdf (aufgerufen 19.11.2008)

Statistisches Bundesamt (Hrsg.) 2006: Einführung des Standardkosten-Modells, Methodenhandbuch der Bundesregierung, Version 1.0

Statistisches Bundesamt (Hrsg.) 2008: Standardkosten-Modell Nutzerdatenbank Version 1.3.12 Wirtschaft mit Stand vom 20. Oktober 2008, https://circa.bund.de/Members/irc/bund/skm_oeffentlichkeit/library?!=/datenbank&vm=detailed&sb=Title, aufgerufen am 18.11.2008

Statistisches Bundesamt (Hrsg.) 2008: Verordnung (EG) Nr.1893 / 2006 des Europäischen Parlaments und des Rates vom 20. Dezember 2006 zur

Aufstellung der statistischen Systematik der Wirtschaftszweige NACE (Nomenclature général des activités économiques dans les Communautés européennes) Revision 2 und zur Änderung der Verordnung (EWG) Nr. 3037 / 90 des Rates sowie einiger Verordnungen der EG über bestimmte Bereiche der Statistik,

www.destatis.de/jetspeed/portal/cms/Sites/destatis/SharedContent/Oeffentlich/AZ/ZD/Rechtsgrundlagen/Statistikbereiche/AllgemeineBestimmungen/035a_VONACE_Rev2.property=file.pdf,
aufgerufen am 10.12.2008

Statistisches Bundesamt (Hrsg.), Die Methode. Was ist das Standardkosten-Modell - SKM?,

www.destatis.de/jetspeed/portal/cms/Sites/destatis/Internet/DE/Content/Projekte/SKM/Methode,templateId=renderPrint.psm, aufgerufen am
12.12.2008

Technische Universität München Chair for Informatics 19 (sebis) (Hrsg.) 2005: Enterprise Architecture Management Tool Survey 2005,
<http://www.matthes.in.tum.de>, aufgerufen am 19.11.2008

WiBe (Hrsg.) 2008: Das WiBe Konzept. Wirtschaftlichkeitsbetrachtung von (IT-)Projekten, www.wibe.de/html/konzept-uberblick.html, aufgerufen am
01.12.2008

Juristischer Apparat

BDSG: Bundesdatenschutzgesetz in der Fassung der Bekanntmachung vom 14. Januar 2003 (BGBl. I S. 66), zuletzt geändert durch Artikel 1 des Gesetzes vom 22. August 2006 (BGBl. I S. 1970),
http://bundesrecht.juris.de/bdsq_1990, aufgerufen am 30.11.2008

BeurkG: Beurkundungsgesetz vom 28. August 1969 (BGBl. I S. 1513), zuletzt geändert durch Artikel 5 des Gesetzes vom 12. Dezember 2007 (BGBl. I S. 2840), <http://bundesrecht.juris.de/beurkg>, aufgerufen am 30.11.2008

BGB: Bürgerliches Gesetzbuch in der Fassung der Bekanntmachung vom 2. Januar 2002 (BGBl. I S. 42, 2909; 2003 I S. 738), zuletzt geändert durch Artikel 7 des Gesetzes vom 30. Oktober 2008 (BGBl. I S. 2122),
<http://bundesrecht.juris.de/bgb>, aufgerufen am 30.11.2008

GBO: Grundbuchordnung in der Fassung der Bekanntmachung vom 26. Mai 1994 (BGBl. I S. 1114), zuletzt geändert durch Artikel 78 Abs. 7 des Gesetzes vom 23. November 2007 (BGBl. I S. 2614 mWv 30.11.2007),
<http://bundesrecht.juris.de/gbo>, aufgerufen am 30.11.2008

GBV: Grundbuchverordnung in der Fassung der Bekanntmachung vom 24. Januar 1995 (BGBl. I S. 114), zuletzt geändert durch Artikel 78 Abs. 8 des Gesetzes vom 23. November 2007 (BGBl. I S. 2614 mWv 30.11.2007)
Verordnung zur Durchführung der Grundbuchordnung (Grundbuchverordnung - GBV), <http://bundesrecht.juris.de/gbvfg>, aufgerufen am 30.11.2008

GwG: Geldwäschegesetz vom 13. August 2008 (BGBl. I S. 1690), Gesetz über das Aufspüren von Gewinnen aus schweren Straftaten (Geldwäschegesetz - GwG). Das Gesetz wurde als Artikel 2 vom Bundestag mit Zustimmung des Bundesrates beschlossen. Es ist gemäß Art. 11 Satz 1 dieses Gesetzes am 21.08.2008 in Kraft getreten,
http://bundesrecht.juris.de/gwg_2008, aufgerufen am 30.11.2008

HGB: Handelsgesetzbuch in der im Bundesgesetzblatt Teil III, Gliederungsnummer 4100-1, veröffentlichten bereinigten Fassung, zuletzt geändert durch Artikel 3 des Gesetzes vom 23. Oktober 2008 (BGBl. I S. 2026),
<http://bundesrecht.juris.de/hgb>, aufgerufen am 30.11.2008

InsO: Insolvenzordnung vom 5. Oktober 1994 (BGBl. I S. 2866), zuletzt geändert durch Artikel 9 des Gesetzes vom 23. Oktober 2008 (BGBl. I S. 2026)
Insolvenzordnung (InsO), <http://bundesrecht.juris.de/ins0>, aufgerufen am 30.11.2008

KWG: Kreditwesengesetz in der Fassung der Bekanntmachung vom 9. September 1998 (BGBl. I S. 2776), zuletzt geändert durch Artikel 24 des Gesetzes vom 23. Oktober 2008 (BGBl. I S. 2026) Gesetz über das Kreditwesen (Kreditwesengesetz - KWG), <http://bundesrecht.juris.de/kredwg>, aufgerufen am 30.11.2008

LDSG: Datenschutzgesetze der Bundesländer,
www.jusline.de/Datenschutzgesetze_aller_Bundeslaender.html

SigG: Signaturgesetz vom 16. Mai 2001 (BGBl. I S. 876), zuletzt geändert durch Artikel 4 des Gesetzes vom 26. Februar 2007 (BGBl. I S. 179) Gesetz über Rahmenbedingungen für elektronische Signaturen, http://bundesrecht.juris.de/sigg_2001, aufgerufen am 30.11.2008

SigV: Signaturverordnung vom 16. November 2001 (BGBl. I S. 3074), zuletzt geändert durch Artikel 9 Abs. 18 des Gesetzes vom 23. November 2007 (BGBl. I S. 2631) Verordnung zur elektronischen Signatur (Signaturverordnung - SigV), http://bundesrecht.juris.de/sigv_2001, aufgerufen am 30.11.2008

StGB: Strafgesetzbuch in der Fassung der Bekanntmachung vom 13. November 1998 (BGBl. I S. 3322), zuletzt geändert durch Artikel 1 des Gesetzes vom 31. Oktober 2008 (BGBl. I S. 2149), <http://bundesrecht.juris.de/stgb>, aufgerufen am 30.11.2008

StPO: Strafprozeßordnung in der Fassung der Bekanntmachung vom 7. April 1987 (BGBl. I S. 1074, 1319), zuletzt geändert durch Artikel 2 des Gesetzes vom 31. Oktober 2008 (BGBl. I S. 2149) <http://bundesrecht.juris.de/stpo>, aufgerufen am 30.11.2008

ZPO: Zivilprozessordnung in der Fassung der Bekanntmachung vom 5. Dezember 2005 (BGBl. I S. 3202; 2006 I S. 431; 2007 I S. 1781), zuletzt geändert durch Artikel 1 des Gesetzes vom 30. Oktober 2008 (BGBl. I S. 2122), <http://bundesrecht.juris.de/zpo>, aufgerufen am 30.11.2008

11 Glossar

Bank. Auch Geschäftsbank und Kreditinstitut. Ein Wirtschaftsunternehmen, welches Bankgeschäfte betreibt und in der Bundesrepublik dem Gesetz über das Kreditwesen (KWG; Kreditwesengesetz) und der Überwachung durch das Bundesaufsichtsamt für das Kreditwesen unterliegt. Bankgeschäfte gemäß §1 KWG sind: Entgegennahme von Sicht-, Termin- (Termingeld) und Spareinlagen, Gewährung von Krediten, Abwicklung des Zahlungsverkehrs, Kauf, Verkauf, Verwahrung und Emission von Wertpapieren, Devisengeschäfte etc. Neben dieser Finanzmittlerfunktion bestehen weitere Hauptaufgaben der Banken darin, die Wirtschaft mit Zahlungsmitteln zu versorgen und den baren sowie den unbaren Zahlungsverkehr abzuwickeln. In Deutschland sind nach der Definition des §1 des Gesetzes über das Kreditwesen diejenigen Unternehmen Kreditinstitute, die bestimmte Bankgeschäfte betreiben (Einlagen-, Kredit-, Diskont-, Effekten-, Depot-, Investment- Garantie- und Girogeschäfte), sofern der Umfang dieser Aktivitäten einen in kaufmännischer Weise eingerichteten Geschäftsbetrieb erfordert. Der Begriff Bank oder Bankbetrieb wird synonym zu dem im Kreditwesengesetz (KWG) definierten Begriff Kreditinstitut verwendet. Häufig wird Bank eher in einem ökonomischen, Kreditinstitut hingegen in einem juristischen Kontext gebraucht. (Quelle: Bundesbank)
siehe auch Finanzdienstleister

Bankenindustrialisierung. Industrialisierung beschreibt die Übertragung von Methoden und Werkzeugen aus dem industriellen Sektor auf Dienstleistungsunternehmen. Im Innovationsforum "Bank & Zukunft" wurde unter Moderation von Fraunhofer IAO ein weit gefasstes Verständnis der Industrialisierung entwickelt. Demnach kann unter Industrialisierung die Optimierung der gesamten Wertschöpfungskette verstanden werden. Mit einer Optimierung geht auch die Möglichkeit des Aufbrechens und der Neuformulierung der Wertschöpfungskette einher.

Basel II. Basel II als die neue Eigenkapitalvorschrift des Basler Ausschusses verfolgt das Ziel, die Stabilität des internationalen Finanzsystems zu erhöhen. Um dies zu erreichen, gliedert sich die Baseler Rahmenvereinbarung in drei Säulen. Säule 1 beinhaltet die Mindestkapitalanforderungen, die eine Eigenkapitalunterlegung für Kreditrisiken, Marktrisiken und operationelle Risiken beinhalten. Auf Säule 2 stützt sich der bankaufsichtliche Überprüfungsprozess, welcher die quantitativen Mindestkapitalanforderungen der Säule 1 um ein qualitatives Element ergänzt. Schließlich besteht Säule 3 aus

der Marktdisziplin, d. h. Erweiterung der Offenlegungspflichten der Institute gegenüber der Bankaufsicht. Die Vorschriften wurden mittlerweile durch die Solvabilitätsverordnung (SolvV) für die erste und dritte Säule sowie durch die Mindestanforderungen an das Risikomanagement (MaRisk) für die zweite Säule in deutsches Recht übernommen.

siehe auch MaRisk

Betreibermodell. Ein Betreibermodell ist ein Geschäftskonzept für die Bereitstellung von Gütern und Dienstleistungen, bei dem diese nicht mehr an Kundinnen oder Kunden verkauft, sondern gegen ein leistungsabhängiges Entgelt zur Nutzung angeboten werden. Betreibermodelle können somit für die Bereitstellung von physischen Produkten und / oder immateriellen Dienstleistungen gestaltet und etabliert werden. Betreibermodelle können gemäß der folgenden Kriterien klassifiziert, beschrieben und gestaltet werden: Leistungsfokus, Organisationsform, Koordinationsform, Kundenfokus, Gegenstand, Leistungsverrechnung, Preismodell, Absatzmarkt, Kontrahierungsform, Center-Konzept, Mitarbeiterinnen oder Mitarbeiter und Recht.

Compliance. Unter dem Begriff "Corporate Compliance" wird die Gesamtheit der Maßnahmen umschrieben, die das rechtmäßige Verhalten eines Unternehmens, der Leitungs- und Aufsichtsorgane und seiner Mitarbeiter sicherstellen soll. Leitungs- und Aufsichtsorgane haben eine sorgfältige und rechtskonforme Organisation des Unternehmens zu gewährleisten. Corporate Compliance-Maßnahmen werden daher als zentraler Bestandteil der gesetzlichen Verpflichtung angesehen.

Datenschutz. Datenschutz soll den Einzelnen davor schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird. Mit Datenschutz wird daher der Schutz personenbezogener Daten vor etwaigem Missbrauch durch Dritte bezeichnet (nicht zu verwechseln mit Datensicherheit). Für den Begriff Datenschutz existieren zwei englische Übersetzungen: Dabei bezeichnet "Data Protection" den Datenschutz als Rechtsbegriff. "Privacy" zielt dagegen auf die gesellschaftliche Lebensweise ab (Schutz der Privatsphäre) und wird überwiegend im amerikanischen Sprachumfeld genutzt, mittlerweile aber auch im EU-Raum vermehrt benutzt. (Quelle: BSI)

E-Government. Fachbegriff für elektronisches Regieren und Verwalten. **Government to Citizen (G2C)** beschreibt dabei Geschäftsprozesse zwischen Verwaltungsstellen und Bürgerinnen und Bürgern (in der Rolle einer Kundin oder eines Kunden) unter Einsatz von Informations- und Kommunikationstechnologien. **Government to Government (G2G)** beschreibt Geschäftsprozesse zwischen öffentlichen Verwaltungsstellen unter Einsatz von Informations- und Kommunikationstechnologien. **Government to Business**

(G2B) beschreibt Geschäftsprozesse zwischen privaten Unternehmen und Behörden unter Einsatz von Informations- und Kommunikationstechnologien.

Elektronische Signatur. Die elektronische Signatur beschreibt ein asymmetrisches Verschlüsselungsverfahren zur Gewährleistung der Authentizität und Integrität elektronischer Daten und zur Überprüfung der Identität der Benutzerin oder des Benutzers. Sie ist praktisch mit einer handschriftlichen Unterschrift oder der Möglichkeit, sich eindeutig gegen Vorlage einer Unterschrift auszuweisen, zu vergleichen. Die Rechtswirksamkeit der elektronischen Signaturen wird in Deutschland durch das Signaturgesetz (SigG) geregelt. Hiernach gibt es drei Arten die (allgemeine) elektronische Signatur, die fortgeschrittene elektronische Signatur und die qualifizierte elektronische Signatur. Hierbei hat jede Signatur eine bestimmte Qualitätsstufe. Je höherwertiger die Signatur, desto größer ist ihre Bedeutung für den Rechtsverkehr und desto größer ist ihre Funktionalität.

Finanzdienstleister (FDL). Finanzdienstleister umfassen alle Unternehmen welche Finanzdienstleistungen i. S. d. KWG für andere gewerbsmäßig oder in einem Umfang erbringt, der einen in kaufmännischer Weise eingerichteten Geschäftsbetrieb erfordert. Kapitalbeteiligungs- und -anlagegesellschaften zählen bankaufsichtsrechtlich zu den Kreditinstituten. Ebenso zählen Versicherungsunternehmen dazu.
siehe auch Bank

Genossenschaftsbank. Geld- und Kreditinstitut in der Rechtsform der eingetragenen Genossenschaft (e.G.). Die Kreditgenossenschaft ist eine Vereinigung von so genannten Genossen, die ein oder mehrere, auf feste Beträge lautende Geschäftsguthaben erworben haben, die dem Geschäftsergebnis entsprechend verzinst werden. Genossenschaftsbanken sind die Volksbanken und die Raiffeisenbanken. (Quelle: Bundesbank)
siehe auch Bank und Finanzdienstleister

Grundwerte der IT-Sicherheit. Der IT-Grundschutz betrachtet die drei Grundwerte der IT-Sicherheit: Vertraulichkeit, Verfügbarkeit und Integrität. Allen Anwenderinnen und Anwendern steht es natürlich frei, bei der Schutzbedarfsfeststellung weitere Grundwerte zu betrachten, wenn dies in seinem individuellen Anwendungsfall hilfreich ist. Weitere generische Oberbegriffe der IT-Sicherheit sind zum Beispiel: Authentizität, Verbindlichkeit, Zuverlässigkeit, Nichtabstreitbarkeit (Quelle: BSI)

Identity Provider (IDP). Ein Identity-Provider ist eine Software, welche die Benutzerin oder den Benutzer authentifizieren kann und einen Service-Provider (SP) mit Informationen zum Benutzer versorgt (Benutzerattribute). Der IDP steht bei der Heimateinrichtung und authentifiziert die Benutzerin

oder den Benutzer mit Hilfe der vorhandenen Benutzerverwaltung (engl. "Identity Management") der Heimateinrichtung. (Quelle: Deutsches Forschungsnetz)

Informationspflicht. Informationspflichten sind auf Grund von Gesetz, Rechtsverordnung, Satzung oder Verwaltungsvorschrift bestehende Verpflichtungen, Daten und sonstige Informationen für Behörden oder Dritte zu beschaffen, verfügbar zu halten oder zu übermitteln. Beispiele: Erklärungen und Meldungen gegenüber Finanzbehörden wie Lohnsteueranmeldung oder Umsatzsteuervoranmeldung, Bilanzierungspflichten von Unternehmen, Handelsregister- oder Grundbucheintragungen, Anträge auf Gewährung von Sozialleistungen oder Subventionen etc. (Quelle: Normenkontrollrat)

ISO 27001 (Zertifizierung nach ISO 27001 auf der Basis von IT- Grundschutz). Um die erfolgreiche Umsetzung von IT-Grundschutz nach außen transparent machen zu können, hat das BSI ein Zertifizierungsschema für Informationssicherheit entwickelt. Dieses Schema berücksichtigt die Anforderungen an Managementsysteme für die Informationssicherheit aus ISO / IEC 27001. Das ISO 27001-Zertifikat auf der Basis von IT-Grundschutz oder auch ein Auditor-Testat bietet Unternehmen und Behörden die Möglichkeit, ihre Bemühungen um Informationssicherheit transparent zu machen. Dies kann sowohl gegenüber Kundinnen und Kunden als auch gegenüber Geschäftspartnern als Qualitätsmerkmal dienen und somit zu einem Wettbewerbsvorteil führen. Grundlage für die Vergabe eines ISO 27001-Zertifikats auf der Basis von IT-Grundschutz ist die Durchführung eines Audits durch einen externen, beim BSI zertifizierten Auditor. Das Ergebnis des Audits ist ein Auditbericht, der der Zertifizierungsstelle vorgelegt wird, die über die Vergabe des ISO 27001-Zertifikats auf der Basis von IT-Grundschutz entscheidet. Kriterienwerke des Verfahrens sind neben der Norm ISO 27001 die IT-Grundschutz-Vorgehensweise und die IT-Grundschutz-Kataloge des BSI. (Quelle: BSI)

Kreditbanken. Im Gegensatz zu den Spezialbanken Institute, die alle Geschäfte einer Bank betreiben, insbesondere das Kredit- und das Wertpapiergeschäft. In Deutschland sind die meisten Banken als Universalbanken tätig, weshalb man auch von einem Universalbankensystem spricht. Demgegenüber haben einige Länder Trennbankensysteme. Dort ist es den Banken verboten, gleichzeitig das Kredit- und das Wertpapiergeschäft zu betreiben. Vorteile des Universalbankensystems sind neben der Versorgung der Kundinnen und Kunden aus einer Hand, die relativ geringe Störanfälligkeit der Banken, da eine breitere Streuung von Risiken möglich ist. (Quelle: Bundesbank)

siehe auch Bank, Finanzdienstleister

MaRisk. Die Überarbeitung der Eigenkapitalanforderungen für Kreditinstitute durch die Umsetzung der qualitativen Anforderungen der Rahmenvereinbarung des Baseler Ausschusses für Bankenaufsicht (*siehe Basel II*) verlangt in der so genannten Säule 2 von Basel II die Einführung eines Internal Capital Adequacy Assessment Process (ICAAP). Dieser bankinterne Prozess muss Verfahren zur Identifizierung, Messung, Steuerung und zum Reporting von Risiken im Kreditinstitut enthalten und soll zum Geschäftsvolumen des jeweiligen Instituts proportional sein. Dieser Prozess ist in Deutschland durch die nationale Gesetzgebung in den "Mindestanforderungen an das Risikomanagement" (MaRisk) verankert. Die Institute der deutschen Kreditwirtschaft hatten ihr bestehendes internes Risikomanagement spätestens bis zum 1. Januar 2008 an die MaRisk anzupassen. (Quelle: Bundesbank) *siehe auch Basel II*

PRK-Bauplan. Die Prozessketten Planung ist eine in der Machbarkeitsstudie entwickelte wissenschaftliche und praktische Methode, um eine Skizze für die Umsetzung von Prozessketten zwischen Wirtschaft und Verwaltung zu erstellen. Dazu werden auf Basis der Ergebnisse des Einsatzes von PRK-Screening und PRK-Scoping und mittels Anwendung der Module A-D u. a. strategische und operative Handlungsempfehlungen abgeleitet.

