

Grete/Held (Hrsg.)

DORA & Cloud-Sicherheit: Praxisleitfaden für Banken & IT-Dienstleister

**Wie Banken und IT-Dienstleister die neuen
regulatorischen Anforderungen meistern**

Annerose Debes

Leiterin IT-Compliance
Kreissparkasse Gelnhausen

Nico Frommholz

Director, Head of Payments
Hamburg Commercial Bank AG

Dr. Patrick Grete (Hrsg.)

Referat TK 22
Bundesamt für Sicherheit in der Informationstechnik (BSI)

Dr. Markus Held (Hrsg.)

Referent Informationssicherheit in der IT-Konsolidierung
Bundesamt für Sicherheit in der Informationstechnik (BSI)

Dr. Sibel Kocatepe

Referatsleiterin Referat CTF 3: Überwachung IT-MMDL und
kritische IKT-Drittdienstleister, IKT-Drittparteibeziehungen
Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin)

Tanja Monika Libiseller
Senior Manager Lead Cloud Technology
PPI AG

Thorsten Planeth
Head of IT Audit, Director

Immo Regener
Senior Manager
PwC Strategy& (Germany) GmbH

Philipp Schulz
Partner
Cyber Security for Financial Services
PricewaterhouseCoopers GmbH

Markus Vehlow
Partner
PricewaterhouseCoopers GmbH

Dr. Hubertus von Poser
Mitglied der Geschäftsleitung
Head of Consulting Payments
PPI AG

Florian Winterer
Wirtschaftsprüfer
Rechnungslegung/Kredit/Prüfungsmethodik
Genossenschaftsverband Bayern e. V.

Inhaltsübersicht

Vorwort	1
A. Von der Bank in die Cloud – eine Einführung zum Cloud Computing in der Finanzindustrie	3
B. Cloud Computing in der Finanzbranche – Eine Einleitung	25
C. Überwachung von IKT-Drittdienstleistern zwischen Abhängigkeit und Resilienz	37
D. Cloud-Computing in der Sparkassenpraxis: Chancen und Herausforderungen aus Sicht von IT-Organisation und Interner Revision	55
E. Prüfung von Cloud-Service-Providern im Rahmen eines Pooled Audits	105
F. Cloud-Dienste bei Kreditinstituten – von Einsatzbereichen bis zur Prüfung	135
G. Digitale Resilienz im Finanzsektor: IKT-Drittdienstleister aus dem Blickwinkel von IT-Compliance und Wirtschaftsprüfung	179
H. Hamburg Commercial Bank: Cloud-Transformation im Zahlungsverkehr	211

Inhaltsverzeichnis

Vorwort (<i>Grete/Held</i>)	1
A. Von der Bank in die Cloud – eine Einführung zum Cloud Computing in der Finanzindustrie (<i>Held</i>)	3
I. Einleitung	5
II. Die Banken-IT im Wandel	6
1. Grundlagen der Banken-IT	6
a) Die »klassische Banken-IT«	6
b) Die Rolle von Mehrmandantendienstleistern	10
2. Banking-IT in der Cloud	10
3. Unterschiede zwischen klassischer Banken-IT und Cloud	13
III. Cloud Computing im Spannungsfeld zwischen Regulierung und Geschäft	15
1. Grundprinzipien der Regulierung	15
2. Umsetzung der Regulierung	17
IV. Besondere strategische Herausforderungen	19
1. Rechtsrisiken im global verteilten IT-Betrieb	19
2. Geostrategische Risiken	19
3. Principal-Agent-Problem und Vendor-Lock-In	20
V. Wege zu einer verantwortungsbewussten Cloud-Nutzung	20
1. Aufrechterhalten der Handlungs- und Beurteilungsfähigkeit	20
2. Cloud-Nutzung über einen geregelten Prozess	21
3. Nutzung gängiger Standards	22
4. Vermeidung von Regelungslücken und von »Schatten-IT«	23
VI. Schluss	24

B. Cloud Computing in der Finanzbranche – Eine Einleitung <i>(Grete)</i>	25
I. Einleitung: Warum Cloud Computing ein Thema für das C-Level ist	27
II. Paradigmenwechsel im Fokus: Von der Technik zur strategischen Neuausrichtung	27
III. Cloud Computing: Kernmerkmale und ihr Einfluss	30
IV. Auswirkungen auf strategischer Ebene	31
V. Folgen auf taktischer und operativer Ebene	32
VI. Risiken und Grenzen	34
VII. Fazit & Take-Home-Messages	35
 C. Überwachung von IKT-Drittdienstleistern zwischen Abhängigkeit und Resilienz <i>(Kocatepe)</i>	 37
I. Überwachung von IKT-Drittdienstleistern zwischen Abhängigkeit und Resilienz	39
1. Status quo	39
2. Abhängigkeitsrisiken im Fokus der Finanzunternehmen: Schlüsselprinzipien des Managements des IKT-Drittparteienrisikos	42
a) Ex-ante-Risikobewertung und Due-Diligence	42
b) Ausstiegsstrategie	43
c) Vertragsanforderungen	44
d) Strategie zur Nutzung mehrerer IKT-Drittdienstleister	44
e) Einhaltung der Datenschutzvorschriften	46
3. Abhängigkeitsrisiken im Fokus der Finanzmarktaufsichtsbehörden: Überwachung kritischer IKT-Drittdienstleister	47
a) Abhängigkeit der Finanzunternehmen als Indikator für die Kritikalität des IKT-Drittdienstleisters	49
b) Gemeinsame Untersuchungsteams und Überwachungsbefugnisse	51

