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.

FCH AG, 2025

Inhaltsübersicht

Inhaltsverzeichnis

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 27.07.2025[1]

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. Einleitung[2]

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.

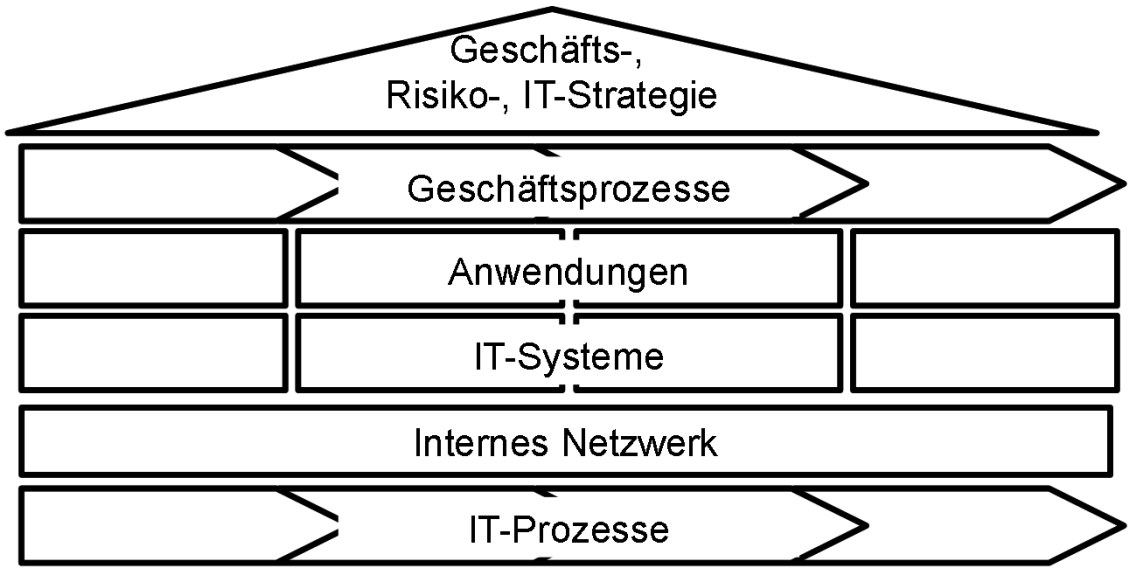

Abbildung 1: Das »Haus der Banken-IT« (Quelle: Illustration von Dr. Markus Held)

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. 7

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. 8

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. 9

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. 10

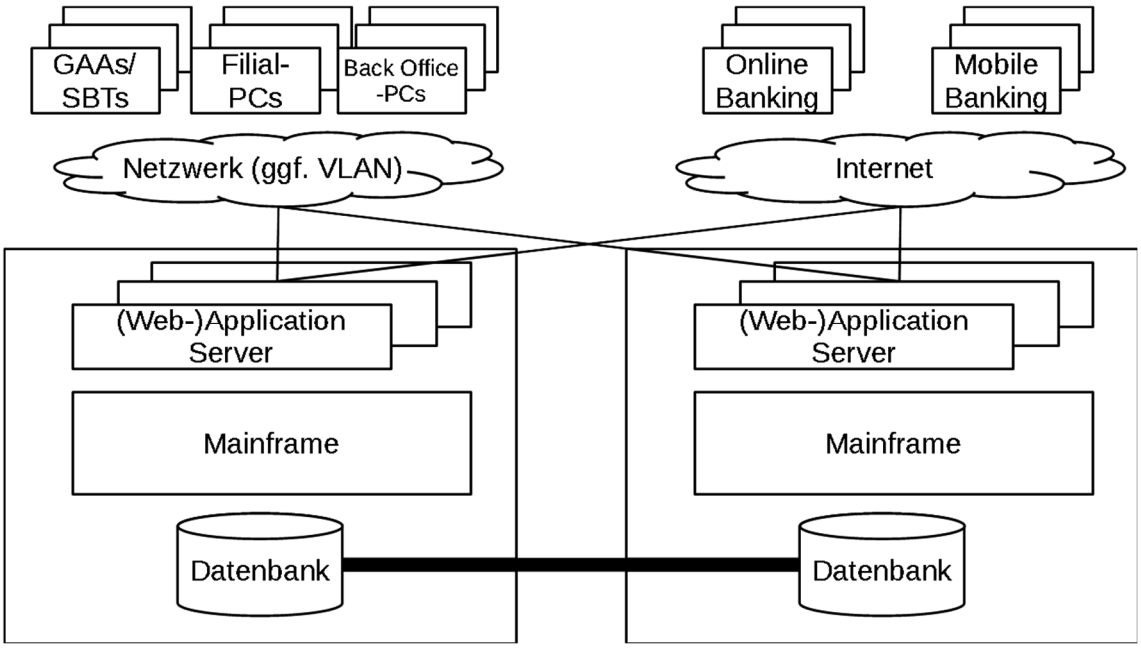

Abbildung 2: Die »klassische« Banken-IT (Quelle: Illustration von Dr. Markus Held)

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.