PRK-Scoping. Das Prozessketten Scoping ist eine in der Machbarkeitsstudie entwickelte wissenschaftliche und praktische Methode, um zu erreichende Ziele von Prozessketten zu planen – wirtschaftlich / prozessual / organisatorisch, IT-architektonisch, sicherheitstechnisch und juristisch.

PRK-Screening. Das Prozessketten Screening ist eine in der Machbarkeitsstudie entwickelte wissenschaftliche und praktische Methode, um Prozessketten in Bezug auf die wichtigsten Merkmale und deren Merkmalsausprägungen zu "screenen", d. h. zu durchleuchten. Die Methode lässt sich je nach Einsatzzweck auf unterschiedliche Analyseebenen (z. B. vergleichende Analyse von Prozessketten bzw. Fallstudie etc.) anpassen.

Prozess. Ein Prozess ist die zielgerichtete Abfolge von Tätigkeiten, die zur Schaffung eines Produktes oder Dienstleistung dienen und in einem direkten Zusammenhang stehen. Prozesse transformieren Inputfaktoren zu einem Outputfaktor.

Prozessbibliothek. Im allgemeinen dient eine Prozessbibliothek dazu, qualitätsgesicherte Standards u. a. in Form von Prozessmodellen und Musterlösungen für die Geschäftsprozessmodellierung und deren IT-Unterstützung (Funktionen, Services, Betriebsplattformen etc.) zur Verfügung zu stellen. In Bezug auf Prozessketten können in Theorie und Praxis unterstützende Ansätze eingesetzt werden. Das Ergebnis des PRK-Screenings bildet eine Pro-

zessbibliothek.

siehe auch *PRK-Screening, PRK-Scoping, PRK-Bauplan*

Prozesskette. Ist eine logische Verknüpfung von Prozessen gesehen werden. Prozessketten stellen damit eine Kette zusammenhängender Prozesse dar, die zur Erstellung einer Dienstleistung oder Produkt (Wertschöpfungsorientierung) sowie zu einem gemeinsamen (Geschäfts-)Prozessziel führen sollen.

Prozesskette Generation. Prozesskette der **Generation 1 (G1)** meint die papiergebundene Interaktion, durch reale Transaktionen wie Gelber Post, Kurierdiensten etc. unterstützt. **Generation 2 (G2)** zielt ab auf (IT-) anwendungsorientierte Interaktion, d. h. dass Datenströme in unterschiedlichen Formaten, auf unterschiedlichen Medien, über unterschiedliche Netze bzw. Kanäle etc. im Hin- und Rückkanal zwischen Wirtschaft und öffentlicher Verwaltung laufen. **Generation 3 (G3)** ist infrastrukturorientiert. Auf einer (Web-)Plattform mit an den realen Geschäftsprozessen orientierten elektronischen Diensten und digitalen Inhalten können die betroffenen Stakeholder ihre ganzheitlichen Prozesse managen. Die Plattform bietet zugeschnittene Lese- und Schreibrechte für alle Mitglieder der Prozesskette (rollenbasierter 24 / 7 Pull-Service auf Anfrage). Die Plattform ist im Hol- und Bringschuld Management intelligent konfiguriert und gibt Benachrichtigung an dedizierte Adressaten bei Systemzustandsänderungen (orts-, zeit- und situationsbedingter Information-Push).

Prozesskette Klasse. Unter Prozessketten der **Klasse I** fallen Prozessketten, die einen neuen Wertschöpfungscharakter besitzen und für die Realisierung entsprechend neue Betreibermodelle, sowohl von Seite der Banken als auch der öffentlichen Verwaltung, voraussetzen. Diese Prozesskettenklasse bietet sehr großen Gestaltungsspielraum für alle beteiligten Akteure. Diese beinhalten Geschäftsprozesse eines FDL, die neue Geschäftsmodelle abbilden; also Geschäftsprozesse, die nicht mit dem originären Leistungsspektrum eines FDL in Verbindung gebracht werden, aber für den FDL einen hohen Wettbewerbsvorteil und / oder wertschöpfenden Nutzen darstellen. Prozessketten der **Klasse II** sind solche, die aufgrund regulatorischer Pflichten von Seite der Banken zu erfüllen sind. Für diese Prozessketten gibt es wenig bis keinen Spielraum, da sie aufgrund gesetzlicher Regelungen etabliert sein müssen. Lediglich die Art und Weise der Erfüllung dieser Pflichten gibt den Beteiligten einen gewissen Gestaltungsspielraum. Diese produzieren Leistungen, die in erster Linie dazu dienen, die regulatorischen Pflichten eines FDL zu erfüllen; der wertschöpfende Anteil in diesen Prozessketten ist gering. Prozessketten der **Klasse III** werden erst durch den Einsatz und Nutzung neuer Technologien überhaupt ermöglicht. Technologien sind Enabler zur Gestaltung dieser Art von Prozesskettenklasse. Daher ist auch hier ein

begrenzter Gestaltungsspielraum für alle Beteiligten gegeben, da die Technologien sowohl von Seite der Banken als auch von Seiten der öffentlichen Verwaltung für den Einsatz und Nutzung freigegeben und bestimmte Voraussetzungen dafür erfüllt sein müssen. Diese beinhalten wettbewerbsentscheidende und im hohen Maße ressourcenrelevante Geschäftsprozesse eines FDL, die, z. B. durch neue behördliche Infrastrukturen (hier als Beispiel ePA), einen Wettbewerbsvorteil und / oder Wertzuwachs (im Sinne der Wertschöpfung) erzielen können.

Prozesskette Level (Systemebene). **Level-3 (L-3)** bedeutet, dass es "punktuelle Informationsverpflichtung und Verfahren mit einer Behörde gibt. Auf einer Wertschöpfungsstufe innerhalb eines Unternehmens erforderlicher punktueller Datenaustausch mit einer Behörde". **Level-2 (L-2)** fokussiert auf eine "unternehmensweite Prozessintegration: Über mehrere Wertschöpfungsstufen eines Unternehmens laufende Prozesskette mit vielfältigen punktuellen Informationspflichten und Verfahren mit Behörden". **Level-1 (L-1)** bedeutet "branchenweite Prozessintegration: Über mehrere Wertschöpfungsstufen einer Branche laufende Prozesskette mit vielfältigen punktuellen Informationspflichten und Verfahren mit Behörden". (Quelle: BMI)

Prozesskette Level (Operationalisierung). Als **Level-3** kann bezeichnet werden, wenn ein Akteur auf Seite der Wirtschaft mit einem Prozessketten-Verfahren mit einem Akteur auf Seite der öffentlichen Verwaltung verbunden ist ("1 : 1 : 1"). Als **Level-2** kann bezeichnet werden, wenn ein oder mehrere Akteure auf Seite der Wirtschaft mit einem oder mehreren Prozessketten-Verfahren mit einem oder mehreren Akteuren auf Seite der öffentlichen Verwaltung verbunden sind; dabei ist aber mindestens eine der genannten Anzahl von Akteuren oder Verfahren gleich 1, d. h. es kann noch nicht von einer branchenweiten oder branchenübergreifenden Prozesskette gesprochen werden ("2-x) : (2-x) : (2-x)"). Als **Level-1** kann bezeichnet werden, wenn mehrere Akteure auf Seite der Wirtschaft mit mehreren Prozessketten-Verfahren mit mehreren Akteuren auf Seite der öffentlichen Verwaltung verbunden sind; es kann von einer branchenweiten oder branchenübergreifenden Prozesskette gesprochen werden ("2+x) : (2+x) : (2+x)").

Prozesslandkarte. Um das Ziel der praktischen Implementierung von Level-1 Prozessketten erreichen zu können und damit die Realisierung einer im übertragenen Sinne, elektronischen Steckdose zwischen Wirtschaft und Verwaltung zu schaffen, ist die Visualisierung von Prozessketten ("Prozesslandkarte") ein weiterer wichtiger Aspekt. Diese Prozesslandkarte ermöglicht die Erschließung von Wissen über die PRK sowie Informationen über die Zusammenhänge mehrerer PRK in einer Prozessbibliothek abzubilden. Diese können von Entscheidungsträgerinnen und Entscheidungsträgern, Anwenderinnen und Anwender, Kundinnen und Kunden sowie der interessier-

ten Öffentlichkeit genutzt werden.
siehe auch PRK-Screening, PRK-Scoping, PRK-Bauplan

Risikoanalyse. (englisch "Risk Assessment / Analysis") Mit einer Risikoanalyse wird untersucht, welche schädigenden Ereignisse eintreten können, wie wahrscheinlich das Eintreten eines schädigenden Ereignisses ist und welche negativen Folgen der Schaden hätte. (Quelle: BSI)

Serviceorientierte Architektur (SOA). Serviceorientierte Architekturen beschreiben fachliche Architekturkonzepte zur Vernetzung und Verwendung verteilter Dienste bzw. Services (meist Webservices). Dabei werden die Anwendungsbausteine (Services) lose miteinander gekoppelt und je nach Bedarf zu umfassenden Diensten und Dienstleistungen verbunden (Service-Orchestrierung). SOA wird zunehmend in E-Government-Architekturen eingesetzt.

Sparkassen. Öffentlich-rechtliche Kreditinstitute, deren Träger meist die Kommunen sind. Eine besonders starke Stellung haben die Sparkassen auch heute noch im Spargeschäft. (Quelle: Bundesbank)
siehe auch Bank, Finanzdienstleister

Standards und Architekturen für E-Government-Anwendungen (SAGA). Das Dokument "Standards und Architekturen für E-Government-Anwendungen" (SAGA) des BMI beinhaltet Empfehlungen zu Standards, Architekturen, Infrastrukturen, Spezifikationen und Technologien für E-Government-Anwendungen. Ziel ist es, die Interoperabilität, Skalierbarkeit, Wiederverwendbarkeit, Plattformunabhängigkeit und eine daraus resultierende Senkung der Kosten und Risiken für den Einsatz dieser Anwendungen zu erreichen.

Universalbank. Im Gegensatz zu den Spezialbanken Institute, die alle Geschäfte einer Bank betreiben, insbesondere das Kredit- und das Wertpapiergeschäft. In Deutschland sind die meisten Banken als Universalbanken tätig, weshalb man auch von einem Universalbankensystem spricht. (Quelle: Bundesbank)
siehe auch Bank, Finanzdienstleister

Wertschöpfung. Wertschöpfung bezeichnet die in den unterschiedlichen Wirtschaftsbereichen erbrachte wirtschaftliche Leistung. Die Wertschöpfung berechnet sich hierbei aus der Differenz zwischen Produktionswert und Vorleistungen. Speziell für Kreditinstitute (und Versicherungsunternehmen) gilt aber eine besondere Berechnungsmethode, da Zinsen (und Versicherungsprämien) nicht zu den Verkäufen von Dienstleistungen gezählt werden.

Wertschöpfungscluster. Wertschöpfungscluster sind definierte Stellen an denen die Wirtschaft (Sender) ihre Meldungen an die öffentliche Verwaltung (Empfänger) abschickt und über die sie Rückmeldungen des Systems wieder empfängt. Hierbei erfolgt in der Studie eine Unterscheidung in direkte Wertschöpfungscluster (Kundenakquisition / -segmentierung, Kundenberatung und Verkauf, Kundenservice, Kundenbindung) und indirekte Wertschöpfungscluster (Führung, Governance, Compliance, IT-Management, Personal, Rechnungswesen, Abwicklung, Produktentwicklung).

Zertifizierung. Zertifizierung nach ISO 27001 auf der Basis von IT-Grundschutz.
siehe auch ISO 27001

12 Abkürzungsverzeichnis

Abs.	Absatz
AG	Aktiengesellschaft
AGB	Allgemeine Geschäftsbedingungen
AnzV	Anzeigenverordnung
ArbschG	Arbeitsschutzgesetz
AWG	Außenwirtschaftsgesetz
AWV	Außenwirtschaftsverordnung
AWV	Außenwirtschaftsverordnung
BaFin	Bundesanstalt für Finanzdienstleistungsaufsicht
BAY	Bayern
BB	Deutsche Bundesbank
BBankG	Bundesbankgesetz
BBKG	Gesetz über die Errichtung des Bundesamtes für Bevölkerungsschutz und Katastrophenhilfe
BdB	Bundesverband deutscher Banken
BDSG	Bundesdatenschutzgesetz
BeurkG	Beurkundungsgesetz
BGB	Bürgerliches Gesetzbuch
BITV	Verordnung zur Schaffung barrierefreier Informa- tionstechnik nach dem Behindertengleichstel- lungsgesetz (Barrierefreie Informationstechnik- Verordnung - BITV)
BKA	Bundeskriminalamt
BMF	Bundesministerium der Finanzen
BMI	Bundesministerium des Innern
BRB	Brandenburg

BSC	Balanced Scorecard
BSI	Bundesamt für Sicherheit in der Informations- technologie
BStatG	Bundesstatistikgesetz
BVR	Bundesverband der Deutschen Volks- und Raiffeisenbanken
BW	Baden-Württemberg
bzw.	beziehungsweise
CA	Certification Authority
ca.	circa
d. h.	das heißt
destatis	Statistisches Bundesamt
DMZ	Demilitarisierte Zone
DVDV	Deutsches Verwaltungsdienstverzeichnis
EFQM	European Foundation for Quality Management
eGOV bzw. E-Government	Electronic Government, elektronisches Regieren und Verwalten
EGVP	Elektronisches Gerichts- und Verwaltungspost- fach
EIF	European Interoperability Framework
ePA	elektronischer Personalausweis
ePass	elektronischer Reisepass
EPK	Ereignisgesteuerte Prozesskette
EPOST	Polizeiinterne Infrastruktur / Anwendung
ErbStG	Erbschaftssteuer- und Schenkungssteuergesetz
EStDV	Einkommenssteuerdurchführungsverordnung
et al.	und andere
etc.	et cetera
eVA	elektronische Verdachtsanzeige

evtl.	eventuell
EWU	Europäische Wirtschaftsunion
f.	folgend
FDL	Finanzdienstleister
FED	Federal Reserve System (US-Notenbank)
ff.	fortfolgend
FIU	Financial Intelligence Unit des BKA
FkSolV	Finanzkonglomerate-Solvabilitäts-Verordnung
FMC	Fundamental Modeling Concepts
G1, G2, G3	Generation 1, Generation 2, Generation 3
GBO	Grundbuchordnung
GBV	Grundbuchverfügung
ggf.	gegebenenfalls
GroMiKV	Großkredit- und Millionenkreditverordnung
GVA	Geldwäscheverdachts-Anzeige
GwG	Geldwäschegesetz
HES	Hessen
HGB	Handelsgesetzbuch
HMG	Hochleistungsportal zum Management von Geldwäsche-Verdachtsanzeigen
Hrsg.	Herausgeber
HTTPS	Hypertext Transfer Protocol Secure
i. d. R.	in der Regel
i. S. d.	im Sinne des
IAO	Fraunhofer-Institut für Arbeitswirtschaft und Or- ganisation
IBH	Investitionsbank Hessen
ID	Identität bzw. Identifikationsnummer
IDABC	Interoperable Delivery of European eGovernment

	Services to public Administrations, Businesses and Citizens
IDP	Identity Provider (IDP)
IEC	International Electrotechnical Commission
IFD	Initiative Finanzstandort Deutschland
ILB	InvestitionsBank des Landes Brandenburg
inkl.	inklusive
INPOL	Anwendungsprogramm (Datenbank) der Polizei
InsO	Insolvenzordnung
InsO	Insolvenzordnung
InvG	Investmentgesetz
IP	Informationspflichten nach SKM
IPsec	Internet Protocol Security
IQC	Industrialisierungs-Quick-Check
ISB	Investitions- und Strukturbank Rheinland-Pfalz (ISB) GmbH
ISO	International Standard Organisation
IT	Informations- und Telekommunikations-technologien
IuK	Informations- und Kommunikationstechnologie
k. A.	keine Angabe
Kap.	Kapitel
KBSt	Koordinierungs- und Beratungsstelle der Bundesregierung für Informationstechnik in der Bundesverwaltung
KfW	KfW Bankengruppe
KWG	Gesetz über das Kreditwesen (Kreditwesengesetz)
LBK	L-Bank Landeskreditbank Baden-Württemberg

LDSG	Datenschutzgesetze der Bundesländer
LFA	LfA Förderbank Bayern
LiqV	Liquiditätsverordnung
LKA	Landeskriminalamt
LR	Landwirtschaftliche Rentenbank
LrV	Länderrisikoverordnung
MaRisk	Mindestanforderungen an das Risikomanagement
MIME	Multipurpose Internet Mail Extensions
MonAwV	Monatsausweisverordnung
MuSchuG	Mutterschutzgesetz
MVP	Melde- und Veröffentlichungsplattform (BaFin)
NACE	Nomenclature statistique des activités économiques dans la Communauté européenne
NBK	NBank Investitions- und Förderbank Niedersachsen GmbH
NDS	Niedersachsen
NRW	Nordrhein-Westfalen
NRWB	NRW BANK
OLA	Operational Level Agreement
OLA	Operational Level Agreement
OSCI	Online Services Computer Interface
ÖV	Öffentliche Verwaltung
p. a.	Per anno / pro Jahr
PDF	Portable Document Format
PGP	Pretty Good Privacy
PostIdent	Verfahren der sicheren persönlichen Identifikation von Personen, die durch die Mitarbeiterinnen und Mitarbeiter der Deutschen Post AG vorgenom-

	men wird
PPP	Public-Private-Partnership
PRK	Prozesskette
RP	Rheinland-Pfalz
s. o.	siehe oben
SAFE	Secure Access to Federated e-Justice / e-Government
SAFE / DIM	Secure Access to Federated e-Justice / e-Government / Distributed Identity Management
SAGA	Standards und Architekturen für E-Government-Anwendungen
SAL	Saarland
SAMBA	Standard Anwendung Meldewesen Banken
SAML	Security Assertion Markup Language
SGB	Sozialgesetzbuch
SigG	Signaturgesetz
SigV	Signaturverordnung
SIKB	Saarländische Investitionskreditbank AG
SINA	Sichere Inter-Netzwerk Architektur
SIT	Fraunhofer-Institut für Sichere Informationstechnologie
SKM	Standardkosten-Modell
SLA	Service Level Agreement
Smaragd	Fachanwendung Fallakte (im Rahmen Geldwäsche)
SOA	Serviceorientierte Architektur
sog.	Sogenannt(e)
SolvV	Solvabilitätsverordnung
SPML 2.0	Service Provisioning Markup Language

SPMLv2 XSD Profile	XML-Schema zu SPML
SSC	Shared Service Center
SSL	Secure Sockets Layer
StGB	Strafgesetzbuch
StPO	Strafprozessordnung
TAB	Thüringer Aufbaubank
TD	Trust-Domain
THÜ	Thüringen
TRIZ	Theorie des erfinderischen Problemlösens (russisches Akronym)
u. a.	unter anderem
usw.	und so weiter
VBS	Vorgangsbearbeitungssystem
VerdStaG	Gesetz über die Statistik der Verdienste und Arbeitskosten (Verdienststatistikgesetz)
VPN	Virtual Private Network
WiBe	Wirtschaftlichkeitsbetrachtungen
WS	Web Service (Webservice)
WS-Federation	Federated Identity-Management für Webservices
WS-Policy	Anforderungen an Web Services
WS-Security	Web Service Security
WS-SecurityPolicy	Web Service Sicherheitsrichtlinie
WS-Trust	Erweiterung der WS-Security Spezifikation
XML	Extensible Markup Language
XÖV	XML-basierte fachliche Standards für den elektronischen Datenaustausch innerhalb und mit der öffentlichen Verwaltung
XPath	XML Path Language
XSD	Extensible Markup Language Schema Definition

z. B.	zum Beispiel
z. T.	zum Teil
ZPO	Zivilprozessordnung
ZSS Einkommens- nachweis	Zentrale Speicherstelle Einkommensnachweis
ZuMonAwV	Zusammengefaßte-Monatsausweise-Verordnung

13 Das Autorenteam

Norbert Frösche M.A.