II.	Fazit	53
D.	Cloud-Computing in der Sparkassenpraxis: Chancen und Herausforderungen aus Sicht von IT-Organisation und Interner Revision (<i>Debes</i>)	55
I.	Einleitung	57
II.	Grundlagen des Cloud-Computing im Sparkassenkontext	59
1.	Definitionen und Servicemodelle (IaaS, PaaS, SaaS)	59
	Die Wahl des Servicemodells determiniert maßgeblich den Grad der eigenen Kontrolle und Verantwortung, die Komplexität der Integration in bestehende Systeme sowie die Anforderungen an das Management der Cloud-Dienste.	61
2.	Bereitstellungsmodelle (Public, Private, Hybrid, Community Cloud)	61
3.	Wesentliche regulatorische Rahmenbedingungen für Sparkassen	62
4.	Relevante Cloud-Standards und Zertifizierungen: Praktischer Nutzen für Sparkassen	63
a)	Internationale Standards als Fundament und Orientierungshilfe	63
b)	Nationale und branchenspezifische Standards/Kataloge – die deutsche Perspektive	65
c)	Die praktische Bedeutung von Standards im Sparkassenalltag	67
III.	Die Revisionssicht auf Cloud-Computing in Sparkassen	68
1.	Gesetzliche und aufsichtsrechtliche Anforderungen an die Prüfung	68
a)	Risikoanalyse und Wesentlichkeitsbeurteilung bei Cloud-Auslagerungen bzw. beim Bezug von IKT-Dienstleistungen	69

b)	Anforderungen an Verträge und Dienstleistersteuerung (SLAs, Weisungsrechte, Kontrollrechte)	70
c)	Informationssicherheit und Datenschutz in der Cloud aus Revisionssicht	71
d)	Kritische IKT-Dienstleister unter DORA	73
2.	Prüfungsplanung und -durchführung bei Cloud-Sachverhalten	74
a)	Identifikation relevanter Prüfungsfelder und -objekte	74
b)	Nutzung von Zertifizierungen und Testaten als Prüfungsnachweis und zur Effizienzsteigerung der Prüfung	75
c)	Prüfung der Angemessenheit von Notfallkonzepten und Exit-Strategien	76
3.	Typische Feststellungen und Handlungsempfehlungen der Revision	77
IV.	Die praktische Umsetzung: Cloud-Computing aus Sicht der IT-Organisation	79
1.	Strategische Überlegungen zur Cloud-Nutzung in einer Sparkasse	80
a)	Chancen und Potenziale	80
b)	Risiken und Herausforderungen aus operativer Sicht	81
c)	Wirtschaftlichkeitsbetrachtungen und Total Cost of Ownership (TCO)	82
2.	Auswahl und Implementierung von Cloud-Lösungen	83
a)	Anforderungsmanagement und Auswahlprozess für Cloud-Dienste und -Anbieter	83
b)	Migrationsstrategien und Integrationsansätze in die bestehende IT-Landschaft	84
c)	Rolle und Zusammenarbeit mit zentralen IT-Dienstleistern (z. B. Finanz Informatik)	85
3.	Betrieb und Management von Cloud-Services	86
a)	Cloud-Governance und Betriebskonzepte in der IT-Organisation	86

b)	Monitoring, Performance-Management und Security Operations in der Cloud	88
c)	Skill-Entwicklung und Anpassung der Aufbau- und Ablauforganisation	89
V.	Datenschutz als zentrale Herausforderung bei Cloudnutzung in Sparkassen	90
1.	Kernanforderungen der DSGVO im Cloud-Kontext	90
2.	Spezifische Datenschutzrisiken und Herausforderungen in der Cloud	92
3.	Praktische Maßnahmen und Lösungsansätze für Sparkassen	93
VI.	Weitere spezifische Herausforderungen und Lösungsansätze für Sparkassen	94
1.	Management von Abhängigkeiten und Sicherstellung der Portabilität	95
a)	Abhängigkeit von der Finanz Informatik:	95
b)	Vendor Lock-in bei Cloud-Anbietern:	96
2.	Gewährleistung von Ausfallsicherheit und Business Continuity	97
3.	Kultureller Wandel und Akzeptanzförderung für Cloud-Technologien	98
4.	Evolution der Sicherheitsarchitektur: Von der Perimetersicherheit zu Zero-Trust und DevSecOps	99
VII.	Fazit und Ausblick	100
1.	Zusammenfassung der Kernerkenntnisse	101
2.	Ausblick auf zukünftige Entwicklungen und Potenziale des Cloud-Computings für Sparkassen	102
E.	Prüfung von Cloud-Service-Providern im Rahmen eines Pooled Audits (<i>Planeth</i>)	105
I.	Einleitung	107
II.	Besondere Rahmenbedingungen bei der Prüfung von Dienstleistern	108

1.	Allgemein	108
2.	Cloud-Anbieter – Hyperscaler	109
3.	Cloud-Anbieter: SaaS-Provider	111
III.	Unterschiedliche Arten der Prüfung	112
1.	Einzelprüfung	112
2.	Wirtschaftsprüfer beauftragen	112
3.	Pooled Audit (oder Sammelaudit)	113
IV.	Durchführung eines Pooled Audits	114
1.	Vorbereitung	114
2.	Prüfungsgegenstand	118
3.	Prüfungskonzept	121
4.	Audit Fieldwork	122
5.	Audit Right Limitation	127
6.	Reporting	128
V.	Collaborative Cloud Audit Group for the Financial Services Industry in the European Union e. V.	130
VI.	Follow Up	132
VII.	Ausblick	132
F.	Cloud-Dienste bei Kreditinstituten – von Einsatzbereichen bis zur Prüfung (<i>Winterer</i>)	135
I.	Einsatzbereiche von Cloud-Dienstleistungen in Kreditinstituten	137
1.	Interne Einsatzbereiche	137
a)	Modernisierung der IT-Infrastruktur	137
b)	Anwendungsentwicklung und Betrieb	138
c)	Data Analytics und Business Intelligence	139
2.	Externe Einsatzbereiche	140
a)	Kundenservices	140
b)	Kooperationen und Plattformstrategien	140
3.	Grenzen des Einsatzes	141

II.	Regulatorischer Rahmen für Cloud-Dienstleistungen	141
1.	Aufsichtsrechtliche Anforderungen	141
a)	EBA-Guidelines/MaRisk	141
b)	DORA aus der Perspektive eines Kreditinstituts	143
2.	Datenschutzrechtliche Anforderungen	148
a)	Verantwortlichkeit und Rechtsgrundlage	148
b)	Auftragsverarbeitung und Vertragspflichten	149
c)	Technische und organisatorische Maßnahmen (Artikel 32 DSGVO)	150
d)	Datenübermittlung in Drittstaaten	150
e)	Transparenzpflichten und Betroffenenrechte	151
f)	Datenschutz-Folgenabschätzung (DSFA)	152
g)	Rechenschaftspflicht und Dokumentation	152
3.	ISO/IEC Standards	153
III.	Herausforderungen durch Cloud-Dienstleistungen	154
1.	Technologische Herausforderungen	155
a)	Komplexität moderner Cloud-Architekturen	155
b)	Technologische Abhängigkeiten und Vendor-Lock-in	155
c)	Transparenz und Steuerbarkeit der Datenverarbeitung	156
2.	Sicherheits- und Datenschutzrisiken	157
a)	Zugriffskontrollen und Konfigurationsrisiken	157
b)	Eingeschränkte Prüfbarkeit und fehlende Transparenz	157
3.	Betriebliche und organisatorische Herausforderungen	158
a)	Strategische Einbindung und Governance	158
b)	Organisationsstruktur und Personalbedarf	159
c)	Prozesse, Kontrollsysteme und Entwicklungszyklen	159
d)	Komplexität durch Lieferketten	159
4.	Kosten- und Vertragsmanagement	160
a)	Kostenstruktur und wirtschaftliche Steuerung	160
b)	Vertragsgestaltung und regulatorische Anforderungen	162
c)	Vertragliches Lifecycle-Management	162

5.	Kundenakzeptanz	163
a)	Verlässlichkeit von Diensten	163
b)	Nutzerfreundlichkeit	164
IV.	Prüfung von Cloud-Dienstleistungen bei Kreditinstituten	164
1.	Relevante Prüfungsstandards	164
a)	Gesetzliche Abschlussprüfung	164
b)	Prüfungen außerhalb der gesetzlichen Abschlussprüfung	166
c)	Standards für die Interne Revision	168
2.	Prüfungsprozess bei Cloud-Dienstleistungen	168
a)	Indirekte oder direkte Prüfung	169
b)	Angemessenheits- und/oder Wirksamkeitsprüfung	170
c)	Prüfungskriterien	172
d)	Berücksichtigung von Subdienstleistern	173
e)	Dokumentation und Bericht	173
3.	Herausforderungen bei der Prüfung von Cloud- Dienstleistungen	174
a)	Gesetzliche Abschlussprüfung	174
b)	Prüfungen außerhalb der gesetzlichen Abschlussprüfung	175
4.	Best Practices für die Prüfung	176
V.	Praxistipps	177
G.	Digitale Resilienz im Finanzsektor: IKT-Drittdienstleister aus dem Blickwinkel von IT-Compliance und Wirtschaftsprüfung <i>(Regener/Schulz/Vehlow)</i>	179
I.	Einleitung	181
1.	Anwendungsbereich und Struktur des Digital Operational Resilience Act (DORA)	182
2.	Zielsetzung von DORA	182
3.	Mehrwert der Wirtschaftsprüfung in der DORA- Umsetzung	183
II.	DORA-Anforderungen	184