Fraunhofer IAO
Projektleiter
Senior Consultant und Internet-Researcher, Sprecher Fraunhofer eGovernment Zentrum



Claus-Peter Praeg Diplom Ökonom (Dipl. oec.)

Fraunhofer IAO
Stv. Projektleiter
Senior Consultant, Verantwortlicher für den Bereich "Bankenindustrialisierung" im Rahmen des Innovationsforums "Bank & Zukunft"



Jürgen Baum Dipl. Geograph

Fraunhofer SIT
Wissenschaftlicher Mitarbeiter, Projektleiter,
IT-Sicherheitsexperte



Prof. **Manfred Gerblinger** Akad. Rat, Ass. iur.
Juristische Fakultät der Universität Tübingen
Rechtsinformatik-Beauftragter
und Leiter des Computer-Zentrums
der Juristischen Fakultät



Peter Heiler Diplom-Kaufmann
Commerzbank AG
Abteilungsleiter



Reiner Kraft
Fraunhofer SIT
Wissenschaftlicher Mitarbeiter,
Projektleiter, IT-Sicherheitsexperte



Klaus Kuper
GAD eG
Portfoliomanagement Produktfeld Kredit
und Finanzierung



Lutz Nentwig Dipl.-Inform.
Fraunhofer ISST
Projektleiter, Geschäftsfeldleiter E-Government,
Service-orientierte Architekturen, Standards (SAGA)



Dr. Gerhard Ringwald
Juristische Fakultät der Universität Tübingen
Rechtsexperte Öffentliches Recht, IT-Recht,
Rechtsinformatik



Rainer Rosenmüller Dipl.-Mathematiker
Fraunhofer ISST
IT-Architektur Experte



Uwe Rubart Dipl. Betriebswirt
GAD eG
Portfoliomanagement Produktfeld Kredit
und Finanzierung



Anhang I – Prozessbibliothek

FDL-Prozesskette in Deutschland – Ergebnistabelle des PRK-Screenings

M1 ID	M2 Name der PRK	M3 Gesetzliche Anspruchsgrundlage	M4 Wertschöpfungs-Cluster (Bankensektor)	M6 Involvierte Akteure (Verwaltung)																M15 prozessketten- browser Generation (Farbe: 1 = rot, 2 = gelb, 3 = grün)	M16 IP-Identnummer (SKM-DB)	M17 Kosten in T Euro (SKM-DB)				
				BaFin	Bundesbank	Stat. Bundes- und Landesämter Insolvenzgerichte PEF	Bundes- und Landeskriminal amt (ggf. noch Staatsanwälte, Bankverlag)	Krankenkassen	Umlagekasse (UZ) bei den gesetzlichen Krankenkassen)	Rentenversich- erung Bundesagentur für Arbeit	Finanzamt	Grundbuchamt / Notariat	Bundesanzeiger	Förderinstitute	Einwohnermelde- amt	Verwaltungs- Berufsgenossenschaft	Arbeitschutz	Integrationsamt	Familienkasse							
24	Kreditnehmerstatistik	§ 18 Bundesbankgesetz	Finanzen / Rechnungswesen		x																		3			
25	K3-Meldung (Vermögen Gebietsansässiger)	§ 56a Abs. 1 Außenwirtschafts- verordnung AWW	Finanzen / Rechnungswesen		x																			3	20061115124723 1	3.775,00
26	K4-Meldung (Vermögen Gebietsfremder)	§56 a Abs. 1 Außenwirtschafts- verordnung AWW	Finanzen / Rechnungswesen		x																			3	20061115124723 3	1.525,00
27	OTC Derivate Statistik und CDS Statistik	§ 18 Bundesbankgesetz	Finanzen / Rechnungswesen		x																			3		
28	Handelsbucheigenschaft und Handelsbuchkriterien	§ 1a Abs. 4 S. 1 KWG	Finanzen / Rechnungswesen	x	x																			1	20061101131826 1	3
29	Handelsbucheigenschaft und Handelsbuchkriterien: Bagatellregelung	§§ 1a und 2 Abs. 11 KWG §§ 44 - 47 GroMiKV	Finanzen / Rechnungswesen	x	x																			1	20061101131826 8	< 0,5
30	Angaben zu den Handelsbuchpositionen	§§ 1a und 2 Abs. 11 KWG §§ 44, 45 und 48 GroMiKV	Finanzen / Rechnungswesen		x																			1		
31	Organisatorische Maßnahmen i.S.d. § 2 XI KWG	§ 47 GroMiKV	Finanzen / Rechnungswesen	x	x																			1		
32	Anzeigepflicht für Inhaber bei Erwerb bedeutender Beteiligung	§ 2c Abs.1 S. 1 KWG i.V.m. § 2 Abs. 1 Nr. 1 AnzV	Finanzen / Rechnungswesen	x	x																			1		
33	Bestellung eines Geschäftsleiters und Person mit Einzelvertretung	Anzeige gemäß § 2 Abs. 3 S. 2 AnzV entbehrlich, wenn Anzeige nach § 24 Abs. 1 Nr. 1 KWG, da nach § 24 Nr.1 KWG die Absicht und den Vollzug der Bestellung von Geschäftsleitern angezeigt wird	Finanzen / Rechnungswesen	x																				1	20061101131702 15, 20061101131702 16	54

M1 ID	M2 Name der PRK	M3 Gesetzliche Anspruchsgrundlage	M4 Wertschöpfungs-Cluster (Bankensektor)	M6 Involvierte Akteure (Verwaltung)																	M15 prozessketten- browser Generation (Farbe: 1 = rot, 2 = gelb, 3 = grün)	M16 IP-Identnummer (SKM-DB)	M17 Kosten in T Euro (SKM-DB)		
				BaFin	Bundesbank	Stat. Bundes- und Landesämter Arbeitsgericht / Insolvenzgeric h PEB	Bundes- und Landeskriminal amt (ggf. noch Staatsanwaltschaft Bankverlag	Krankenkassen	Umlagekasse (UZ) bei den gesetzlichen Krankenkassen	Dr. Rentenversicherungs- Bundessagentur für Arbeit	Finanzamt	Grundbuchamt / Notariat	Bundesanzeiger	Förderinstitute	Einwohnermeld eamt	Verwaltungs- Berufsgenossenschaft Arbeitsamt für	Integrationsamt	Familienkasse							
34	Absicht der Erhöhung einer bedeutenden Beteiligung	§ 2c Abs. 1 S. 7 KWG i.V.m. § 2 Abs. 1 Nr. 3 AnzV	Finanzen / Rechnungswesen	x	x																		2	2006110113182610	< 0,5
35	Abweichende Durchführung beabsichtigter Maßnahmen (Erhöhung)	§ 2c Abs. 1a S. 2 u. 3 KWG i.V.m. § 2c Abs. 4 S. 3 i.V.m. § 2 Abs. 1 S. 1 Nr. 5 AnzV	Finanzen / Rechnungswesen	x	x																		1		
36	Absicht der Absenkung einer bedeutenden Beteiligung	§ 2c Abs. 4 S. 1 KWG i.V.m. § 2 Abs. 1 Nr. 4 AnzV	Finanzen / Rechnungswesen	x	x																		1		
37	Ggf. Nicht-bzw.unveränderte Durchführung beabsichtigter Maßnahmen	§ 2c Abs. 4 S. 3. u 4 KWG i.V.m. § 2 Abs. 1 S. 2 AnzV	Finanzen / Rechnungswesen	x	x																		1		
38	Abweichende Durchführung beabsichtigter Maßnahmen (Absenkung)	§ 2 Abs. 1 Nr. 5 AnzV	Finanzen / Rechnungswesen	x	x																		1		
39	Änderung der Verhältnisse beim Inhaber einer bedeutenden Beteiligung	§ 2 Abs. 4 S. 1 AnzV	Finanzen / Rechnungswesen	x	x																		1		

M1 ID	M2 Name der PRK	M3 Gesetzliche Anspruchsgrundlage	M4 Wertschöpfungs-Cluster (Bankensektor)	M6 Involvierte Akteure (Verwaltung)																		M15 prozessketten- browser Generation (Farbe: 1 = rot, 2 = gelb, 3 = grün)	M16 IP-Identnummer (SKM-DB)	M17 Kosten in T Euro (SKM-DB)		
				BaFin	Bundesbank	Stat. Bundes- und Landesämter Insolvenzgerichte IFED	Bundes- und Landeskriminal- amt (ggf. noch Staatsanwaltschaft Bankverträge)	Krankenkassen	Umlagekasse (UZ) bei den gesetzlichen Krankenkassen)	Rentenversich- erung Bundesagentur für Arbeit	Finanzamt	Grundbuchamt / Notariat	Bundesanzeiger	Förderinstitute	Einwohnermeld- eamt	Verwaltungs- Berufsgenosse beschäft Amt für Arbeitsschutz	Integrationsam- t	Familienkasse								
40	Angaben zur Eigenkapitalausstattung	§ 10 Abs. 1e KWG i.V.m. § 6 II SolvV	Finanzen / Rechnungswesen	x	x																			3		
41	Angabenüberprüfung bzgl. angemessenen Eigenmittelausstattung (SolvV)	ergänzend zu 35 § 10 Abs. 1 S. 9 KWG § 6 Abs. 1 S. 1 SolvV	Finanzen / Rechnungswesen		x																			1		
42	Angaben zur Überprüfung angemessenen Eigenmittelausstattung (SolvV)	§ 10 Abs. 1 S. 9 KWG § 6 Abs. 1 S. 2 SolvV	Finanzen / Rechnungswesen	x	x																			1		
43	Berechnung der nicht realisierten Reserven	§ 10 Abs. 4a S. 4 KWG i.V.m. § 3 Abs. 1 AnzV	Finanzen / Rechnungswesen	x	x																			1	20061101131601 9	282
44	Sachverständigenausschuss zur Beleihungswertermittlung	§ 10 Abs. 4b S. 4 KWG i.V.m. § 77 Abs. 3 S. 1 InvG i.V.m. § 3 Abs. 2 AnzV	Finanzen / Rechnungswesen	x																				1	20061101131601 10	26
45	Ausscheiden eines Sachverständigen oder Änderungen der Tatsachen	§ 3 Abs. 2 S. 1 AnzV	Finanzen / Rechnungswesen	x																				1		
46	Anzeigespflicht- bei Absicht der Ingebrauchnahme der Marktpflege	§ 10 Abs. 5 S. 7, Abs. 5a S. 7, Abs. 7 S. 6 KWG	Finanzen / Rechnungswesen	x	x																			1	20061101131601 10	< 100
47	Absinken der Eigenmittel auf kurzfristige nachrangige Verbindlichkeiten	§ 10 Abs. 7 S. 7 KWG	Finanzen / Rechnungswesen	x	x																			1	20061101131601 10	< 100
48	Abzugspositionen vom Kern- und Ergänzungskapital	§ 10 Abs. 6 S. 2, 3 und 6 KWG	Finanzen / Rechnungswesen	x																				1	20061101131601 10	< 0,5
49	Abzugskredite	§ 10 Abs. 8 S. 1, 3, 4 KWG i.V.m. § 4 AnzV	Finanzen / Rechnungswesen	x	x																			1	20061101131601 19, 20061101131601 20, 20061101131601 21	< 100
50	Verlust i.H.v. 25% des haftenden Eigenkapitals	§ 24 Abs. 1 Nr. 4 KWG	Finanzen / Rechnungswesen	x	x																			1	20061101131702 3	< 100
51	Absinken des Anfangskapitals unter die gesetzl. Mindestanforderung	§ 24 Abs. 1 Nr. 9 KWG	Finanzen / Rechnungswesen	x	x																			1	20061101131702 10	Nullmessung!

M1 ID	M2 Name der PRK	M3 Gesetzliche Anspruchsgrundlage	M4 Wertschöpfungs-Cluster (Bankensektor)	M6 Involvierte Akteure (Verwaltung)																	M15 prozessketten- browser Generation (Farbe: 1 = rot, 2 = gelb, 3 = grün)	M16 IP-identnummer (SKM-DB)	M17 Kosten in T Euro (SKM-DB)				
				BaFin	Bundesbank	Stat. Bundes- und Landesämter insolvenzgeric ht	Bundes- und Landeskriminal amt (ggf. noch Staatsanwälte, Bankverlag)	Krankenkassen	Umsatzkasse (Uz) bei den gesetzlichen Krankenkassen)	De Rentenversich erung Bundesagentur für Arbeit	Finanzamt	Grundbuchamt / Notariat	Bundesanzeig e	Förderinstitute	Einwohnermeld eamt	Verwaltungs- Berufsgenosse nschaft	Arbeitschutz	Integrationsam t	Familienkasse								
52	Überschreitung der Grenze bei qualifizierten Beteiligungen §12 IS.1KWG	§ 12 Abs. 1 S. 1 KWG	Finanzen / Rechnungswesen	x																				1			
53	Überschreitung der Grenze bei qualifizierten Beteiligungen §12 IS.2KWG	§ 12 Abs. 1 S. 2 KWG	Finanzen / Rechnungswesen	x																					1		
54	Überschreitung der Grenze bei qualifizierten Beteiligungen §12 IS.1KWG	§ 12 Abs. 2 S. 3 KWG	Finanzen / Rechnungswesen	x																					1		
55	Überschreitung der Grenze bei qualifizierter Beteiligungen §12 IS.2KWG	§ 12 Abs. 2 S. 3 KWG	Finanzen / Rechnungswesen	x																					1		
56	Aktivische Beteiligungen	§ 24 Abs. 1 Nr. 12 KWG, § 24 Abs. 1 Nr. 13 KWG, § 24 Abs. 1a Nr. 1 u. 2 KWG § 12a Abs.1 S.3 KWG, § 7 AnzV	Finanzen / Rechnungswesen	x																					3		

M1 ID	M2 Name der PRK	M3 Gesetzliche Anspruchsgrundlage	M4 Wertschöpfungs-Cluster (Bankensektor)	M6 Involvierte Akteure (Verwaltung)																	M15 prozessketten- browser Generation (Farbe: 1 = rot, 2 = gelb, 3 = grün)	M16 IP-Identnummer (SKM-DB)	M17 Kosten in T Euro (SKM-DB)		
				BaFin	Bundesbank	Stat. Bundes- und Landesämter Insolvenzgeric h IFED	Bundes- und Landeskriminal amt (ggf. noch Staatsanwälte, Bankverlag)	Krankenkassen	Umlagekasse (UZ) bei den gesetzlichen Krankenkassen)	Dt. Rentenversich erung	Bundesagentur für Arbeit	Finanzamt	Grundbuchamt / Notariat	Bundesanzeiger	Förderinstitute	Einwohnermeld eamt	Verwaltungs- Berufsenosse pschaft	Arbeitschutz	Integrationsam t	Familienkasse					
57	Aktivbeteiligungen	§ 24 Abs. 1a Nr. 1 u. 2 KWG, § 7 Abs. 2 AnzV	Finanzen / Rechnungswesen		x (zur Weiterleitung an die BaFin)																		3	2006110113170222	118
58	Passivbeteiligungen	§ 24 Abs. 1 Nr. 10 KWG, § 24 Abs. 1 Nr. 12 KWG, § 24 Abs. 1a Nr. 1 KWG, § 8 Abs. 1 AnzV	Finanzen / Rechnungswesen		x (zur Weiterleitung an die BaFin)																		3		
59	Sammelanzeige	§ 24 Abs. 1a Nr. 1 KWG, § 8 Abs. 2 AnzV	Finanzen / Rechnungswesen		x																		3	2006110113170220	118
60	Aktivische und Passivische Beteiligung - § 24 la Nr.3KWG	§ 24 Abs. 1a Nr. 3 KWG, § 8 Abs. 2 AnzV	Finanzen / Rechnungswesen		x (zur Weiterleitung an die BaFin)																		3	2006110113170210	18
61	Großkredit	§§ 13b Abs. 1 i.V.m. 13a Abs. 1 S. 1 KWG i.V.m. §§ 8 Abs. 2 u. 5, 53 u. 70 GroMiKV	Finanzen / Rechnungswesen		x																		3	200611011318031	23.384,00
62	Sammelanzeige der Betragdaten	§ 13 Abs. 1 S. 1 i.V.m. S. 2 KWG § 13a Abs. 1 S. 1 KWG § 13b Abs. 1 KWG §§ 8 Abs. 2 u. 5, 53 u. 70 GroMiKV	Finanzen / Rechnungswesen		x																		3	200611011318032	8.682,00

M1 ID	M2 Name der PRK	M3 Gesetzliche Anspruchsgrundlage	M4 Wertschöpfungs-Cluster (Bankensektor)	M6 Involvierte Akteure (Verwaltung)																	M15 prozessketten- browser Generation (Farbe: 1 = rot, 2 = gelb, 3 = grün)	M16 IP-Identnummer (SKM-DB)	M17 Kosten in T Euro (SKM-DB)		
				BaFIN	Bundesbank	Stat. Bundes- und Landesämter Arbeitsgericht / Insolvenzgerichte PEB	Bundes- und Landeskriminal- amt (ggf. noch Staatsanwälte, Bankverlag)	Krankenkassen	Umlagekasse (UZ) bei den gesetzlichen Krankenkassen	Deutscher Rentenversicherungs- bund Bundesagentur für Arbeit	Finanzamt	Grundbuchamt / Notariat	Bundesanzeiger	Förderinstitute	Einwohnermeldeamt	Verwaltungs- Berufsenosse beschäftigt Amt für Arbeitsschutz	Integrationsamt	Familienkasse							
63	Unerlaubte Überschreitung der Anlagebuch-Großkrediteinzelobergrenze	§§ 13b Abs. 1 i.V.m. § 13a Abs. 3 S. 2 u. 4 KWG i.V.m. §§ 72 i.V.m. 56 GroMiKV	Finanzen / Rechnungswesen	x	x																	3	2006110113180312	18	
64	Überschreitung der Anlagebuch-Großkreditgesamtobergrenze	§§ 13b Abs. 1 i.V.m. 13a Abs. 3 S. 6 KWG i.V.m. §§ 72 i.V.m. 56 GroMiKV	Finanzen / Rechnungswesen	x	x																		2	2006110113180310	<0,5
65	Unerlaubte Erhöhung der Gesamtbuch-Großkrediteinzelobergrenze	§§ 13b Abs. 1 i.V.m. 13a Abs. 4 S. 2 - 4 KWG i.V.m. §§ 72 i.V.m. 56 GroMiKV	Finanzen / Rechnungswesen	x	x																		2		
66	Unerlaubte Überschreitung der Gesamtbuch-Großkreditgesamtobergrenze	§§ 13b Abs. 1 i.V.m. 13a Abs. 4 S. 6 KWG i.V.m. §§ 72 i.V.m. 56 GroMiKV	Finanzen / Rechnungswesen	x	x																		2	2006110113180317	< 500
67	Überschreitung kreditnehmerbezogenen Handelsbuch-Gesampositionen	§§ 13b Abs. 1 i.V.m. 13a Abs. 5 S. 2 KWG i.V.m. §§ 72 i.V.m. 56 GroMiKV	Finanzen / Rechnungswesen	x	x																		2	2006110113180318	1
68	Überschreitung der Gesamtüberschreitungspositionen	§§ 13b Abs. 1 i.V.m. 13a Abs. 5 S. 4 KWG i.V.m. §§ 72 i.V.m. 56 GroMiKV	Finanzen / Rechnungswesen	x	x																		2	2006110113180319	< 100
69	Nachholung einstimmigen Beschluss § 13 Abs.2 S.5,8 KWG (Großkredite)	§ 13 Abs.2 S. 5 u. S.8, Abs. 4, § 13 a Abs. 2 u. Abs. 6 KWG i.V.m. §§ 55 u. 71 GroMiKV	Finanzen / Rechnungswesen	x	x																		2	200611011318034	< 100
70	Nachholung Beschluss § 13 II S.5,8 KWG (Kreditrahmenkontingente)	gem. Bundesbank: § 13 Abs. 2 S. 5 u. 8, Abs. 4 KWG § 13a Abs. 2 und 6 KWG §§ 55 u. 71 GroMiKV	Finanzen / Rechnungswesen		x																		1	200611011318036	< 100