1.	IKT-Risikomanagement	184
2.	Behandlung, Klassifizierung und Berichterstattung IKT-bezogener Vorfälle	185
3.	Testen der digitalen operationellen Resilienz	186
4.	Informationsaustausch	187
5.	Management von Risiken durch IKT-Drittdienstleister	188
a)	Pflichten von IKT-Drittdienstleistern bzw. Anforderungen an IKT-Drittdienstleister	189
b)	Vertragliche Mindestanforderungen	190
III.	Steuerung und Überwachung von IKT-Drittdienstleistern	192
1.	Prüfprogramm zur Steuerung und Überwachung von IKT-Drittdienstleistern	192
2.	Selbstauskunft des IKT-Drittdienstleisters	194
3.	Eigene Überwachungshandlungen des Finanzunternehmens	194
4.	Verwerten von Konformitätsbestätigungen beim Überwachen und Steuern von IKT-Drittdienstleistern	195
a)	ISO/IEC 27001	197
b)	ISO/IEC 27017, ISO/IEC 27018 und BSI IT-Grundschutz	198
c)	Kriterienkatalog Cloud Computing (BSI C5)	199
d)	System and Organization Controls 2 (SOC 2)	201
e)	Controls Reports gemäß ISAE 3402 bzw. IDW PS 951	202
f)	BSI KRITIS & NIS 2	203
g)	Weitere Zertifikate wie TIER-, TSI- oder DIN EN 50600-Zertifizierung	204
IV.	Multi Compliance-Kontrollsystem zwecks Konformität mit mehreren Standards	205
1.	Funktionsweise und Aufbau eines Multi Compliance-Kontrollsystems	205
2.	Validierung und Nutzung eines Multi Compliance-Kontrollsystems aus dem Blickwinkel der Wirtschaftsprüfung	208

V.	Fazit	209
H.	Hamburg Commercial Bank: Cloud-Transformation im Zahlungsverkehr (<i>Frommholz/Libiseller/von Poser</i>)	211
I.	Einleitung	213
II.	Systemarchitektur	216
III.	Cloud-Anforderungen	220
1.	Anwendungen und Infrastruktur	221
a)	Konfiguration/Staging	222
b)	Credentials	222
c)	Operatoren	223
d)	Zugänge	223
e)	Rollen und Rechte	224
f)	Datenablage	224
g)	Logging	225
2.	Service-Architektur	226
a)	Monitoring und Alerting	226
b)	Zielzustand	227
c)	Abhängigkeiten zu externen Services	227
d)	Nutzung und Traffic	228
e)	Systemkomponenten	229
3.	Nicht-funktionale Anforderungen	229
4.	Sicherheit und Regulatorik	231
5.	Betreiberperspektive	233
IV.	Infrastructure as Code	235
V.	Staging	237
VI.	Schlussbemerkungen	240
VII.	Literatur	241

Vorwort

Einige Argumente für die Nutzung externer Cloud-Dienste liegen so sehr auf der Hand, dass sie zu regelrechten Binsenweisheiten geworden sind. Als Erstes zu nennen sind Skaleneffekte, also Kostenvorteile, die sich aus der gemeinsamen Nutzung von IT-Ressourcen durch viele Kunden ergeben. Für den einzelnen Kunden ergibt sich dabei idealerweise eine gesteigerte Flexibilität durch die Miete skalierbarer IT-Leistungen. Durch die Leistungserbringung über das Internet ist zudem eine globale Verfügbarkeit der Anwendungen naheliegend.

Die Kunden dürfen zudem in Zeiten des Fachkräftemangels auf eine besonders hohe Professionalität des Cloud-Dienstleisters und seiner Mitarbeiter hoffen. Zentrale IT-Sicherheitsmaßnahmen des Cloud-Dienstleisters können ggf. sogar ein höheres Sicherheitsniveau erzielen, als dies für einige Anwendungsszenarien für einzelne Kunden wirtschaftlich darstellbar wäre. Schließlich partizipieren die Kunden am technischen Fortschritt durch die laufende Fortentwicklung des Cloud-Dienstes.

Dem stehen aber mindestens ebenso prominente Risiken entgegen. Die Kunden können schnell in eine technisch-ökonomische Abhängigkeit vom Cloud-Dienstleister geraten – dem Vendor Lock-In. Der Cloud-Dienst selbst und die darin verarbeiteten Daten unterliegen häufig einer fremden Jurisdiktion – und damit Rechtsrisiken und geostrategischen Gefährdungen. Der hohe Automatisierungsgrad der Cloud sorgt zudem nicht nur im positiven Sinne für Effizienz. Schlägt ein Fehler zu, dann schlägt er automatisiert durch und richtet besonders verheerende Schäden an. Die genannten Skaleneffekte ergeben sich auch für Cyber-Kriminelle: Attackiere einen Cloud-Dienst und triff all seine Kunden!

Für Finanzunternehmen, die die Cloud nutzen wollen, ergeben sich also potenziell enorme Chancen, denen immense Risiken gegenüberstehen können. Die Risiken müssen gemanagt werden, damit die Chancen verwirklicht werden können. Zugleich findet jede Cloud-Nutzung unter den Argusaugen der Aufsichtsbehörden statt. Der europäische Gesetzgeber hat diese und die Unternehmen mit DORA sogar dazu verpflichtet, das Thema besonders ernst zu nehmen.

Dieses Buch richtet sich an Entscheidungsträger in Geschäftsleitung, Fachbereichen und IT von Finanzunternehmen, besonders aber an Innenrevisoren und andere Prüfer. Es soll zu einem aufgeklärten, pragmatischen und sorgfältigen Umgang mit der Cloud-Nutzung beitragen.

Dr. Markus Held

Dr. Patrick Grete

Bonn, den 27.07.2025¹

1 Die Herausgeber geben in diesem Buch ihre persönlichen Auffassungen wider. Dieses Buch ist keine Veröffentlichung des Bundesamts für Sicherheit in der Informationstechnik.

A.

**Von der Bank in die Cloud – eine Einführung zum
Cloud Computing in der Finanzindustrie**

A. Von der Bank in die Cloud – eine Einführung zum Cloud Computing in der Finanzindustrie

I. Einleitung²

Die Cloud ist Alltag. Streaming von Filmen und Serien, Musik und Podcasts, Werbeanzeigen, Videospiele, Bücher- wie Essensbestellungen, Unternehmenswebseiten, Video- und Audiokonferenzen, Terminabstimmungen, die Routenplanung für die Autofahrt und den Ferienflug, Steuerung von Fabrik- wie Staubsaugerrobotern, gemeinsame Arbeit an Dokumenten, Künstliche Intelligenz als intellektuellen Sparringspartner, Auftragskünstler und unermüdlichen Bürosachbearbeiter – all das und noch viel mehr leistet die Cloud. 1

Die Cloud ist Muskel und Achillesferse der Digitalgesellschaft zugleich. Alle möglichen Anwendungen hängen von ihrer Verfügbarkeit und ihrer korrekten Funktion ab. Mehr noch: Jedermanns Daten liegen in der Cloud, verführerische Beute für Kriminelle und Geheimdienste gleichermaßen. 2

Man könnte meinen: 2025 ist genau der falsche Zeitpunkt, um sich mit Cloud Computing für die Finanzindustrie zu befassen. Aktuelle internationale Krisen werfen die alte Weltordnung der Globalisierung in eine »Weltunordnung« mit gegenseitigem Misstrauen und gefährdeten Lieferketten um. De-Risking und De-Coupling sind en vogue – sogar gegenüber alten Verbündeten. Wäre es nicht besser, gar keine Cloud mehr zu betreiben und alle Datenverarbeitung »on premise« zu betreiben? 3

Wie wir sehen werden, ergeben sich tatsächlich zahlreiche Herausforderungen beim Weg zur rechtskonformen, effizienten und vor allem sicheren Nutzung des Cloud Computing in der aus guten Gründen stark regulierten Finanzindustrie. Zugleich führt auf Dauer kein Weg an der Befassung mit Cloud Computing vorbei. 4

² Dieses Kapitel und die Herausgebertätigkeit für das Buch sind eine private Veröffentlichung von Dr. Markus Held und unabhängig vom Bundesamt für Sicherheit in der Informationstechnik.

II. Die Banken-IT im Wandel

1. Grundlagen der Banken-IT

a) Die »klassische Banken-IT«

- 5 Exemplarisch für regulierte Finanzunternehmen im Allgemeinen soll im Folgenden die Banken-IT betrachtet werden. Banken waren stets Pioniere in beim Einsatz neuer Technologien und Methoden zur Datenverarbeitung. Daraus hat sich eine Einsatzform von Informationstechnik entwickelt, die äußerst ausgereift und zuverlässig funktioniert. Die IT dient dabei stets dem Geschäftsmodell des Instituts und ist stets in sein Internes Kontrollsystem eingebunden. Die folgende Abbildung illustriert die logische Struktur der der IT-Organisation eines Instituts.