M1	M2	M3	M4	M6 Involvierte Akteure (Verwaltung)																	M15	M16	M17					
				BaFin	Bundesbank	Stat. Bundes- und Landesämter	Insolvenzgerichte	PEF	Bundes- und Landeskriminalamt (ggf. noch Staatsanwaltschaft)	Bankvertrag	Krankenkassen	Umlagekasse (UZ) bei den gesetzlichen Krankenkassen	Dr. Rentenversicherung	Bundesagentur für Arbeit	Finanzamt	Grundbuchamt / Notariat	Bundesanzeiger	Förderinstitute	Einwohnermeldedienst	Verwaltungs-Berufsenosse paschäft				Arbeitschutz	Integrationsamt	Familienkasse		
71	Kreditrahmenkontingente	§§ 13b Abs. 1 i.V.m. 13a Abs. 6 KWG i.V.m. § 13a Abs. 1 u 2 KWG und §§ 73 u. 57 GroMiKV (Hinweis: § 13b = Institutgruppe) § 13 Abs. 4 KWG § 13a Abs. 6 KWG § 13b Abs. 1 KWG §§ 57 u. 73 GroMiKV	Finanzen / Rechnungswesen		x																					2	20061101131803 15	49
72	Obergrenze nach §§ 13, 13 a KWG bei übergeordnete Unternehmen	§ 13b Abs. 1 u 4 KWG § 14 Abs. 1 KWG	Finanzen / Rechnungswesen		x (tw. zur Weiterleitung an die BaFin)																				1			
73	Abrufbereitschaft	§ 54 Abs. 1 GroMiKV § 59 GroMiKV § 54 Abs. 2 GroMiKV	Finanzen / Rechnungswesen	x	x																				1			
74	Millionenkredite	§ 14 Abs. 1 S.1 u. 2 KWG i.V.m. §§ 8 u 74 GroMiKV	Finanzen / Rechnungswesen		x																				1			
75	Anzeige der Betragsdaten	§ 14 Abs. 1 S.1 u. 2 KWG i.V.m. §§ 74 und 8 Abs. 1 u 5 GroMiKV	Finanzen / Rechnungswesen		x																				2			
76	Meldepflichtig ist (ggf.) analog für das übergeordnete Unternehmen	§ 14 Abs. 1 S. 2 u 3 KWG	Finanzen / Rechnungswesen		x (tw. zur Weiterleitung an die BaFin)																				1			

M1 ID	M2 Name der PRK	M3 Gesetzliche Anspruchsgrundlage	M4 Wertschöpfungs-Cluster (Bankensektor)	M6 Involvierte Akteure (Verwaltung)																	M15 prozessketten- browser Generation (Farbe: 1 = rot, 2 = gelb, 3 = grün)	M16 IP-Identnummer (SKM-DB)	M17 Kosten in T Euro (SKM-DB)		
				BaFin	Bundesbank	Stat. Bundes- und Landesämter Insolvenzgerichte IFED	Bundes- und Landeskriminal- amt (ggf. noch Staatsanwälte, Bankverlag)	Krankenkassen	Umlagekasse (UZ) bei den gesetzlichen Krankenkassen)	Dr. Rentenversich- erung	Bundesagentur für Arbeit	Finanzamt	Grundbuchamt / Notariat	Bundesanzeiger	Förderinstitute	Einwohnermeld- eamt	Verwaltungs- Berufsenosse paschäft	Arbeitschutz	Integrationsam- t	Familienkasse					
77	unterlassene Nachholung der Organkredit-Beschlussfassung	§ 15 Abs. 4 S. 5 KWG	Finanzen / Rechnungswesen	x																			1	20061101131803 23	< 100
78	Bestellung eines Geschäftsleiters und einer Person mit Einzelvertretung	§ 24 Abs. 1 Nr. 1 KWG i.V.m. § 5 AnzV	Recht	x	x																		2	20061101131702 10	39
79	Vollzug der Bestellung eines Geschäftsleiters	§ 24 Abs. 1 Nr. 1 a.E. KWG	Recht	x	x																		2	20061101131702 10	15
80	Ermächtigung eines Vetreters des Instituts im gesamten Geschäftsbereich	§ 24 Abs. 1 Nr. 1 KWG i.V.m. § 5 AnzV	Recht	x	x																		2		
81	Ausscheiden eines Geschäftsleiters	§ 24 Abs. 1 Nr. 2 KWG § 5 AnzV	Recht	x	x																		2	20061101131702 10	15
82	Geschäftsleiter: Nebentätigkeit	§ 24 Abs. 3 S. 1 Nr. 1 KWG i.V.m. § 11 Abs. 1 AnzV	Recht	x	x																		3	20061101131724 1	72
83	Geschäftsleiter: Beteiligung ab (25%)	§ 24 Abs. 3 S. 1 Nr. 2 KWG i.V.m. § 11 Abs. 2 AnzV	Finanzen / Rechnungswesen	x	x																		3	20061101131724 2	13
84	Anzahl inländischer Zweigstellen	§ 24 Abs. 1a Nr. 4 KWG i.V.m. § 9 AnzV	Finanzen / Rechnungswesen	x	x																		1	20061101131702 14	18

M1	M2	M3	M4	M6 Involvierte Akteure (Verwaltung)																M15	M16	M17				
ID	Name der PRK	Gesetzliche Anspruchsgrundlage	Wertschöpfungs-Cluster (Bankensektor)	BaFin	Bundesbank	Stat. Bundes- und Landesämter	Arbeitsgericht / Insolvenzgericht	RFED	Bundes- und Landeskriminalamt (ggf. noch Staatsanwaltschaft)	Bankvertrag	Krankenkassen	Umlagekasse (UZ) bei den gesetzlichen Krankenkassen	Dt. Rentenversicherung	Bundesagentur für Arbeit	Finanzamt	Grundbuchamt / Notariat	Bundesanzwäger	Förderinstitute	Einwohnermeldeamt	Verwaltungs-Berufsenosse paschäft	Arbeitschutz	Integrationsamt	Familienkasse	prozessketten-browser Generation (Farbe: 1 = rot, 2 = gelb, 3 = grün)	IP-Identnummer (SKM-DB)	Kosten in T Euro (SKM-DB)
85	Absicht der Errichtung einer Zweigniederlassung in einem anderen EWR-Staat	§ 24a Abs. 1 KWG i.V.m. § 12 Abs. 1 u. 4 AnzV	Finanzen / Rechnungswesen	x (zzgl. 1x Kopie bei Österreich, Liechtenstein, Luxemburg, ansonsten zzgl. 1x Übersetzung Bundesbank)																				1	200611011317249	< 0,5
86	Änderung bzgl. von EWR-Zweigniederlassungen	§ 24a Abs. 1 KWG i.V.m. § 12 Abs. 1 AnzV	Finanzen / Rechnungswesen	x (zzgl. 1x Kopie bei Österreich, Liechtenstein, Luxemburg, ansonsten zzgl. 1x Übersetzung Bundesbank)																				1	2006110113172410	< 0,5
87	Errichtung einer Repräsentanz von einem Institut mit Sitz im Ausland	§ 53a S. 2 u. 5 KWG § 15 Abs. 2 Nr. 4 KWG	Finanzen / Rechnungswesen	x		x																		1	200611011321139, 2006110113211310, 2006110113211311	< 100
88	Errichtung grenzüberschreitende Dienstleistungsverkehr § 24a III s.1 3.HS KWG	§ 24a Abs. 3 KWG i.V.m. § 12 AnzV	Finanzen / Rechnungswesen	x (zzgl. 1x Kopie bei Österreich, Liechtenstein, Luxemburg, ansonsten zzgl. 1x Übersetzung Bundesbank)																				2	2006110113172410	1

M1 ID	M2 Name der PRK	M3 Gesetzliche Anspruchsgrundlage	M4 Wertschöpfungs-Cluster (Bankensektor)	M6 Involvierte Akteure (Verwaltung)																M15 prozessketten- browser Generation (Farbe: 1 = rot, 2 = gelb, 3 = grün)	M16 IP-Identnummer (SKM-DB)	M17 Kosten in T Euro (SKM-DB)		
				BaFin	Bundesbank	Stat. Bundes- und Landesämter Arbeitsgericht / Insolvenzgeric h PFED	Bundes- und Landeskriminal amt (ggf. noch Staatsanwälte, Bankverträge)	Krankenkassen	Umlagekasse (UZ) bei den gesetzlichen Krankenkassen)	Dt. Rentenversich erung Bundesagentur für Arbeit	Finanzamt	Grundbuchamt / Notariat	Bundesanzeiger	Förderinstitute	Einwohnermeld eamt	Verwaltungs- Berufsenosse pschaft	Arbeitschutz	Integrationsam t	Familienkasse					
89	Änderungen von Grenzüberschreitenden Dienstleistungsverkehr	§ 24a Abs. 4 S. 1 KWG i.V.m. § 12 Abs. 1 AnzV	Finanzen / Rechnungswesen	x (zzgl. 1x Kopie bei Österr eich, Liechte nstein, Luxem burg, ansons ten zzgl. 1x Überse tzung Bunde sbank)																	2	20061101131724 10	< 100	
90	Änderungen der Verhältnisse § 24 IV S. 3 KWG	§ 24a Abs. 4 S. 3 KWG i.V.m. § 12 AnzV	Finanzen / Rechnungswesen	x (zzgl. 1x Kopie bei Österr eich, Liechte nstein, Luxem burg, ansons ten zzgl. 1x Überse tzung Bunde sbank)																		2	20061101131724 13	Nullmessung!
91	Errichtung/Verlegung oder Schließung einer Zweigstelle im Drittstaat	§ 24 Abs. 1 Nr. 6 KWG i.V.m. § 6 AnzV	Finanzen / Rechnungswesen	x	x																	2	20061101131702 5	5
92	Aufnahme/Beendigung der Dienststelle im Drittstaat	§ 24 Abs. 1 Nr. 6 KWG i.V.m. § 6 AnzV	Finanzen / Rechnungswesen	x	x																	1	20061101131702 4	< 100
93	Ausscheiden aus einer Einlagen- Sicherungseinrichtung	§ 23a Abs. 2 S.1 KWG	Finanzen / Rechnungswesen	x	x																	1	2,00611E+15	< 100
94	Erfüllung der Offenlegungsanforderungen eines Instituts	§ 26a Abs. 1 - 3 KWG § 319 ff SolvV	Finanzen / Rechnungswesen	x	x																	1		

M1 ID	M2 Name der PRK	M3 Gesetzliche Anspruchsgrundlage	M4 Wertschöpfungs-Cluster (Bankensektor)	M6 Involvierte Akteure (Verwaltung)																	M15 prozessketten- browser Generation (Farbe: 1 = rot, 2 = gelb, 3 = grün)	M16 IP-Identnummer (SKM-DB)	M17 Kosten in T Euro (SKM-DB)		
				BaFin	Bundesbank	Stat. Bundes- und Landesämter Amtsgericht / Insolvenzgeric h	PEF	Bundes- und Landeskriminal amt (ggf. noch Staatsanwälte, Bankverlag)	Krankenkassen	Umlagekasse (UZ) bei den gesetzlichen Krankenkassen)	Dr. Rentenversich erung	Bundesagentur für Arbeit	Finanzamt	Grundbuchamt / Notariat	Bundesanzeiger	Förderinstitute	Einwohnermeld eamt	Verwaltungs- Berufsgenosse nschaft	Arbeitschutz	Integrationsam t				Familienkasse	
95	Änderung der Rechtsform oder der Firma (beachte § 32 I KWG)	§ 24 Abs. 1 Nr. 3 KWG: Änderung der Rechtsform (soweit keine neue Erlaubnis gem. § 32 Abs. 1 KWG erforderlich ist) oder der Firma	Finanzen / Rechnungswesen	x	x																		1	20061101131702 1, 20061101131702 2	< 100 + 4
96	Verlegung der Niederlassung oder des Sitzes	§ 24 Abs. 1 Nr. 5 KWG	Führung, Steuerung, Governance	x	x																		1		
97	Einstellung des Geschäftsbetriebs	§ 24 Abs. 1 Nr. 7 KWG	Führung, Steuerung, Governance	x	x																		1	20061101131702 7	1
98	Absicht der Organe, eine Entscheidung zur Auflösung herbeizuführen	§ 24 Abs. 1 Nr. 8 KWG	Führung, Steuerung, Governance	x	x																		1	20061101131702 8	Nullmessung!
99	Unregelmäßigkeiten bei Wertpapierpensions-/darlehensgeschäften	§ 24 Abs. 1 Nr. 11 KWG	Finanzen / Rechnungswesen	x	x																		1	20061101131702 13	< 0,5
100	Fusion von Instituten-Absicht und Vollzug bzw. Scheitern	§ 24 Abs. 2 KWG i.V.m. § 10 AnzV	Finanzen / Rechnungswesen	x	x																		3	20061101131702 20	< 0,5
101	Betreiben eines Zahlungs-, Wertpapierliefer- oder -abrechnungssystems	§ 24b Abs. 1 S. 1 und S. 2 KWG	Organisation / IT	x	x																		1	20061101131724 14	0
102	Betreiben eines System gemäß § 1 XVI KWG	§ 24b Abs. 1 S. 2 KWG	Organisation / IT	x	x																		1		
103	Aufgestellter und festgestellter Jahresabschluss sowie Prüfungsbericht	§ 26 Abs. 1 S. 1 KWG i.V.m. § 13 AnzV	Finanzen / Rechnungswesen	x	x																		1	20061101131743 16	785
104	Zwischenabschlüsse	§ 10 Abs. 3 S. 3 KWG	Finanzen / Rechnungswesen	x	x																		1	20061101131601 4	< 100

M1 ID	M2 Name der PRK	M3 Gesetzliche Anspruchsgrundlage	M4 Wertschöpfungs-Cluster (Bankensektor)	M6 Involvierte Akteure (Verwaltung)																		M15 prozessketten- browser Generation (Farbe: 1 = rot, 2 = gelb, 3 = grün)	M16 IP-Identnummer (SKM-DB)	M17 Kosten in T Euro (SKM-DB)		
				BaFin	Bundesbank	Stat. Bundes- und Landesämter Arbeitsgericht / Insolvenzgeric h PEB	Bundes- und Landeskriminal amt (ggf. noch Staatsanwälte, Bankverlag)	Krankenkassen	Umlagekasse (UZ) bei den gesetzlichen Krankenkassen)	De Rentenversich erung	Bundesagentur für Arbeit	Finanzamt	Grundbuchamt / Notariat	Bundesanzeiger	Förderinstitute	Einwohnermeld eamt	Verwaltungs- Berufsgenosse nschaft	Arbeitschutz	Integrationsam t	Familienkasse						
105	Übergeordnetes Institut einer Gruppe: Zwischenabschluss	§ 10a Abs. 10 S. 4 KWG	Finanzen / Rechnungswesen	x	x																			1		
106	Konzernabschluss und Konzernlagebericht	§ 26a Abs. 4 KWG § 319 ff SolvV	Finanzen / Rechnungswesen	x	x																			1	20061101131743 20, 20061101131743 21	2
107	Bestellung des Prüfers	§ 28 Abs. 1 S. 1 KWG	Führung, Steuerung, Governance	x	x																			1	20061101131534 10	30
108	Gewerbmäßiger Betrieb von Bankgeschäften/ Finanzdienstleistungen	§ 32 Abs. 1 S. 1 KWG i.V.m. § 14 AnzV	Führung, Steuerung, Governance	x																				2	20061101131534 1	1
109	Auskunft/Prüfungen über alle Geschäftsangelegenheiten der Instituten	§ 44 Abs. 1 S. 1, Abs. 2 S. 1 KWG	Finanzen / Rechnungswesen	x																				1	20061101131534 2	1.042
110	Drohende Zahlungsunfähigkeit, Zahlungsunfähigkeit oder Überschuldung	§ 46b Abs. 1 S. 1 KWG	Führung, Steuerung, Governance	x																				1	20061101131534 6	< 100
111	Eröffnung des Insolvenzverfahrens	§ 46b Abs. 1 S. 7 KWG	Führung, Steuerung, Governance	x																				1		
112	Revisionsberichte (Übrige Anzeigespflicht nach der MaRisk BT)	MaRisk BT 2.4.5	Finanzen / Rechnungswesen	x	x																			1		
113	Ausnahmen für Übergeordnete Institute einer Gruppe	§ 2a Abs. 6 KWG	Finanzen / Rechnungswesen	x (und zustän dige Stelle im EWR Staat)																				1		
114	Ausnahmen für Nachgeordnete Institute einer Gruppe	§ 2a Abs. 1, 2 u. 5 KWG	Finanzen / Rechnungswesen	x (und zustän dige Stelle im EWR Staat)																				1		
115	Nachgeordnetes Institut einer Gruppe: Anlassbezogene Überprüfung	§ 2a Abs. 3 KWG	Finanzen / Rechnungswesen	x																				1		

M1	M2	M3	M4	M6 Involvierte Akteure (Verwaltung)																	M15	M16	M17			
				BaFin	Bundesbank	Stat. Bundes- und Landesämter	Landesämter / Amtsgericht / Insolvenzgerichte	PEF	Bundes- und Landes-kriminalamt (ggf. noch Staatsanwälte)	Bankvertrag	Krankenkassen	Umlagekasse (UZ) bei den gesetzlichen Krankenkassen	Dr. Rentenversicherung	Bundesagentur für Arbeit	Finanzamt	Grundbuchamt / Notariat	Bundesanzeiger	Förderinstitute	Einwohnermeldesamt	Verwaltungs-Berufsgenossenschaft				Arbeitschutz	Integrationsamt	Familienkasse
116	Meldevorschriften im Auslandszahlungsverkehr	§ 26 Abs. 2 AWG i.V.m. §§ 59-69 AWW	Finanzen / Rechnungswesen		x																			1		
117	Auslandskreditvolumen	§ 1 Abs. 1 LrV, § 25 Abs. 3 KWG	Finanzen / Rechnungswesen		x																			3	200611011331301, 200611011331302	358 + < 100
118	Entsprechende Konzernmeldung	§ 1 Abs. 2 LrV	Finanzen / Rechnungswesen		x																			2	200611011331303, 200611011331304, 200611011331305	89 +
119	Monatsausweise und weitere Angaben von Instituten an Dt. Bundesbank	§ 25 Abs. 1 S. 3 KWG Anordnung zu § 18 BBkG	Finanzen / Rechnungswesen		x																			1		
120	Zusammengefasster Monatsausweis durch übergeordnetes Unternehmen	§ 25 Abs. 2 KWG i.V.m. ZuMonAwV	Finanzen / Rechnungswesen		x																			1		
121	Verdachtsanzeige nach § 11 Geldwäschegesetz	§ 11 GWG	Compliance							x														1	200709261102011	35.978,00
122	Erfassung Kundendaten für Legitimationsprüfung	Abgabenordnung	Abwicklung (Marktfolge)																					1		
123	Kundenneuanlage im OnlineBanking	Abgabenordnung	Abwicklung (Marktfolge)																					1		
124	Anzeigepflicht gruppeninterner Transaktionen mit gemischten Unternehmen	§ 13c Abs. 1 S. 1 KWG § 64g Abs. 2 i.V.m. Abs. 1 Satz 1 Nr. 4 KWG	Finanzen / Rechnungswesen	x	x																			1	200611011318431	< 0,5
125	Anzeige bei Überschreitung der Obergrenze gruppeninterner Transaktionen	§ 13c Abs. 3 S. 3 KWG	Finanzen / Rechnungswesen	x	x																			1		
126	Online Kontenabfrage	§ 24c KWG	Organisation / IT	x									x											3	200611231115421, 200611231115422	