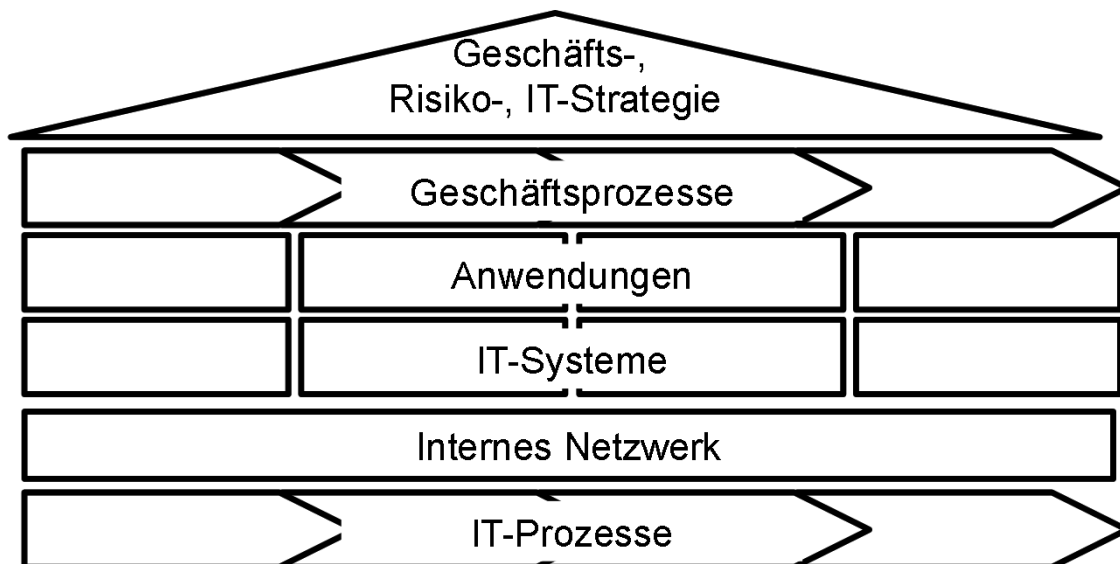


Abbildung 1: Das »Haus der Banken-IT« (Quelle: Illustration von Dr. Markus Held)

- 6 Das Geschäftsmodell des Instituts wird grundsätzlich durch seine Geschäfts- und seine Risikostrategie beschrieben, die sich in weiteren Strategien des Hauses verästeln (z. B. die Auslagerungsstrategie). Die IT-Strategie kann dabei als derjenige Teil der Geschäftsstrategie aufgefasst werden, der die IT-Organisation adressiert. Die Geschäftsprozesse des Instituts setzen die Geschäftsstrategie um und werden durch Anwendungen unterstützt, die auf den IT-Systemen des Instituts laufen, welche ihrerseits durch (mindestens) ein internes Netzwerk verbunden sind. Anwendungen, IT-Systeme und Netzwerke werden durch die IT-Prozesse verwaltet, die mithin die Geschäftsprozesse der IT-Organisation darstellen.

Die IT-Systeme der klassischen Banken-IT sind durch eine mehrschichtige Architektur gekennzeichnet: Selbstbedienungsterminals, Geldausgabeautomaten, Arbeitsplatzrechner in Filialen (und im Home Office) sowie Online-Banking-Webseiten und mobile Apps greifen – ob über das Internet oder dedizierte Netzwerke – auf zentrale Applikationen zu, die die verschiedenen bankfachlichen Geschäftsprozesse umsetzen.

Abbildung 2 zeigt die sich ergebende technische Architektur der »klassischen Banken-IT«: Endgeräte in selbst betriebenen Netzen ggf. unterschiedlicher Sicherheitsniveaus (Geldausgabeautomaten, Selbstbedienungsterminals, Arbeitsplatzrechner in Filialen und Backoffice) greifen über dedizierte Netzwerkverbindungen auf zentral betriebene Anwendungsserver zu. Online-Banking-Webseiten und Mobile Apps werden ebenso mithilfe von Anwendungsservern betrieben.

Die Anwendungsserver unterscheiden sich hinsichtlich ihrer Hardware-Architektur (i. d. R. x86-Prozessoren) und der verwendeten Betriebssysteme (Linux, Windows, sonstige Unix-Derivate) kaum von Personal Computern.

Die Anwendungsserver greifen für die rechtssichere Transaktionsverarbeitung, also die Buchungen in Konten und Wertpapierdepots, auf einen Mainframe zu, der eine Datenbank verwaltet. Alle Server sind redundant ausgelegt und auf Ebene der Datenbank findet eine Spiegelung der Daten statt.