M1 ID	M2 Name der PRK	M3 Gesetzliche Anspruchsgrundlage	M4 Wertschöpfungs-Cluster (Bankensektor)	M6 Involvierte Akteure (Verwaltung)																	M15 prozessketten- browser Generation (Farbe: 1 = rot, 2 = gelb, 3 = grün)	M16 IP-Identnummer (SKM-DB)	M17 Kosten in T Euro (SKM-DB)								
				BaFIN	Bundesbank	Stat. Bundes- und Landesämter Anspruch / Insolvenzgeric ht	PEF	Bundes- und Landeskriminal amt (ggr. noch Staatsanwälte, Bankverträge)	Krankenkassen	Umlagekasse (UZ) bei den gesetzlichen Krankenkassen)	Dt. Rentenversich erung	Bundesagentur für Arbeit	Finanzamt	Grundbuchamt / Notariat	Bundesanzeiger	Förderinstitute	Einwohnermeld eamt	Verwaltungs- Berufsenosse pschaft	Arbeitschutz	Integrationsam t				Familienkasse							
127	Meldewesen Aussenwirtschaftsverordnung	AWV / AWG	Organisation / IT		x																				3						
128	Meldungen zur Sozialversicherung / Lohnsteuer		Personal							x			x			x												2			
129	elektronische Übermittlung von Jahresabschlussdaten (Bilanzen)	im Zusammenhang mit § 18 KWG	Finanzen / Rechnungswesen	x	x											x													1		
130	Geschäftsleiter: Nebentätigkeit (Aufnahme oder Beendigung)	§ 24 Abs. 3 S. 1 Nr. 1 KWG / § 11 Abs. 1 AnzV	Finanzen / Rechnungswesen	x	x																							3	20061101131724 1	72	
131	Unmittelbare Beteiligung an einem anderen Unternehmen	§ 24 Abs. 3 S. 1 Nr. 2 KWG / § 11 Abs. 2 AnzV	Finanzen / Rechnungswesen	x	x																							3	20061101131702 18	108	
132	Anzeigepflicht für gemischte Finanzholding-Gesellschaften	§ 12a (1) S. 3 u. (3) KWG / § 64g (3) Nr. 2 KWG / § 16 (1) AnzV	Finanzen / Rechnungswesen	x	x																							1			
133	Anzeigepflicht für gemischte Finanzholding-Gesellschaften (In-und Ausland)	§ 24 Abs. 3a S. 4 u. 5 KWG / § 64g (3) Nr. 2 KWG / § 16 (1) AnzV	Finanzen / Rechnungswesen	x	x																							2	20061101131724 8	< 100	
134	Im Inland und im Ausland: jährliche Sammelanzeige	§ 24 (3a) S. 2 u. 5 KWG / § 64g (3) Nr. 2 KWG / § 16 (1) AnzV	Finanzen / Rechnungswesen	x	x																							2	20061101131724 7	< 100	
135	Bestellung einer Person für Geschäfte der (gemischten) Finanzholding	§ 24 (3a) S. 1 Nr.1 KWG / § 24 (3a) S. 5 KWG / § 64g (3) Nr. 1a u. b KWG / § 16 (2) AnzV	Finanzen / Rechnungswesen	x	x																							3	20061101131724 2, 20061101131724 3, 20061101131724 4	13	
136	Ausscheiden einer solchen Person	§ 24 (3a) S.1 Nr. 2 KWG / § 24 (3a) S. 5 KWG	Finanzen / Rechnungswesen	x	x																							1	20061101131724 5	< 100	
137	Nur für Finanzholding- Gesellschaften: Änderung der Struktur der Gruppe	§ 24 (3a) S.1 Nr. 3 KWG	Finanzen / Rechnungswesen	x	x																							1	20061101131724 6	< 0,5	

M1 ID	M2 Name der PRK	M3 Gesetzliche Anspruchsgrundlage	M4 Wertschöpfungs-Cluster (Bankensektor)	M6 Involvierte Akteure (Verwaltung)																M15 prozessketten- browser Generation (Farbe: 1 = rot, 2 = gelb, 3 = grün)	M16 IP-Identnummer (SKM-DB)	M17 Kosten in T Euro (SKM-DB)				
				BaFin	Bundesbank	Stat. Bundes- und Landesämter Arbeitsgericht / Insolvenzgeric h IFZ	Bundes- und Landeskriminal amt (ggf. noch Staatsanwaltschaft Bankverlag	Krankenkassen	Umlagekasse (UZ) bei den gesetzlichen Krankenkassen)	Deutscher Rentenversicherungs- bund Bundesagentur für Arbeit	Finanzamt	Grundbuchamt / Notariat	Bundesanzeiger	Förderinstitute	Einwohnermeldeamt	Verwaltungs- Berufsgenossenschaft	Arbeitschutz	Integrationsamt	Familienkasse							
138	Angemessene Eigenmittelausstattung	§ 10b Abs. 2 S. 2 KWG / §§ 8, 9 FkSoLV	Finanzen / Rechnungswesen	x	x																			3	2006110113160126	< 500
139	Wahl/Wechsel der Methode zur Eigenmittelberechnung	§ 10b Abs. 3 S. 4 KWG / § 2 Abs. 2 FkSoLV	Finanzen / Rechnungswesen	x	x																			1	2006110113160128	Nullmessung!
140	Ausgleich der Negative Differenz anhand Finanzkonglomerat-Solvabilität	§ 3 Abs. 6 S. 1 FkSoLV	Finanzen / Rechnungswesen	x	x																			1		
141	Bedeutende Risikokonzentration auf Konglomeratsebene	§ 13b Abs. 1 KWG / § 64g Abs. 1 Nr. 1 KWG	Finanzen / Rechnungswesen	x	x																			1	2006110113211314	< 100
142	Gruppeninterne Transaktionen innerhalb des Finanzkonglomerats	§ 13 b Abs. 1 KWG / § 64g Abs. 1 Nr. 1 u. 4 S. 2 KWG	Finanzen / Rechnungswesen	x	x																			1	2006110113211317, 2006110113211318	< 500
143	Verstoß gegen Risikokonzentrationen und gruppeninterne Transaktionen	§ 13d (4) S. 4 KWG	Finanzen / Rechnungswesen	x	x																			1	2006110113184310	< 0,5
144	Risikokonzentrationen aus Versicherungsrisiken	§ 64g (1) Nr. 2 KWG	Finanzen / Rechnungswesen	x	x																			1	2006110113211310	< 100
145	Kombinationen und Wechselwirkungen zwischen einzelnen Risikoarten	§ 64g (1) Nr. 3 KWG	Finanzen / Rechnungswesen	x	x																			1	2006110113211310	< 100
146	Anzeige der konglomeratsangehörigen Unternehmen im Ausland	§ 12a (3) KWG / § 12a (1) S. 3 KWG / § 7 (1) AnzV	Finanzen / Rechnungswesen	x	x																			1		
147	Elektronischer Datenaustausch im Mahnverfahren		Abwicklung (Marktfolge)																					1		
148	Elektronische Auskunft über Insolvenzbekanntmachungen	Insolvenzordnung	Abwicklung (Marktfolge)																					1		

M1 ID	M2 Name der PRK	M3 Gesetzliche Anspruchsgrundlage	M4 Wertschöpfungs-Cluster (Bankensektor)	M6 Involvierte Akteure (Verwaltung)																		M15 prozessketten- browser Generation (Farbe: 1 = rot, 2 = gelb, 3 = grün)	M16 IP-Identnummer (SKM-DB)	M17 Kosten in T Euro (SKM-DB)						
				BaFin	Bundesbank	Stat. Bundes- und Landesämter Amtsgericht / Insolvenzgeric ht PEB	Bundes- und Landeskriminal amt (ggf. noch Staatsanwälte, Bankvertr	Krankenkassen	Umsatzsteuer (Uz) bei den gesetzlichen Krankenkassen Dt.	Rentenversich erung Bundesagentur für Arbeit	Finanzamt	Grundbuchamt / Notariat	Bundesanzeiger	Förderinstitute	Einwohnermeld eamt	Verwaltungs- Berufsenosse nschaft	Arbeitschutz	Integrationsam t	Familienkasse											
149	Meldung über die Abtretung von Lebensversicherungs-an sprüchen	§ 29 ESiDV	Abwicklung (Marktfolge)														x										1	20060717100559 1	222	
150	Beratung und Beantragung von Fördermitteln		Abwicklung (Marktfolge)																	x								1		
151	Bezug von Informationen zu Handelsregistereintragungen	Abgabenordnung	Abwicklung (Marktfolge)																	x								1		
152	Bezug von Jahresabschlußdaten von Unternehmen	§ 18 KWG	Abwicklung (Marktfolge)																	x								1		
153	Grundbuchauskunft, Grundschuldbestellung, Grundschuldlöschung		Abwicklung (Marktfolge)																		x							1		
154	Erbfallmeldung	§ 33 ErbStG i.V.m. § 5 ErbStDV	Abwicklung (Marktfolge)																	x								1		

Anhang II – Werkzeuge für Prozessketten

Modul A "eGOV-Rechner"	1
Modul A Industrialisierungs-Quick-Check für Banken ("IQC")	3
Submodul E "Betreibermodell und Changemanagement"	7
Modul B "IT-Architektur und IT-Governance für Prozessketten"	9
Modul C "IT-Sicherheitsmechanismen und Regelwerke für Prozessketten"	32
Modul D "Die rechtssichere Prozesskette"	46

Modul A "Industrialisierungs-Quick-Check für Banken (IQC)"

Innovationsforum »Bank & Zukunft«

 **Fraunhofer**
IAO

»Industrialisierungs- Quick -Check«

1. Ausgewählte strategische Optionen und Prozesse

[Strategische Zukunfts-Optionen für Banken](#)

[Übersicht Industrialisierungsbereiche und Prozesse](#)

2. Prozess-Score-Werte

[Liste der Prozess-Score-Werte](#)

3. Prozess-Bewertung

[Durchführung Industrialisierungs-Quick-Check](#)

[Ermittlung GAP ZIEL-IST Stand bezüglich Industrialisierung](#)

5. Thesen / Aussagen

[Ergebnis der Einzelbewertungen im Überblick](#)

[Strategische Maßnahmen](#)

© Fraunhofer IAO, Stuttgart

Modul A "Industrialisierungs-Quick-Check für Banken (IQC)"

[zurück zur Übersicht](#)
Industrialisierungs-Quick-Check



Zentrale Fragestellung:

In welchen Bereichen möchten Sie gut sein und In welchen Bereichen möchten Sie exzellent sein?

Strategische Option / Business Modell	Einschätzung der Bedeutung	Geschäftsprozesse / Organisationsbereiche	Teilprozesse	Relevanz	beanspruchte Kapazität
				0 = nicht relevant 1 = gering 2 = mittel 3 = hoch 4 = sehr hoch	0 = nicht bedeutend 1 = geringer Kapazitätsbedarf Volumen 2 = mittlerer Kapazitätsbedarf 3 = hoher Kapazitätsbedarf 4 = sehr hoher Kapazitätsbedarf
Vertriebsbank	64%	Private Immobilienfinanzierung	Kundenberatung / -beurteilung durchführen	1	1
			Kreditantrag bearbeiten	1,5	1,5
			Kreditvertrag erstellen	3	4
			Kreditantrag genehmigen und Kundenunterschrift einholen	4	3
			Kreditvertrag bearbeiten	2	2
			Bonitätsunterlagen auswerten	3	3
			Rückständigkeit bearbeiten	4	1
			Darlehensvertrag auflösen	3	4

Modul A "Industrialisierungs-Quick-Check für Banken (IQC)"

Prozess-Score-Werte



Stufen		Kundenberatung / -beurteilung durchführen				
		IST Wert		ZIEL- Werte		Differenz zwischen ZIEL- und IST- Wert
Stufen	Prozessdefinition	Bewertungs-ergebnis (%)	Bewertungsergebnis in Punkten	Bewertungs-ergebnis (%)	Bewertungsergebnis in Punkten	
1	Geschäftsprozesse sind identifiziert und dokumentiert 1.1 Geschäftsprozess ist identifiziert 1.2 aktuelle Prozessroadmap liegt vor 1.3 Teilprozesse sind dokumentiert 1.4 Input/ Output/ Prozessschritte der Teilprozesse sind dokumentiert	66%	2,48	66%	2,48	0%
		10%	0,38	20%	0,75	10%
		25%	0,94	45%	1,69	20%
		20%	0,75	100%	3,75	80%
2	Prozessverantwortung Für GP und ihre Teilprozesse sind Prozessverantwortliche ernannt	100%	3,75	100%	3,75	0%
	2.1 Prozessverantwortlicher ist festgelegt	100%	3,75	100%	3,75	0%
	2.2 Teilprozessverantwortliche sind festgelegt	0%	0,00	66%	2,48	66%
	2.3 Geschäftsprozessverantwortlicher hat ausreichend Befugnisse und Kompetenzen (Personal, Budget)	0%	0,00	66%	2,48	66%
	2.4 Teilprozessverantwortliche hat ausreichend Befugnisse und Kompetenzen (Personal, Budget)	0%	0,00	66%	2,48	66%
3	Prozessmessung Die Leistung der GP wird regelmäßig anhand von Messgrößen gemessen	0%	0,00	0%	0,00	0%
	3.1 Messgrößen sind für Geschäftsprozess definiert	0%	0,00	0%	0,00	0%
	3.2 Messgrößen sind für alle Teilprozesse definiert	0%	0,00	0%	0,00	0%
	3.3 Messgrößen werden regelmäßig erfasst	0%	0,00	0%	0,00	0%
	3.4 Messergebnisse werden regelmäßig ausgewertet	0%	0,00	0%	0,00	0%
	3.5 Verbesserungsmaßnahmen werden durchgeführt	0%	0,00	0%	0,00	0%
4	Definition Prozessziele Es werden systematisch Zielgrößen für die GP festgelegt	40%	1,60	40%	2,00	0%
	4.1 Zielgrößen sind für Geschäftsprozesse festgelegt	50%	2,00	75%	3,75	25%
	4.2 Verbesserung / Optimierungspotentiale sind pro Geschäftsprozess definiert und budgetiert	0%	0,00	24%	1,20	24%
	4.3 Effizienzbarrieren sind ermittelt (und finanziell bewertet)	50%	2,00	65%	3,25	15%
	4.4 Aktueller Maßnahmenplan zur Realisierung liegt vor	0%	0,00	0%	0,00	0%
	4.5 Effizienzpotentiale liegen vor	0%	0,00	0%	0,00	0%
5	Kontrolle Zielerreichung Die Zielerreichung der GP wird regelmäßig überwacht und in Prozessbereichen ausgewiesen	25%	0,71	75%	3,00	50%
	5.1 Aktuelle (und vollständige) Cockpit-Charts liegen vor	5%	0,14	25%	1,00	20%
	5.2 Maßnahmen zur Zielerreichung sind festgelegt	5%	0,14	10%	0,40	5%
	5.3 Maßnahmen zur Zielerreichung sind umgesetzt	5%	0,14	10%	0,40	5%
	5.4 Ein positiver Trend der Kennzahl in Richtung Zielerreichung ist nachgewiesen	5%	0,14	15%	0,60	10%
	5.5 Ursachen für negative Trends sind bekannt	5%	0,14	10%	0,40	5%
	5.6 Maßnahmen zu deren Beseitigung sind in Umsetzung	5%	0,14	10%	0,40	5%
	5.7 Aktuelle Übersicht über Effizienzbarrieren liegen vor	5%	0,14	10%	0,40	5%
6	Prozessverbesserung Die Geschäftsprozesse werden laufend verbessert	0%	0,00	5%	0,20	5%
	6.1 Prozess-Team arbeitet regelmäßig	0%	0,00	5%	0,20	5%
	6.2 In Engpass-Beseitigungs-Teams sind mehr als 30 % der Mitarbeiter des Prozesses integriert	0%	0,00	5%	0,20	5%
	6.3 (Six Sigma) Verbesserungs-Teams sind etabliert und arbeiten regelmäßig	0%	0,00	0%	0,00	0%
	6.4 (Six Sigma) Verbesserungs-Fortschritt wird verfolgt (Visualisierung, Review)	0%	0,00	0%	0,00	0%
	6.5 Prozessverbesserungen sind nachweislich realisiert	0%	0,00	0%	0,00	0%
7	Managementunterstützung Das Management wertet regelmäßig die Prozessberichte aus und unterstützt aktiv Prozessverbesserungen	20%	1,20	20%	1,20	0%
	7.1 Management-Team tagt regelmäßig mit allen GP-Verantwortlichen	25%	1,50	25%	1,50	0%
	7.2 Cockpit-Charts werden im Management-Team analysiert und Maßnahmen werden umgesetzt	0%	0,00	0%	0,00	0%
	7.3 Geschäftsleitung treibt aktiv die GP-Verbesserung voran (Nachweise)	0%	0,00	0%	0,00	0%
	7.4 Geschäftsleitung tritt sichtbar als Treiber der Prozessverbesserung auf	0%	0,00	0%	0,00	0%
	7.5 Es werden Veränderungen zu einer prozessorientierten Organisation eingeleitet	0%	0,00	0%	0,00	0%

Bewertungsmodell für Scorewerte

Stufen	Scorewerte	IST Werte		Ziel Werte	
		Bewertungs-ergebnis (%)	Erreichte Punktzahl	Zielwert %	angestrebte Punktzahl
1	Prozessdefinition	30%	4,54	58%	8,66
2	Prozessverantwortung	50%	7,50	83%	12,45
3	Messung Prozessleistung	0%	0,00	0%	0,00
4	Definition Prozessziele	28%	5,60	51%	10,20
5	Kontrolle Zielerreichung	8%	1,57	31%	6,20
6	Prozessverbesserung	0%	0,00	3%	0,60
7	Managementunterstützung	9%	2,70	9%	2,70

Gesamtpunktzahl

Geschäftsprozesse

22

41

Erfüllungsgrad

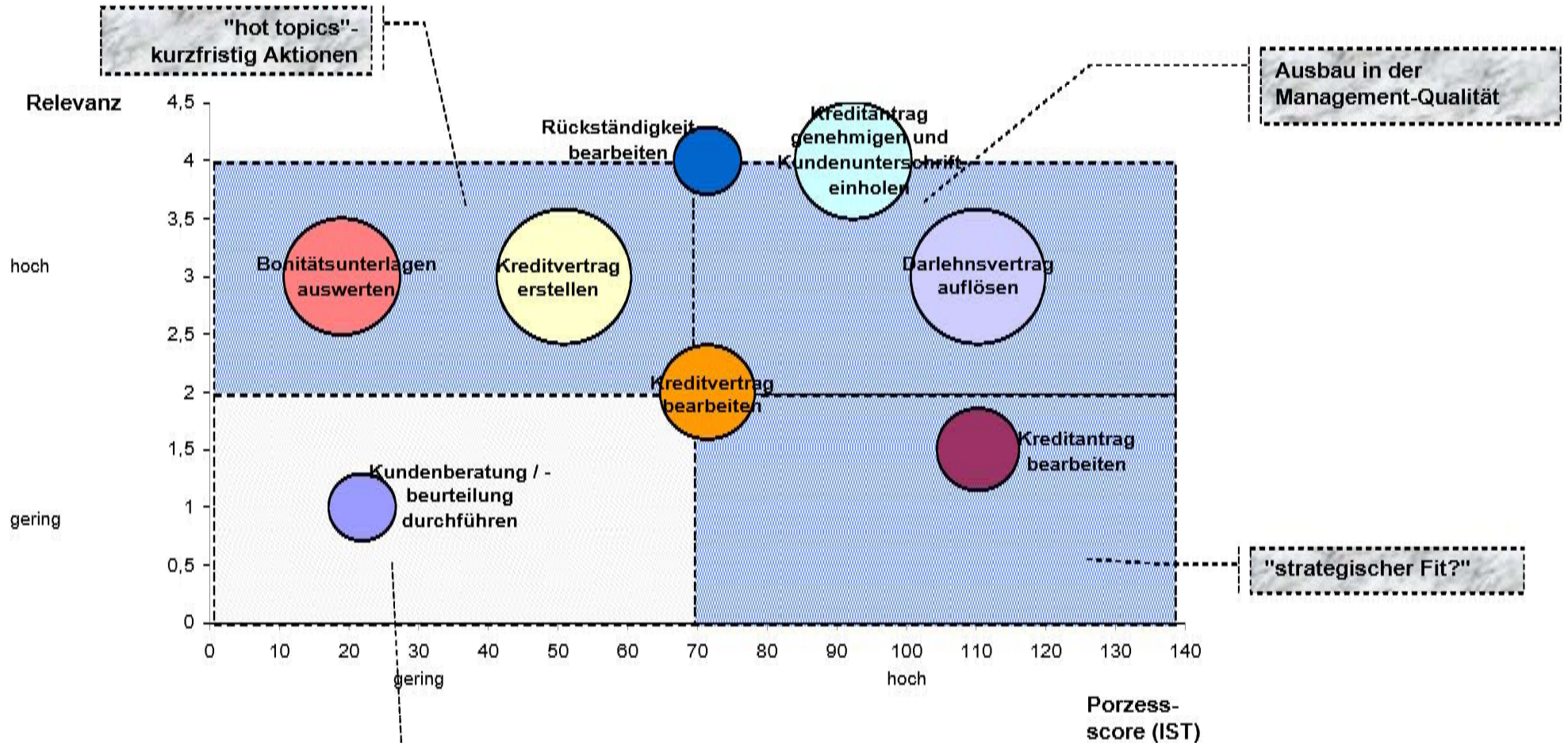
Geschäftsprozesse

16%

29%

Modul A "Industrialisierungs-Quick-Check für Banken (IQC)"

Ableitung strategischer Optionen



Legende:
 x-Wert = IST-Score des Prozesses
 y-Wert = Relevanz des Prozesses
 Bubble-Größe = Kapazitätsbedarf

Submodul E "Betreibermodell und Changemanagement"

Die Vielzahl von Betreibermodellen können anhand der in der nachfolgenden Tabelle beschriebenen Ausprägungsformen klassifiziert, beschrieben und gestaltet werden.

Nach der Systematik eines "Morphologischen Kastens" lassen sich die alternativen Merkmalsausprägungen (Spalte) je Betreibermodell-Kriterium (Zeile) mit einer einzuzeichnenden Linie zu einem spezifischen, gewünschten Betreibermodell verbinden.

Kriterium	Merkmalsausprägungen			
Leistungsfokus	Produkt	Produkt und Dienstleistung	Dienstleistung	
Organisationsform	Eigene privatwirtschaftliche Organisation bzw. Organisationseinheit	Gemeinschaftsunternehmen privatwirtschaftlich (z.B. Shared Service Center)	Gemeinschaftsunternehmen öffentlich (z.B. PPP, Shared Service Center)	Öffentliche Einrichtung
Koordinationsform	Hierarchisch	Gemischte Koordinationsform	Marktmechanismus	
Kundenfokus	Einzelkunde	Kundengruppe (branchenspezifisch)	Kundengruppe (branchenübergreifend)	
Gegenstand	Funktionen	Geschäftsprozess	Prozesskette	
Leistungsverrechnung	Umlageverfahren	Direkt	Produkt- / Leistungsorientiert	
Preismodell	Fixbetrag pro Zeiteinheit (Flatrate) (z.B. Euro pro Monat)	Fixer Grundbetrag plus nutzungsabhängiger Aufschlag	Rein nutzungsabhängiges Entgelt (pay-per-use)	
Absatzmarkt	Kein Zugang	Beschränkter Zugang	Freier Zugang	
Kontrahierungsform	Kontrahierungszwang	Kontrahierungsangebot	Wettbewerb	
Center-Konzept	Costcenter	Servicecenter	Investmentcenter	Profitcenter
Mitarbeiterinnen und Mitarbeiter	Mitarbeiterinnen- und Mitarbeiterkompetenzen evaluieren und weiter entwickeln			
Recht	Rechtliche Rahmenbedingungen berücksichtigen			

Modul B "IT-Architektur und IT-Governance für Prozessketten"

1.1 Die Datenerhebung

1.1.1 Das Ziel der Datenerhebung

Ziel der Datenerhebung ist es, zwischen mehreren Parteien die IT-Zusammenarbeit für gemeinsame Prozessketten zu optimieren. Unterziele und die zugehörigen Maße sind in den folgenden Tabellen zusammengestellt.

Ziel	Maß
IT1. Realisierung eines hohen Grad an IT-Unterstützung Ein hoher Grad an IT-Unterstützung verspricht für viele Prozesse eine Verbesserung der Effektivität und damit auch eine schnellere Abwicklung und eine Kostenreduktion.	Gemessen wird dieses Ziel am Automatisierungsgrad, an der Anzahl der IT-unterstützten Prozesse/Prozessschritte und an gemessenen Zeiten und Kosten (einschließlich der Aufwendungen für die IT).
IT2. Orientierung der technische Dienste an den Geschäftsprozessen Nur wenn die unterstützenden Dienste im Kontext der Geschäftsprozesse, ihren Schritten und auf deren Abstraktionsebene konzipiert sind, besteht die Möglichkeit die Prozesse und die IT-Anwendungen evolutionär zu verändern. Wenn die obersten IT-Komponenten und Dienste nur technisch nach implementationsnahen Gesichtspunkten zugeschnitten sind, werden in der Regel Prozessänderungen tiefere technische Änderungen erfordern.	Gemessen wird dieses Ziel an der Anzahl der Dienste, die keine Unterstützung eines Geschäftsprozess anbieten bzw. deren Funktionalität nicht mit dem Bedarf der zugeordneten Prozessschritte übereinstimmt.
IT3. Kompatibilität der IT-Anwendungen	Gemessen wird dieses Ziel an der

Ziel	Maß
<p>optimieren Das Zusammenspiel nicht kompatibler Anwendungen setzt immer zusätzliche Transformatoren voraus. Wo diese fehlen, ist keine Zusammenarbeit möglich. Jede Inkompatibilität reduziert das Verständnis der Vorgänge und der Bedeutung der auszutauschenden Daten zwischen den Partnern und kann zu Missverständnissen führen. Jede zusätzliche Transformation reduziert die zu erzielende Effektivität.</p>	<p>Anzahl der Medienbrüche und der Anzahl der nur technisch bedingten Transformationen (zwischen Protokollen und Datenschemata)</p>
<p>IT4. Kompatibilität zum SAGA-Standard (Bundesverwaltung) ausbauen Dieser Standard (BMI 2008a) gilt zwar nur für die Bundesverwaltung, er bietet aber auch allen anderen Parteien, besonders wenn sie mit der Bundesverwaltung zusammenarbeiten wollen, eine gute Vorlage für die zu entwickelnde IT-Infrastruktur.</p>	<p>Gemessen wird dieses Ziel an der Anzahl der nicht SAGA-konformen Objekte (Prozessmodelle, Datenmodelle, technische Standard und Architekturmuster)</p>
<p>IT5. Nutzung offener Standards ausweiten Eine grundlegende Forderung auch in SAGA ist die Forderung der Verwendung offener Standards und von Lösungen, für die die Gewährung von Lizenzen sicher ist, um Abhängigkeiten und Gefahren proprietärer Lösungen zu vermeiden.</p>	<p>Gemessen wird dieses Ziel an der Anzahl der verwendeten, aber nicht offenen Artefakte</p>

Tabelle 1: Übersicht der Unterziele und Maßnahmen

1.1.2 Gegenstand, Granularität und Vorgehen

Der Startpunkt des Vorgehens ist die Erhebung der an der Prozesskette beteiligten IT-Komponenten. Betrachtet werden alle Prozessketten, Prozesse oder Prozessschritte (im Folgenden Prozessbaustein genannt), die mehrere Parteien (z.B. Bank, Staat; Bürgerinnen und Bürger, Unternehmen) einschließen.

Am Anfang können einige Fragen bezüglich IT-Entwicklungsumgebung und Beschreibungssprachen gestellt werden (siehe Tabelle 2). Wichtiger sind die Fragen zur strategischen Ausrichtung der Institution (Tabelle 3).

Danach sind folgende Schritte auszuführen:

- 1 Die Abbildung der Geschäftsprozessarchitektur auf die Softwarearchitektur vornehmen (Tabelle 4).
Die IT-Komponenten sind Fachanwendungen (oder Module davon) oder technische Infrastrukturkomponenten (d. h. betrachtet werden Globale Architektur, Unternehmens-Architektur, System-Architektur nach (KBSt 2007) S. 5) und deren Schnittstellen.
- 2 Die Schnittstellen zwischen den Fachanwendungen beschreiben.
In der Granularität der ersten Erfassung sollten die Schnittstellen der Prozessbausteine noch mit denen der Fachanwendungen identisch sein (siehe Tabelle 5).
- 3 Die Modellierung mit Hilfe der Methoden der "Softwarekartographie" (LA 2005) und der "Fundamental Modeling Concepts (FMC)" ausführen.
Hier sind erste Schwachstellen feststellbar.
- 4 Für genauere Aussagen sind die Eigenschaften der relevanten Schnittstellen und Anwendungen zu erfassen (Tabelle 6 und Tabelle 7).
Alle technologischen Architekturfragen sind natürlich nur im Zusammenhang mit den ermittelten wirklich relevanten Prozessen von Bedeutung.

Die Tabellen 3 bis 6 sind mit jeweils einer Beispiel-Zeile bzw. Spalte vorbelegt, um die Fragen anschaulicher zu machen.

Die Tabellen 2 bis 4 oder 5 stehen in engem Zusammenhang mit dem Modul A und können dort in die Fragebögen mit integriert werden.

1.1.3 Begriffe

- Ein **Fachverfahren** ist die Gesamtheit aller organisatorischen Anweisungen und Abläufe (manuell, elektronisch) zu einem bestimmten Zweck nach fachlichen Gesichtspunkten.
- Eine **Fachanwendung** ist eine IT-Anwendung, die ursprünglich zur Unterstützung eines Fachverfahrens entwickelt wurde.
- Die **Schnittstelle** ist auf jeden Fall beschrieben durch die Klasse der Daten (z.B. Person, Konto, Buchung, ...). Eventuell bietet die Anwendung eine Funktion nach außen an (in SOA ein Service). Die Daten können in

- einem Format/Sprache (z.B. XML) nach einem internen Schema oder nach einem öffentlichen Standard ausgetauscht werden.
- **Rollen und Rechte** definieren, welche Personengruppen agieren mit welchem Auftrag, mit welchen Rechten (auflisten, lesen, hinzufügen, ändern) bzgl. welchen Daten oder Services der Anwendung.
 - Die **Programmsteuerung** zeigt an, wie starr ist der Kontrollfluss. Ist ein fester Algorithmus programmiert, wird ein Workflow-System, eine BPEL-Umgebung oder eine völlig freie Ereignissteuerung verwendet?
 - Mit der **Technologie** ist der Architekturansatz gemeint (z.B. Schichtenmodelle).
 - Die **Plattform** gibt an, welche Middleware eingesetzt wird.
 - **Benutzte Infrastruktur-Komponenten** sind nicht nur einer Fachanwendung zugeordnete Komponenten. Das sind in der Regel übergreifende fachnahe Komponenten, wie Loggingdienste, Druckdienste oder Dokumentenmanagement-Systeme, oder im ISO-Schichtenmodell unter der Anwendungsschicht liegende Komponenten wie FTP u.ä.
 - **Kommunikation/Vernetzung** bedeutet, in was für einem Netz (LAN, WLAN, Internet, Intranet) agiert die Anwendung. Ist dieses Netz ein virtuelles durch Hard- oder Software gesichertes Netz? Welche Protokolle nutzt die Anwendung (z.B. TCP/IP, SSH u.a.)?

1.2 Fragen zur IST-Erhebung der IT-Grobarchitektur

1.2.1 Allgemeine Fragen zur Modellierung

Frage	Antwort
Haben Sie ein Vorgehensmodell, mit dem Sie von den Prozessen die IT-Architektur ableiten? Welches?	
Setzen Sie für die Modellierung und Dokumentation der IT-Landschaft und Architektur Werkzeuge ein? Welche?	
Setzen Sie für die Abbildung der Geschäftsarchitektur auf die IT-Architektur Werkzeuge ein? Welche?	

Frage	Antwort
-------	---------

Tabelle 2: Allgemeine Fragen zur Modellierung

1.2.2 Fragen zur strategischen Ausrichtung

Frage	Antwort
-------	---------

Welche Bereiche befinden sich im Wandel?

Welche Bereiche werden ausgelagert?

Welche Bereiche würden durch zusätzliche elektronische Services den größten Nutzen haben?

Tabelle 3: Fragen zur strategischen Ausrichtung

1.2.3 Zuordnung der Prozesse zu den Anwendungen

Prozess Prozessschritt	Beteiligte Fachanwendung (bzw. Rolle der Mitarbeiterin und des Mitarbeiters bei manueller Bearbeitung)	Manuelle oder automatische Abwicklung	Organisation Abteilung
Basel II Meldung abgeben	BaFin-Extranet Server (MVP) BB ExtraNet Server Berichtssoftware (SAMBA)	M (manuell) HA (halbautomatisch) A (automatisch) AB (Änderungsbedarf)	

Tabelle 4: Zuordnung der Prozesse zu den Anwendungen

1.2.4 Fachanwendungen und deren Schnittstellen

Fachanwendung (bzw. Rolle der Mitarbeiterin und des Mitarbeiters bei manueller Bearbeitung)	Kurzbeschreibung	Verbundene Fachanwendung	Schnittstelle
Berichtssoftware (SAMBA)	Allgemeine Software für Generierung und versand von Basel II Berichten	BaFin-Extranet Server (MVP) BB ExtraNet Server	Beteiligungsanzeigen

Tabelle 5: Fachanwendungen und deren Schnittstellen

1.2.5 Eigenschaften der Schnittstelle

Schnittstelle	Beteiligungsanzeigen
Kommunikation	
Benutzte Infrastruktur-Komponenten (z.B. FTP-, LDAP-, http-, Web-, Server, Authentifizierungs-, Identifizierungs-Technologien)	HTTPS Webservice Nutzername/Kennwort Austausch von Zertifikaten
Vernetzung Verbindung, Protokoll	Internet TCP/IP, SSL

Schnittstelle	Beteiligungs- anzeigen
Richtung	Bidirektional
Datenmodell	
Objekte	Beteiligungsanzeige (Kunde, Konten, Transaktionen, ...)
Sprache, Schema, Standards	XML, XSD (siehe BB)
Services/angebotene Funk- tionen	
Rollen/Rechte	Anzeigender
Verfügbarkeit	Bürozeiten
Schutzbedarf	Hoch (sehr hoch)
Volumen je Zeit	
Medienbruch	Nein
Fehlende Kompatibilität	Nein
Manuelle Übertragung	Nein
Bemerkungen	

Tabelle 6: Eigenschaften der Schnittstelle

1.2.6 Eigenschaften der Anwendungen

Fachanwendung	Muster- anwen- dung_1
Betriebssystem	Solaris

Fachanwendung	Musteranwendung_1
Programmsteuerung (Fix, Workflow, BPEL)	Fix
Datenbank	Oracle 8
Technologie (Host, SOA, Altanwendung, 1/3/4-tier)	2-tier
Plattform (J2EE, .net)	keine
SAGA konform	Nein
Offene Standards	Nein
Bemerkung	Geschäftslogik im Client implementiert

Tabelle 7: Eigenschaften der Anwendungen

1.3 Allgemeine Hinweise zur Migration

Die Bewältigung des Migrationsprozesses stellt eine sehr individuelle, oft auch langfristige Aufgabe dar. Darum können hier nur einige kurze allgemeine Hinweise gegeben werden.

1.3.1 Analyse

Zur allgemeinen Schwachstellenanalyse sei auf die Veröffentlichungen aus dem Portfoliomanagement besonders auf SEBIS (Ernst et al. 2007) verwiesen. Das Primat haben die ökonomischen Bewertungen, erst danach kommen die oben genannten Ziele. Besonderes Augenmerk soll auf folgende Umstände gerichtet werden:

- keine oder mangelnde IT-Unterstützung für Prozessbausteine
- Medienbrüche
- fehlende Kompatibilität bei Protokollen, Sprachen und Datenschematas
- unterbrochener Programmfluss, der manuell überbrückt werden muss

Für die der Prozesskette zugrundeliegenden IT-Systeme sind Interoperabilität, Wiederverwendbarkeit und Flexibilität Kernanforderungen an die IT-Architekturen. Daher werden dienstorientierte Systeme und deren Architekturen (SOA) für die Konzeption solcher Systeme vorgeschlagen. Mit ihnen lassen sich kooperative Verwaltungs- und Prozessstrukturen aufbauen und IT-Systeme bzw. Fachanwendungen plattformunabhängig in eine Prozesskette integrieren (siehe auch Kapitel 5 in (KBSt 2007)). Für den Prozess der Analyse ist es notwendig, dass sich alle beteiligten Stakeholder aktiv beteiligen (Interviews, Workshops), wie es zum Beispiel in der Architecture Trade-off Analysis Method (ATAM) (Clements et al. 2001) beschrieben wird.

1.3.2 Optimierung

In der, der Analyse folgenden, Optimierung sind folgende Aspekte zu berücksichtigen:

Zum einen müssen die Anwendungen und Abläufe, die zusammengenommen eine Prozesskette bilden, von vorneherein mit geeigneten Sicherheitsmechanismen ausgestattet werden, beispielsweise zum Zugriffsschutz, zur Identifizierung oder zum Vertraulichkeitsschutz. Bereits beim Entwurf einer Prozesskette sind der jeweilige Sicherheitsbedarf und die erforderlichen Schutzmaßnahmen explizit zu berücksichtigen, einschließlich der dafür notwendigen Architektur/IT-Komponenten/Dienste.

Zum zweiten müssen die Sicherheitsmechanismen auch organisationsübergreifend wirken. Alle an einer praktizierten Prozesskette beteiligten Organisationen müssen gewährleisten können, dass erforderliche Sicherheitsmaßnahmen nicht umgangen und ausgehebelt werden können. Dies erfordert einen gemeinsamen Bezugsrahmen mit Mindeststandards zur organisatorischen, infrastrukturellen und technischen Sicherheit voraus, für die geeignete IT-Komponenten/Dienste in der Architektur vorgesehen werden müssen.

Zum dritten müssen die Frequenz und die Mengen der Informationsflüsse betrachtet werden, um eine geeignete wirtschaftliche skalierbare Architektur zu entwerfen.

Zum vierten ist zu beachten, dass Altsysteme vorhanden und eingebunden werden müssen und eine Vielzahl von Produkten im Einsatz sind. Ziel ist es durch den Einsatz von Standards und der Definition von Fassade-Interfaces nicht nur unterschiedliche Institutionen, sondern auch deren heterogenen

Infrastrukturen zu verknüpfen. Das soll eine wirtschaftliche Wiederverwendung bestehender Komponenten ermöglichen.

Zum fünften ist es wichtig, manuelle und elektronische Vorgänge miteinander zu verknüpfen um einen kontinuierlichen, sicheren Ablauf der Prozesse zu gewährleisten.

Die Referenzarchitektur orientiert sich am Architekturkonzept des Bundes und dem SAGA-Standard, speziell am Informationale und der Computational Viewpoint.

Zur Beschreibung von Dateien zum Datenaustausch und zur Definition von Schnittstellen für WEB Services wird im Wesentlichen die XML-Technologie verwendet. Konkrete semantische Modelle müssen eng mit den XÖV-Projekten (OSCI 2008) abgestimmt werden.

1.3.3 Realisierung

Nach der Optimierung der Prozesse und der daraus resultierenden Veränderung der groben Anwendungsarchitektur ist für jede Schnittstelle zu klären, liegt bereits eine Webservice Schnittstelle vor oder muss erst eine geschaffen werden.

Im ersten Fall muss man prüfen, ob Datenschema und Funktionsbeschreibung geändert wurden. Wenn ja, müssen die Realisierungen des Service angepasst werden.

Ist kein passender Webservice vorhanden, so ist zu prüfen, ob ein anderer Service schon vorhanden ist und ob die vorhandene Schnittstelle fachlich sinnvoll um die geforderte erweitert werden kann. Wenn nicht, so ist auf jeden Fall ein neuer Webservice zu schaffen, da aus Schutzgründen der Webservice in einer anderen Sicherheitszone als die Fachanwendung betrieben werden muss.

Der Webservice wird bei allen größeren Behörden oder FDL seine Aufgaben an ein Vorgangsbearbeitungssystem/Workflowsystem weiterleiten, das dann die Fachanwendung ansteuert. Diese inneren Schnittstellen sind ebenfalls anzupassen.

Eine wichtige Aufgabe ist es also, an allen Stellen von Inkompatibilitäten die Schnittstellen zu standardisieren bzw. sich auf einen Standard zu einigen.