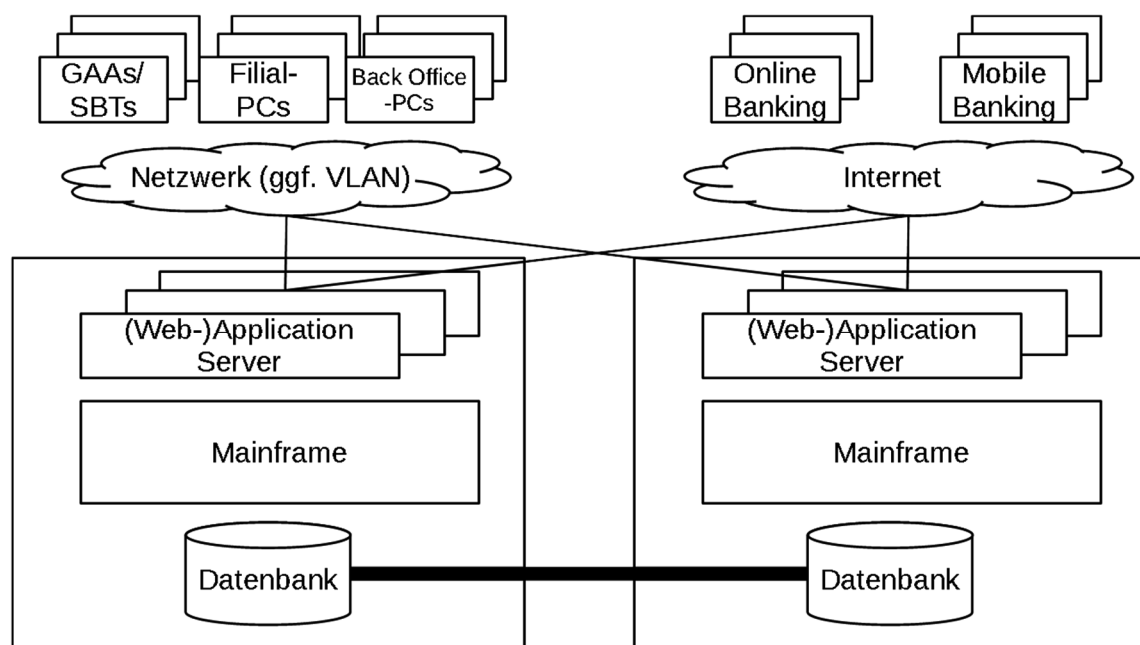


Abbildung 2: Die »klassische« Banken-IT (Quelle: Illustration von Dr. Markus Held)

- 11 Banken setzen für ihre Kernprozesse im Backend deshalb häufig Mainframes ein, weil diese mehrere entscheidende Vorteile bieten, die für die spezifischen Anforderungen des Bankensektors besonders wichtig sind.
 - aa) Besonders hohe Verarbeitungsleistung für Transaktionen
- 12 Mainframes sind in der Lage, enorme Anzahlen an Transaktionen schnell und effizient – rechtssicher – zu verarbeiten. Dies ist entscheidend, um tagesaktuell Millionen von Transaktionen abwickeln zu können.
 - bb) Zuverlässigkeit und Ausfallsicherheit
- 13 Mainframes sind auf extreme Zuverlässigkeit und geringe Ausfallrate ausgelegt. Üblich ist eine Kombination aus synchronen und asynchronen Datenspiegelungen über mehrere Rechenzentrumsstandorte hinweg, bei der Transaktionsverarbeitung explizit berücksichtigt wird. Da Systemausfälle erhebliche finanzielle und reputative Schäden verursachen können, ist dies ein wesentlicher Faktor.
 - cc) Sicherheit
- 14 Mainframes bieten ein hohes Maß an Sicherheit, was für Banken, die mit sensiblen Kundendaten und finanziellen Transaktionen umgehen, unerlässlich ist. Sie verfügen über besonders lang gereifte und robuste Sicherheitsfunktionen, die vor Cyberangriffen und Datenverlust schützen. Dabei wird seit Jahrzehnten u. a. auf eine Kombination aus dedizierter Krypto-Hardware, mehrschichtigen Virtualisierungsverfahren, sowie Rollen- und Rechteverwaltungen für die Applikationsebene gesetzt.
 - dd) Skalierbarkeit
- 15 Mainframes können mit Vorlauf längerfristig und in besonderen Situationen kurzfristig skaliert werden, um mit steigenden Anforderungen an die Datenverarbeitung und Speicherung Schritt zu halten. Beispielsweise können in besonderen Lastsituationen physisch verbaute, aber im Alltagsbetrieb ungenutzte zusätzliche CPU-Ressourcen gegen Geld freigeschaltet werden.
 - ee) Kompatibilität
- 16 Mainframes unterstützen oft ältere Anwendungen und Systeme, die über Jahrzehnte hinweg entwickelt wurden. Dies ermöglicht es, die bestehende IT-Infrastruktur weiter zu nutzen und gleichzeitig neue Technologien zu integrieren.