Danach müssen die neuen Schnittstellen und Services bereitgestellt werden, bevor nicht mehr benötigte abgeschaltet werden können.

Für die Frage, was wird erweitert und was wird vollkommen neu entwickelt, bieten die ökonomischen Bewertungen des Nutzens der optimierten und automatisierten Prozesse einen Anhaltspunkt, aber die wichtigsten Entscheidungskriterien werden die Kosten- und Risiko-Abschätzungen zu den beiden Alternativen sein.

Webservices sind ausreichend, wenn ihre Funktionalitäten in die Fachanwendungen integriert werden. Wenn aber eine Nutzerin oder ein Nutzer mehrere nicht oder nur sehr locker miteinander verbundene Webservices gleichzeitig bedienen muss, so kann es sein, dass die Entwicklung einer integrierenden Fachanwendung zu aufwendig wäre, besonders wenn das mehrfach geschehen müsste. In dem Fall bietet sich an, eine integrierende Webanwendung (Webportal) zu schaffen, welche aus Portal-Plugins der einzelnen Webservices zusammengestellt wird. Hierfür ist es notwendig, dass zusammen mit dem Webservice das zugehörige Plugin entwickelt und bereitgestellt wird. Ein Beispiel dafür könnte die Fördermittelberatung im Rahmen einer Kreditberatung sein. Die Förderinstitute könnten jeweils allen Kreditbanken ihr Beratungsmodul bereitstellen.

Sehr detailreiche Hinweise zur Migration von bestehenden IT-Infrastrukturen und Anwendungen findet man unter anderem in (BMI 2008).

1.4 SAGA Check

Zum Prüfen der Konformität des Anwendungssystems wurde für die folgende Tabelle im wesentlichen das Kapitel 8 des Standards SAGA Version 4.0 (BMI 2008a) ausgewertet. Es ist je Punkt zu prüfen:

Ist der Punkt zutreffend für das System? Werden die geforderten Standards¹ eingesetzt oder werden andere benutzt?

¹ In der Tabelle werden nur die obligatorischen (O) und empfohlenen (E) Standards aufgeführt

Thema	Standard	Anwendungssysteme
4. Prozessmodellierung und Datenschutz		
Prozessoptimierung	Nach: E-Government-Handbuch, Kapitel III, Modul "Phase 3 – Analyse"	
	Weitere	
	andere	
Datenschutz	Nach: E-Government-Handbuchs, Kapitel II, Modul "Datenschutzgerechtes E-Government"	
	Weitere	
	andere	
5. Datenmodellierung	Die Internetbibliothek XRepository (https://www.xrepository.deutschland-online.de/xrepository/) der Bundesverwaltung wurde hinsichtlich verwandter Projekte untersucht, um ggf. bereits vorhandene Datenmodelle wieder zu verwenden.	
	Weitere	
	andere	
6. Software-Architektur		
Interoperabilität und Wiederverwendbarkeit	Wo möglich, werden EfA-Angebote (Dienste und Systeme) der Webseite http://www.cio.bund.de/cln_093/sid_6BB9127439618C262D55A	

Thema	Standard	Anwendungssysteme
	E87AC31B510/DE/IT-Angebot/it-angebot_node.html eingesetzt (siehe SAGA 4.0, Abschnitt 6.3.6). Die EfA-Angebote sind geprüft und die Entscheidung protokolliert.	
	Weitere	
	andere	
Allgemeine Anforderungen an Software-Architektur	Die Grundanforderungen an die Software-Architektur werden erfüllt (siehe SAGA 4.0, Abschnitt 6.1).	
	Weitere	
	andere	
Software-Architektur	Für die Entwicklung der Einheit wurde eine Vierschichtenarchitektur eingesetzt (siehe SAGA 4.0, Abschnitt 6.3.4).	
	Weitere	
	Andere	
7. IT-Service-Management und Infrastruktur		
IT-Service-Management	Als Grundlage für die Gestaltung, die Implementierung und das Management der IT-Steuerungsprozesse wird ITIL v2.0 genutzt (siehe SAGA 4.0, Abschnitt 7.1)	
	Weitere	
	andere	

Thema	Standard	Anwendungssysteme
Infrastruktur allgemein	Die Entwicklung einer Infrastruktur erfolgt auf der Basis von E-Government-Handbuch und IT-Grundschutzhandbuch (siehe SAGA 4.0, Abschnitt 7.2 bis 7.4).	
	Weitere	
	andere	
Zonenkonzept	Die Mindestanforderungen an ein Zonenkonzept nach SAGA 4.0, Abschnitt 7.2.2, werden erfüllt	
	Bei der Realisierung des Zonenkonzepts wurde ein Zugangskontrollsystem eingesetzt (siehe SAGA 4.0, Abschnitt 7.2.3).	
	Weitere	
andere		
8.1 IT-Sicherheitskonzeption		
8.1.1 Managementsysteme für Informationssicherheit	(O) BSI-Standard 100-1: Managementsysteme für Informationssicherheit (ISMS) v1.0	
	andere	
8.1.2 IT-Grundschutzvorgehensweise	(O) BSI-Standard 100-2: IT-Grundschutz-Vorgehensweise v1.0	
	Andere	
8.1.3 Risikoanalyse	(O) BSI-Standard 100-3: Risikoanalyse auf der Basis von IT-Grundschutz v2.0	

Thema	Standard	Anwendungssysteme
	Andere	
8.1.4 Umsetzung der Sicherheitskonzeption	(O) Industrial Signature Interoperability Specification – Mail-Trust (ISIS-MTT) v1.1	
	(O) BSI, IT-Grundschutz-Kataloge	
	(E) KoopA ADV, Handlungsleitfaden für die Einführung der elektronischen Signatur und Verschlüsselung in der Verwaltung v1.1	
	(E) BSI, E-Government-Handbuch	
	andere	
8.2 Prozessmodelle		
8.2.1 Technologien zur Prozessmodellierung	(O) Rollenmodelle und Flussdiagramme	
	(O) Unified Modeling Language (UML) v2.0	
	andere	
8.2.2 Austauschformate für Prozessmodelle	(E) XML Metadata Interchange (XMI) v2.x	
	andere	
8.3 Datenmodelle		
8.3.1 Technologien zur Datenmodellierung	(O) Entity Relationship Diagramme (ERD)	
	(O) Unified Modeling Language (UML) v2.0	
	andere	
8.3.2 Austauschformate für Datenmodelle	(O) XML Schema Definition (XSD) v1.0	

Thema	Standard	Anwendungssysteme
delle		
	(E) Regular Language Description for XML New Generation (Relax NG)	
	(E) XML Metadata Interchange (XMI) v2.x	
	andere	
8.3.3 Beschreibungssprachen für Metadaten von Dateien	(E) Resource Description Framework (RDF)	
	(E) Dublin Core (DC)	
	andere	
8.4 Applikationsarchitektur		
8.4.1 Applikationsarchitektur mit Middleware	(O) Java Platform, Enterprise Edition (Java EE) v5	
	(O) Java Platform, Standard Edition (Java SE) v5	
	andere	
8.4.2 Applikationsarchitektur ohne Middleware	(E) PHP: Hypertext Preprocessor (PHP) v5.x	
	andere	
8.5 Client		
8.5.1 Informationszugriff mit Computern	(O) Java Network Launching Protocol (JNLP) v1.5	
	andere	
8.5.2 Informationszugriff mit mobilen Endgeräten		

Thema	Standard	Anwendungssysteme
8.5.3 Informationszugriff durch externe Systeme		
8.5.4 Technologien zur Authentisierung	(O) BSI, E-Government-Handbuch, Modul "Authentisierung im E-Government"	
	(E) Security Assertion Markup Language (SAML) v2.0	
	andere	
8.6 Präsentation		
8.6.1 Barrierefreie Darstellung	(O) Barrierefreie Informationstechnik Verordnung (BITV)	
	andere	
8.6.2 Zeichensätze	(O) Unicode v4.x UTF-8	
	(E) Unicode v4.x UTF-16	
	andere	
8.6.3 Technologien zur Informationsaufbereitung	(O) Hypertext Markup Language (HTML) v4.01	
	(O) Multipurpose Internet Mail Extensions (MIME) v1.0	
	(O) Java Servlet v2.5	
	(O) Java Server Pages (JSP) v2.1	
	(E) Extensible Hypertext Markup Language (XHTML) v1.0	
	(E) Cascading Style Sheets Language Level 2 (CSS2)	
	(E) Extensible Stylesheet Language (XSL) v1.0	
	(E) Extensible Stylesheet Language Transformations (XSLT) v1.0	

Thema	Standard	Anwendungssysteme
	andere	
8.6.4 Aktive Inhalte	(O) ECMAScript Language Specification	
	andere	
8.6.5 Formulare		
8.6.6 Austauschformate für Daten	(O) Extensible Markup Language (XML) v1.0	
	andere	
8.6.7 Austauschformate für Dokumente	(O) Portable Document Format (PDF) v1.4	
	(O) Hypertext Markup Language (HTML)	
	(E) Portable Document Format (PDF) v1.5	
	(O) Text	
	(E) Open Document Format for Office Applications (OpenDocument) v1.0	
	(O) Comma-Separated Values (CSV)	
	(O) Industrial Signature Interoperability Specification - Mail-Trust (ISIS-MTT) v1.1, Teil 3	
	(O) XML Signature	
	(O) XML Encryption	
	andere	
8.6.8 Austauschformate für Bilder	(O) Graphics Interchange Format (GIF) v89a	
	(O) Joint Photographic Experts Group (JPEG)	
	(E) Portable Network Graphics (PNG) v1.2	

Thema	Standard	Anwendungssysteme
	(E) Tagged Image File Format (TIFF) v6.0	
	(E) Geo Tagged Image File Format (GeoTIFF)	
	andere	
8.6.9 Animation	(O) Animated Graphics Interchange Format (Animated GIF) v89a	
	andere	
8.6.10 Audio- und Videodaten	(E) Quicktime	
	(E) MPEG-4 Part 14 (MP4)	
	(E) Ogg Encapsulation Format (Ogg)	
	(O) Hypertext Transfer Protocol (HTTP) v1.1	
	andere	
8.6.11 Austauschformate für Geoinformationen	(E) Geography Markup Language (GML) v3.1.1	
	(E) Geography Markup Language (GML) v2.1.2	
	andere	
8.6.12 Datenkompression	(O) ZIP v2.0	
	(E) Gnu ZIP (GZIP) v4.3 / Tape ARchive (TAR)	
	andere	
8.6.13 Technologien für die Präsentation auf mobilen Endgeräten	(O) Short Message Services (SMS)	
	andere	

Thema	Standard	Anwendungssysteme
8.7 Kommunikation		
8.7.1 Middleware-Kommunikation	(O) Remote Method Invocation (RMI)	
	(O) Simple Object Access Protocol (SOAP) v1.1	
	(O) Web Services Description Language (WSDL) v1.1	
	(O) Java Message Service (JMS) v1.1	
	(O) J2EE Connector Architecture (JCA) v1.5	
	(E) Java Language Mapping to OMG IDL	
	(E) Web Services (WS)-Security v1.1	
	andere	
8.7.2 Netzwerkprotokolle	(O) Internet Protocol (IP) v4	
	(O) Domain Name System (DNS)	
	andere	
8.7.3 E-Mail-Kommunikation	(O) Simple Mail Transfer Protocol (SMTP) / Multipurpose Internet Mail Extensions (MIME) v1.0	
	(O) Post Office Protocol (POP) v3 / Internet Message Access Protocol (IMAP) v4rev1	
	(O) Industrial Signature Interoperability Specification - Mail-Trust (ISIS-MTT) v1.1, Teile 1 bis 6	
	andere	
8.7.4 IP-Telefonie	(E) H.323	

Thema	Standard	Anwendungssysteme
		andere
8.7.5 Anwendungsprotokolle	(O) File Transfer Protocol (FTP)	
	(O) Hypertext Transfer Protocol (HTTP) v1.1	
	(O) Online Service Computer Interface (OSCI)-Transport v1.2	
	(O) Transport Layer Security (TLS) v1.0	
	(E) Secure Shell v2 (SSH-2)	
	(E) WWW Distributed Authoring and Versioning (WebDAV)	
		andere
8.7.6 Geodienste	(E) Catalogue Services Specification v2.0 – ISO Metadata Application Profile v1.0	
	(E) Web Map Service Deutschland (WMS-DE) v1.0	
	(E) Web Coverage Service (WCS) v1.0	
	(E) Web Feature Service (WFS) v1.0	
	(E) Web Feature Service (WFS) v1.1	
	(E) Simple Feature Access – Part 2: SQL option (SFA-2) v1.1.0	
		andere
8.8 Backend		
8.8.1 Verzeichnisdienste und Registries	(O) Lightweight Directory Access Protocol (LDAP) v3	
		andere

Thema	Standard	Anwendungssysteme
8.8.2 Zugriff auf Datenbanken	(O) Java Database Connectivity (JDBC) v3.0	
	andere	
8.8.3 Zugriff auf Bestandssysteme	Siehe 8.7.1	
8.9 Verschlüsselung		
8.9.1 Asymmetrische Verschlüsselungsverfahren	(O) RSA	
	andere	
8.9.2 Symmetrische Verschlüsselungsverfahren	(O) Advanced Encryption Standard (AES)	
	andere	
8.10 Elektronische Signatur	(O) Kryptoalgorithmen nach Bundesnetzagentur für die elektronische Signatur	
	andere	
8.10.1 Hashen von Daten	(O) Secure Hash Algorithm (SHA)-256	
	(E) Secure Hash Algorithm (SHA)-224 / Secure Hash Algorithm (SHA)-384 / Secure Hash Algorithm (SHA)-512	
	andere	
8.10.2 Asymmetrische Signaturverfahren	(O) RSA	
	(E) Digital Signature Algorithm (DSA)	
	andere	
8.10.3 Key Management	(E) XML Key Management Specification (XKMS) v2	

Thema	Standard	Anwendungssysteme
	andere	
8.11 Smartcards		
8.11.1 Kontaktbehaf- tete Smartcards	(O) Identification Cards - Inte- grated circuit cards	
	andere	
8.11.2 Kontaktlose Smartcards	(O) Identification Cards – Con- tactless integrated circuit cards	
	andere	
8.11.3 Lesegeräte und Schnittstellen für Smartcards	(O) Technische Richtlinie für die eCard-Projekte der Bundesre- gierung (BSI TR- 03116) v1.0	
	(O) Industrial Signature Interop- erability Specification - Mail- Trust (ISIS-MTT) v1.1, Teil 7	
	Andere	
8.12 Langzeitarchi- vierung	(E) Tagged Image File Format (TIFF) v6.0	
	(E) Joint Photographic Experts Group (JPEG)	
	(E) Extensible Markup Langua- ge (XML) v1.0	
	(E) ArchiSig, Grundsätze für die beweiskräftige und sichere Langzeitarchivierung digital signierter Dokumente	
	(E) Portable Document Format Archive - 1 (PDF/A-1)	
	Andere	

Tabelle 8: SAGA Check

Modul C "IT-Sicherheitsmechanismen und Regelwerke für Prozessketten"

Checkliste nach ISO / IEC 27001/02

Standards zur Informationssicherheit liefern Kriterien für die Beantwortung der Frage, ob die Vorkehrungen, die eine Organisation zum Schutz ihrer geschäftskritischen Informationen getroffen hat, anerkannten Maßstäben genügt. Die nachfolgenden Tabellen enthalten eine Auswahl an Prüffragen, die aus der Norm ISO / IEC 27001 abgeleitet werden können.

Bereich 1 – Bedeutung der Informationssicherheit		Ja			
		Nein			
		nicht relevant			Bemerkungen
>> Leitlinie zur Informationssicherheit <<					
Die grundsätzliche Verantwortung für Informationssicherheit liegt bei der Leitung einer Organisation. Eine von ihr getragene Leitlinie zur Informationssicherheit (IS) ist eine wesentliche Voraussetzung für die Etablierung, Aufrechterhaltung und Weiterentwicklung eines Managementsystems zur Informationssicherheit.	Gibt es in der Organisation eine von der Leitung getragene, den Mitarbeiterinnen und Mitarbeitern sowie betroffenen Dritten bekannt gegebene sowie regelmäßig aktualisierte Leitlinie zur Informationssicherheit?				

Bereich 2 – Organisation der Informationssicherheit		Ja			
		Nein			
		nicht relevant			Bemerkungen
>> Organisatorische Sicherheitsmaßnahmen und Managementprozess <<					
Informationssicherheit erfordert ein geeignetes organisatorisches Umfeld mit geregelten Zuständigkeiten. Dazu gehört neben der aktiven Unterstützung der Unternehmensleistung eine möglichst	Wird die Sicherheit in der Organisation aktiv durch die Leitung unterstützt?				
	Sind die verschiedenen Bereiche und Abteilungen der Organisation angemessen an den zur Informationssicherheit gehörenden Steu-				

breite Beteiligung aller Organisationseinheiten am IS-Prozess sowie die Ernennung eines oder einer mit hinreichenden Befugnissen ausgestatteten IT-Sicherheitsbeauftragten als zentraler Koordinierungsstelle für die anstehenden Aufgaben.	erungsaufgaben beteiligt?				
	Ist eine zentrale Koordinierungsstelle (IT-Sicherheitsbeauftragte/r) für Fragen der Informationssicherheit eingerichtet?				
	Wird regelmäßig überprüft, ob die vorhandenen organisatorischen Vorkehrungen zur Informationssicherheit noch angemessen sind?				
	Gibt es in der Organisation systematische Prozesse zur Identifikation, Bewertung und Behandlung von Risiken für die Informationssicherheit?				
	Wird hinreichend darauf geachtet (zum Beispiel durch vertragliche Vorkehrungen), dass die Sicherheitsziele der Organisation nicht gefährdet werden, wenn Aufgaben an Fremdfirmen ausgelagert werden?				

Bereich 3 – Unternehmenswerte		Ja			
		Nein			Bemerkungen
>> Verantwortung und Klassifizierung von Informationswerten <<		nicht relevant			
Informationen über Kunden, Geschäftsverbindungen, Lieferanten, Produktionsabläufe und Details zur Leistungserbringung gehören ebenso zu den Werten einer Organisation wie die vorhandenen Sachwerte. Die Informationswerte sollten daher im Inventar einer Organisation berücksichtigt und ebenso wie die Sachwerte mit einer Sicherheitseinstufung (Schutzbedarf) versehen werden. Auf die Aktualität von Inventar und Schutzbedarfseinstufungen ist zu achten.	Gibt es in der Organisation ein Inventar, das neben den Sachwerten auch alle wichtigen Informationswerte enthält?				
	Enthält das Inventar Einstufungen zum Schutzbedarf bezüglich der Sicherheitsziele Vertraulichkeit, Verfügbarkeit und Integrität der verschiedenen Werte?				
	Sind für die im Inventar aufgeführten Informationswerte und deren Schutz Verantwortliche benannt?				

Bereich 4 – Personelle Sicherheit		Ja		
		Nein		
>> Erhöhung des Sicherheitsbewusstseins der Mitarbeiter <<		nicht relevant		
		Bemerkungen		
<p>Ein ausgeprägtes Sicherheitsbewusstsein der Mitarbeiterinnen und Mitarbeiter sowie ausreichende Kenntnisse sind wichtige Grundlagen für Informationssicherheit: Sicherheitsrelevante Fehler und Unaufmerksamkeiten werden eher vermieden und potenziell gefährliche Ereignisse rascher erkannt. Der Schulung und Sensibilisierung der Mitarbeiterinnen und Mitarbeiter kommt daher ein hoher Stellenwert zu.</p>	Werden die Mitarbeiterinnen und Mitarbeiter hinreichend auf die Sicherheitsziele der Organisation verpflichtet (z. B. durch Unterzeichnung von Vertraulichkeitsvereinbarungen)?			
	Finden regelmäßig Schulungen die Mitarbeiterinnen und Mitarbeiter sowie im Bedarfsfall an Mitarbeiterinnen und Mitarbeiter von Fremdfirmen Sicherheit statt?			
	Werden regelmäßig aktuelle Informationen zur Sicherheit an die Mitarbeiterinnen und Mitarbeiter sowie im Bedarfsfall an Mitarbeiterinnen und Mitarbeiter von Fremdfirmen ausgegeben?			
	Werden bei entsprechend hohen Sicherheitsanforderungen die Mitarbeiterinnen und Mitarbeiter einer Sicherheitsüberprüfung unterzogen?			
	Ist ein formales disziplinarisches Verfahren etabliert, das bei Sicherheitsverstößen angewendet wird?			
	Werden bei entsprechendem Bedarf die Mitarbeiterinnen und Mitarbeiter von Fremdfirmen auf die Sicherheitsziele der eigenen Organisation verpflichtet?			
	Ist geregelt, dass beim Ausscheiden oder der Versetzung von Mitarbeiterinnen und Mitarbeitern ausgehändigte Arbeitsausstattung und Dokumente zurückgegeben werden sowie Zugangsrechte entzogen werden?			