ff) Kosteneffizienz

Obwohl die Anschaffungskosten für Mainframes hoch sein können, sind sie oft kosteneffizient im Betrieb, insbesondere wenn es um die Verarbeitung großer Datenmengen geht. Die langfristige Nutzung und die geringe Ausfallrate tragen zur Kosteneffizienz bei. 17

gg) Echtzeitverarbeitung von Transaktionen

Mainframes können Transaktionen praktisch in Echtzeit verarbeiten, was für die schnelle und zuverlässige Transaktionsabwicklung von entscheidender Bedeutung ist. Eine Transaktion ist dabei dadurch gekennzeichnet, dass ein Buchungsvorgang entweder vollständig oder überhaupt nicht durchgeführt wird. Dabei werden die »ACID«-Properties jeder einzelnen Buchung gewahrt, sodass Daten stets in einem eindeutigen Zustand befinden (»atomicity, consistency, integrity, durability«). In Mainframes sind zu diesem Zwecke Spezialkomponenten verbaut, die diese Eigenschaften speziell unterstützen. Dies ermöglicht es, jederzeit Datenbanken, Bücher, Depots und Konten in einem rechtssicheren Zustand zu halten. 18

Zusammengefasst ist die klassische Banken-IT über Jahrzehnte in einer evolutionären Entwicklung gewachsen. Sie bietet eine Kombination aus Leistung, Sicherheit und Zuverlässigkeit, die auf die individuellen Anforderungen der Institute zugeschnitten ist. Besonders prägende Aspekte sind dabei die stete Garantie der Datenintegrität, die rechtssichere Transaktionsverarbeitung in Echtzeit und die Sicherstellung der dauerhaften Verfügbarkeit der Daten. Die Anforderungen der Banken-IT wirkten spiegelbildlich auf die Entwicklung marktgängiger Technologien und Standards. 19

Die Schattenseite ist: Die Banken-IT ist aufwendig in Entwicklung, Wartung und Betrieb. Es wird zunehmend schwieriger, Personal zu finden, das geeignet ist, besonders anspruchsvolle Systeme, insbesondere die Mainframes, zu administrieren oder Entwicklung zu betreiben. 20

Als weiteres Problem tritt eine erhebliche Marktkonzentration bei den Herstellern von Mainframe-Computern hinzu. Weltweit verfügt IBM hier seit über zwanzig Jahren eine klare Dominanz. Der bedeutende Konkurrent Fujitsu kündigte 2022 seinen Ausstieg aus dem Mainframe-Markt bis 2030 an.³ 21

3 <https://www.heise.de/news/Fujitsu-kuendigt-das-Mainframe-Aus-an-und-schmiedet-neue-Mainframe-Plaene-6539577.html>

b) Die Rolle von Mehrmandantendienstleistern

- 22 Darum geht der Trend seit Jahrzehnten zur Konsolidierung der Banken-IT, ob im Eigenbetrieb eines Konzerns oder durch den Mehrmandantendienstleister innerhalb einer Finanzgruppe. In Deutschland stehen die Finanz Informatik als IT-Dienstleister der S-Finanzgruppe und die Atruvia als IT-Dienstleister der genossenschaftlichen Finanzgruppe exemplarisch für diese Entwicklung.
- 23 Das Angebot dieser Mehrmandantendienstleister aber auch der konzerneigenen IT-Töchter zeichnet sich dadurch aus, dass den Kunden über ein Netzwerk standardisierte, skalierbare IT-Leistungen angeboten werden, von Standardanwendungen bis hin zum Hosting selbst nutzbarer Server. Wichtige Anwendungen können flexibel durch Scripting und Konfiguration an die eigenen Bedürfnisse angepasst werden und stellen mithin eine Basisplattform für das gesamte Bankgeschäft dar. Viele der gebotenen Leistungen können dabei direkt über Portale der Mehrmandantendienstleister gebucht werden.
- 24 Beispielhaft für das umfassende und branchenspezifische Leistungsportfolio sind dabei Kernbanksysteme. Diese bilden unter Berücksichtigung regulatorischer Vorgaben, mit besonderem Augenmerk auf die Ordnungsmäßigkeit der Buchführung und Revisionssicherheit der Datenhaltung die Kernprozesse eines Kreditinstituts ab. Für die einzelnen Kunden ist im Regelfall eine Anpassung an die eigenen Prozesse durch umfangreiche Konfigurationsmöglichkeit und Scripting (Customizing) oder durch die Entwicklung spezifischer Module erforderlich. Den Kunden werden darüber hinaus teilweise Zusatzleistungen angeboten, die individuell vereinbart werden können.
- 25 Die traditionellen Mehrmandantendienstleister der Finanzwirtschaft bilden gemeinsam mit ihren Kunden ein Ökosystem, in dem Kunden, deren Interessensverbände und die Dienstleister selbst durch Verträge und teils auch durch Beteiligungen über Jahrzehnte eng verbunden sind.

2. Banking-IT in der Cloud

- 26 Abbildung 3 zeigt eine vereinfachte und generische Darstellung der technischen Architektur, die dem Cloud-Betrieb zu Grunde liegt.