Bereich 5 – Physische und umgebungsbezogene Sicherheit		Ja		
		Nein		
		nicht relevant		

>> Physische Sicherheit und Zutrittsbeschränkungen <<					Bemerkungen
Es muss dafür gesorgt werden, dass der Zutritt zu den Räumlichkeiten einer Organisation sowie die Zugriffe auf deren Informations- und Kommunikationstechnik so kontrolliert werden, dass das Risiko von Beschädigungen, Diebstählen oder unsachgemäßer Anwendung gering gehalten wird.	Sind IT-Systeme, auf denen Informationen mit einem höheren Schutzbedarf gespeichert oder verarbeitet werden, in eigenen räumlichen Sicherheitszonen mit entsprechenden Zutrittskontrollen untergebracht?				
	Werden Zutritt und Zugang (von Mitarbeiterinnen und Mitarbeitern, Besuchern, Fremdfirmen) auf der Basis schriftlich festgelegter Regeln kontrolliert?				
	Werden besonders sensible Bereiche eher unauffällig präsentiert?				
Physischer Schutz gegen Zerstörung durch Feuer, Überschwemmung, Erdbeben, Explosionen, Unruhen und andere Formen durch Natur oder Mensch verursachter Katastrophen sollte geplant und angewendet werden. Der Verlust oder die Beschädigung von IT-Systemen oder anderen Geräten kann Geschäftsprozesse wesentlich behindern.	Sind Geräte vor Diebstahl, mutwilliger Zerstörung oder Beschädigung durch Katastrophen geschützt?				
	Sind Mitarbeiterinnen und Mitarbeiter auf einen sorgsamem Umgang mit den Geräten verpflichtet (z. B. ggf. Essen, Trinken oder Rauchen zu vermeiden)?				
	Sind die elektrischen Geräte vor Netzausfall und Überspannung geschützt?				
	Werden IT-Systeme, die bedeutsame Geschäftsprozesse unterstützen, durch eine unterbrechungsfreie Stromversorgung (USV) geschützt?				
	Ist ein Notstromaggregat vorhanden?				
	Werden USV-Geräte und Notstromaggregate regelmäßig auf Funktionsfähigkeit und ausreichende Kapazität getestet?				
	Ist eine Notbeleuchtung vorhanden, die sich bei Ausfall der Stromversorgung automatisch einschaltet?				
	Sind Gebäude und Gebäude mit Blitzschutzanlagen versehen?				
	Ist die Führung der Kabel für Daten, Telekommunikation und Energieversorgung gut dokumentiert und sicher (gegen Abhörungen und physische Beschädigung geschützt) ausgelegt?				
Mobile Geräte sind besonderen	Gibt es schriftlich festgelegte Regeln für den				

Bedrohungen ausgesetzt und müssen daher besonders geschützt werden.	Einsatz von IT-Systemen und geschäftskritischen Dokumenten außerhalb der Geschäftsräume (z. B. bei Telearbeit oder auf Dienstreisen)?				
Bei Außerbetriebnahme oder Reparatur von Datenträgern und IT-Systemen können vertrauliche Informationen bekannt werden.	Werden sensible Daten auf Speichermedien und in IT-Systemen vor einer Außerbetriebnahme, Reparatur oder Wiederverwendung zuverlässig gelöscht?				

Bereich 6 – Kommunikation und Betriebsablauf		Ja		
		Nein		
>> Netz- und Betriebssicherheit <<		nicht relevant		
		Bemerkungen		
Gut dokumentierte Geschäftsprozesse und schriftliche Arbeitsanweisungen (einschließlich der dabei erforderlichen Kommunikations- und Meldewege) tragen zu einem korrekten und sicheren IT-Betrieb bei.	Sind die Organisationsstrukturen, Geschäftsprozesse, Kommunikations- und Meldewege im Bereich der Informationsverarbeitung dokumentiert?			
	Gibt es schriftliche Arbeitsanweisungen zu diesen Prozessen (insbesondere auch zur Administration der IT-Systeme)?			
	Sind die Arbeitsanweisungen für die Betroffenen hinreichend verfügbar?			
	Sind die Verfahrensweisen zur Änderung von Arbeitsanweisungen dokumentiert?			
Durch eine Trennung von Aufgaben kann das Risiko des Missbrauchs von Berechtigungen erheblich gesenkt werden.	Wird auf eine Funktions- und Aufgabentrennung geachtet (z. B. unterschiedliche Zuständigkeiten bei der Durchführung und Kontrolle von Aufgaben)?			
In gleicher Weise kann durch die Trennung von Entwicklungs-, Test- und Produktionssystemen unbeabsichtigte und nachteilige Wechselwirkungen vermieden werden.	Werden unterschiedliche Systeme für Entwicklungsaufgaben, Test und Produktion eingesetzt?			
Schadsoftware (Viren, Würmer, trojanische Pferde, logische Bomben) kann massive Schadenswirkung entfalten. Maßnahmen zu ihrer Beseitigung gehen zu Lasten wertvoller Ressourcen des Unternehmens.	Werden die Benutzerinnen und Benutzer von IT-Systemen regelmäßig über Schadsoftware (Gefahren, Arten, Verbreitungswege) informiert und wissen sie, wie sich bei Verdacht auf Vorhandensein von Schadsoftware verhalten sollen?			
	Ist auf den IT-Systemen Virenschutzsoftware installiert und aktiviert?			
	Werden die installierten Schutzprogramme regelmäßig und in kurzen Abständen aktualisiert?			

Bereich 6 – Kommunikation und Betriebsablauf		Ja			
		Nein			
		nicht relevant			
		Bemerkungen			
>> Netz- und Betriebssicherheit <<					
	Gibt es schriftliche Regeln zur Beschränkung und zur Vorgehensweise beim Datenimport (von Datenträgern, aus dem Internet oder anderen Netzen)?				
	Gibt es Regelungen zum Schutz gegen schädliche aktive Inhalte (JavaScript, Java, ActiveX) und Plugins.?				
Insbesondere zur Vorsorge vor Schäden nach Betriebsstörungen müssen Integrität und Verfügbarkeit von Datenbeständen des Unternehmens gewährleistet sein. Voraussetzung dafür ist das Vorhandensein eines Datensicherungskonzepts, das alle wesentlichen Daten einbezieht.	Gibt es dokumentierte Verfahrensweisen für die Datensicherung?				
	Werden die Sicherheitskopien an einem sicheren Ort und vor dem unbefugten Zugriff durch Dritte geschützt aufbewahrt?				
	Wird regelmäßig getestet, ob die Datensicherung wie geplant funktioniert hat und Daten mit Hilfe der Sicherungskopien rekonstruiert werden können?				
Datenträger, die z. B. für Datensicherungszwecke eingesetzt werden, oder Dokumente enthalten sensible Informationen.	Gibt es schriftlich festgelegte Regeln für den Umgang mit vertraulichen Informationen in Dokumenten und auf Datenträgern (z. B. zu deren Aufbewahrung oder Entsorgung)?				
Auch bei der Kommunikation und dem Austausch von Informationen mit anderen Organisationen sind Sicherheitsanforderungen (insbesondere zur Vertraulichkeit) zu beachten.	Wird beim Austausch von Informationen mit anderen Organisationen auf die Einhaltung von Sicherheitsvorgaben geachtet?				
	Werden Datenträger, die zum Informationsaustausch benutzt werden, beim Transport hinreichend geschützt?				
	Sind Regeln für die sichere Nutzung von E-Mail definiert (z. B. zu)?				
	Sind Regeln für die sichere Nutzung von E-Commerce und anderen Webanwendungen definiert (z. B. Verwendung von SSL)?				
	Werden Systeme, die Ihr Unternehmen für die elektronische Außendarstellung nutzt (z. B. Webserver), besonders geschützt?				

Bereich 6 – Kommunikation und Betriebsablauf		Ja		
		Nein		
>> Netz- und Betriebssicherheit <<		nicht relevant		
		Bemerkungen		
	Wird sichergestellt, dass über diese Systeme keine Zugriffe auf das interne Netz und auf sensible Informationen möglich sind?			
	Gibt es ein allen Mitarbeitern bekanntes und geregeltes Verfahren für die Veröffentlichung unternehmensbezogener Informationen?			

Bereich 7 – Zugangskontrolle		Ja			
		Nein			
>> Sicherung der organisationsinternen Informationen <<		nicht relevant			
		Bemerkungen			
Die Möglichkeit zum Zugriff auf geschäftliche Informationen sollte nur insoweit möglich sein, wie dies fachlich erforderlich ist. Die Umsetzung dieser Anforderung setzt geeignete Konzepte für das Management von Zugangs- und Zugriffsrechten sowie die Kontrolle der erfolgten Zugriffe voraus.	Gibt es schriftlich fixierte Anforderungen und Vorgehensweisen für die Kontrolle des Zugangs zu Geschäftsinformationen?				
	Werden Berechtigungen, die einzelnen Benutzerinnen und Benutzern oder Benutzergruppen zur Erfüllung ihrer Aufgaben erteilt werden müssen, nach festgelegten Regeln vergeben und administriert?				
	Werden die Berechtigungen nach Erfüllung der Aufgaben wieder gelöscht?				
	Gibt es eine schriftliche Anweisung zum Umgang mit Passwörtern?				
	Wird die Umsetzung der Anweisung (z. B. mit technischen Hilfsmitteln) überprüft?				
	Wird die Notwendigkeit der erteilten Zugangsberechtigungen regelmäßig und anlassbezogen, z.B. bei Tätigkeitswechsel, überprüft?				
	Ist festgelegt, wie IT-Systeme am Arbeitsplatz zu schützen sind, wenn diesen (auch kurzzeitig) unbeaufsichtigt sind?				
	Sind Netzverbindungen, die von externen Stellen aus initiiert werden können (z. B. für Fernwartung oder Telearbeit), besonders gesichert?				
	Werden Zugriffe per Ferndiagnose oder Fernadministration einschließlich versuchter Zugriffe protokolliert?				
	Ist das Netz physisch und logisch so strukturiert, dass dies dem ggf. unterschiedlichen Schutzbedarf der Daten und Anwendungen im jeweiligen Segment entspricht?				

Bereich 8 – Entwicklung, Beschaffung und Wartung von IT-Systemen		Ja			
		Nein			
>> Systembeschaffung, -entwicklung und -wartung <<		nicht relevant			
		Bemerkungen			
Die Sicherheitsstrategie eines Unternehmens spiegelt sich auch in den IT-Systemen wider, die entwickelt, beschafft oder eingesetzt werden. Sicherheitsanforderungen an IT-Systeme, die aus der Sicherheitsstrategie des Unternehmens abgeleitet werden, sind dabei der Ausgangspunkt für die Auswahl neuer Produkte.	Werden bei der Beschaffung und Entwicklung von neuen IT-Systemen Sicherheitsanforderungen angemessen berücksichtigt?				
	Wird beim Betrieb von IT-Systemen darauf geachtet, dass die Korrektheit von Ein- und Ausgabedaten sowie Verarbeitungsfolgen und Systemmeldungen geprüft wird?				
	Gibt es für jedes IT-System eine festgelegte Soll-Konfiguration für die auf dem System laufende Software?				
	Wird regelmäßig kontrolliert, welche Software und in welcher Konfiguration auf den IT-Systemen installiert ist?				
	Gibt es in Ihrem Unternehmen schriftlich festgelegte Regelungen zur Durchführung von Software-Upgrades und anderen Software-Änderungen?				
Kryptographische Verfahren bieten bei sachgerechtem Einsatz Schutz vor dem Verlust der Vertraulichkeit von sensiblen Geschäftsinformationen. Sie können den Verlust der Integrität von Daten und deren Herkunft erkennen lassen.	Gibt es ein dokumentiertes Kryptokonzept				
	Werden vertrauliche Daten durch Verschlüsselung gegen Missbrauch geschützt?				
	Werden elektronische Signaturen zum Schutz der Integrität und zum Nachweis der Authentizität von sensiblen Daten angewendet?				
Um auf Schwachstellen von Informationssystemen schnell reagieren und angemessene Maßnahmen ergreifen zu können, ist eine frühzeitige Kenntnis solcher Schwachstellen sinnvoll.	Ist geregelt, wer für die Informationsbeschaffung im Bereich Systemschwachstellen zuständig ist?				
	Gibt es ein systematisches Patch-Management?				

Bereich 9 – Umgang mit Sicherheitsvorfällen		Ja			
		Nein			
>> Umgang mit Funktionsstörungen und Sicherheitsvorfällen <<		nicht relevant			
		Bemerkungen			
Geregelte Meldewege sind eine wesentliche Voraussetzung für die effektive und effiziente Reaktion auf Sicherheitsvorfälle.	Gibt es schriftlich festgelegte Regeln, wie Sicherheitsvorfälle und Auffälligkeiten (z. B. Funktionsstörungen von Software) zu melden sind?				
	Sind diese Regeln den Mitarbeiterinnen und Mitarbeitern bekannt gemacht worden?				
	Gibt es eine feste Anlaufstelle zur Meldung von Sicherheitsvorfällen?				
Es ist notwendig, dass Unternehmen schnell, effektiv und ordnungsgemäß auf Sicherheitsvorfälle reagieren. Dadurch wird das Ausmaß des Schadens begrenzt.	Ist in Ihrem Unternehmen ein Verantwortlicher für das Management von Sicherheitsvorfällen benannt?				
	Sind Verfahrensweisen zum Umgang mit Sicherheitsvorfällen etabliert?				
	Werden Sicherheitsvorfälle und deren Behandlung dokumentiert?				
	Gibt es schriftlich festgelegte Regeln, wie mögliche Beweismittel ermittelt und aufbewahrt werden?				
	Wird an der kontinuierlichen Verbesserung des Managements (Handhabung, Reaktion, Überwachung) von Sicherheitsvorfällen gearbeitet?				
	Wird die Durchführung dieser Maßnahmen vom Management kontrolliert?				
Die Kooperation mit anderen kompetenten Organisationen trägt zur Effektivität und Effizienz der Behandlung von Sicherheitsvorfällen bei.	Stehen Sie in Kooperation mit anderen Organisationen, um bei einem Sicherheitsvorfall schnelle Hilfe erhalten und entsprechende Maßnahmen zügig umsetzen zu können?				

Bereich 10 – Kontinuierlicher Geschäftsbetrieb		Ja		
		Nein		
		nicht relevant		
>> Notfallvorsorgeplanung <<				Bemerkungen
Um bei gravierenden Unterbrechungen, die organisationskritischen Geschäftsprozesse möglichst rasch wiederaufnehmen zu können, um schwerwiegende Schäden zu vermeiden und die Existenz der Organisation nicht zu gefährden, sind geeignete Vorsorgepläne für die relevanten Notfallszenarien erforderlich.	Gibt es Pläne, wie der Geschäftsbetrieb auch im Katastrophenfall möglichst reibungslos fortgeführt bzw. wiederaufgenommen werden kann?			
	Werden diese Pläne einer regelmäßigen Kontrolle auf Angemessenheit und Aktualität unterzogen?			
	Sind Notfallverantwortliche benannt?			
	Werden die Mitarbeiterinnen und Mitarbeiter regelmäßig über das Verhalten bei Katastrophen oder anderen schwerwiegenden Betriebsstörungen unterrichtet?			
	Wird das Verhalten im Katastrophenfall geübt?			
	Gibt es in Ihrem Unternehmen einen Benachrichtigungsplan für den Fall einer Katastrophe oder schwerwiegenden Betriebsstörung, der den Mitarbeiterinnen und Mitarbeitern bekannt ist?			

Bereich 11 – Gesetze, Normen und andere Richtlinien		Ja		
		Nein		
		nicht relevant		
>> Leitlinie zur Informationssicherheit <<				Bemerkungen
Der Betrieb von Informationstechnik ist in vielfältiger Weise durch externe Vorschriften (Gesetze, Normen, vertragliche Vereinbarungen etc.) geregelt. Durch geeignete Verfahren muss sichergestellt sein, dass diese Vorgaben auch tatsächlich eingehalten werden. Audits und Zertifizierungen können dazu beitragen, die Einhal-	Ist im Einzelnen dokumentiert, welche externen Anforderungen die Organisation erfüllen muss?			
	Gibt es schriftlich festgelegte Regeln, die gewährleisten, dass die Rechte zum Schutz geistigen Eigentums und anderer urheberrechtlich geschützter Objekte (einschließlich Software) eingehalten werden?			
	Ist ein Datenschutzbeauftragter (bzw. eine Datenschutzbeauftragte) ernannt worden?			

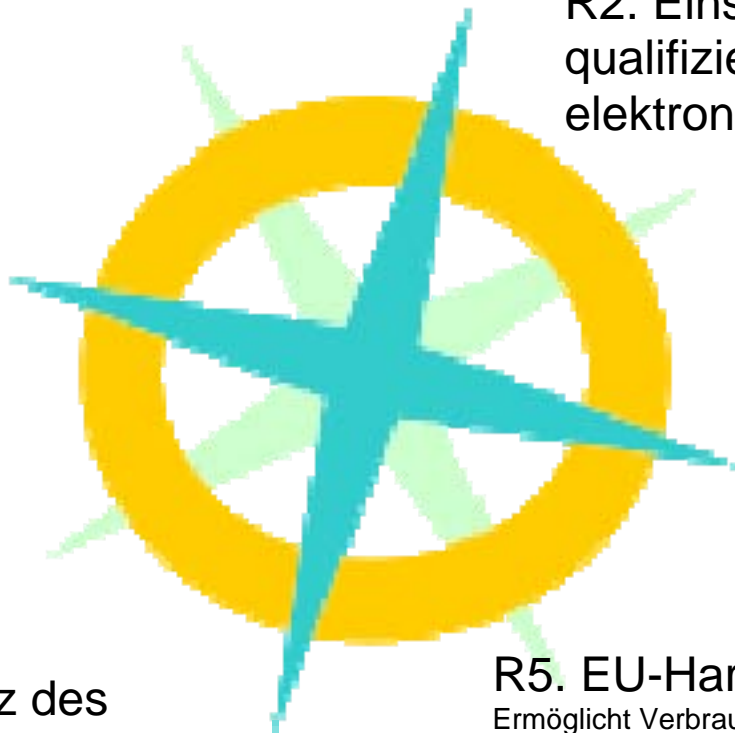
Bereich 11 – Gesetze, Normen und andere Richtlinien		Ja		
		Nein		
>> Leitlinie zur Informationssicherheit <<		nicht relevant		
		Bemerkungen		
tung geltender Vorschriften und Standards zu überprüfen und nach außen hin zu dokumentieren.	Werden die Belange des betrieblichen Datenschutzes (z. B. bei der Überwachung und Protokollierung) beachtet?			
	Werden die Belange des betrieblichen Datenschutzes (z. B. bei der Überwachung und Protokollierung) beachtet?			
	Werden die IS-Prozesse in der Organisation nach anerkannten Standards (ISO 27001, IT-Grundschutz) regelmäßig auditiert?			
	Sind die IS-Prozesse in der Organisation nach anerkannten Standards (ISO 27001, IT-Grundschutz) zertifiziert?			

Modul D "Die rechtssichere Prozesskette"

R1. Datenschutz:

Verbot jeglicher Vorratshaltung von personenbezogenen Daten

R2. Einsatz
qualifizierte
elektronische Signatur



R4. Einsatz des
elektronischen
Personalausweises (ePA)

R5. EU-Harmonisierung:

Ermöglicht Verbraucherkreditvertrag mit qualifizierter elektronischer Signatur (§ 492 BGB zukünftige Fassung)