IT-OUTSOURCING IM STARK REGULIERTEN UMFELD

Rechtssicher und verantwortungsvoll in die Cloud

Der Kostendruck ist in der Finanzbranche ständig präsent, die digitale Transformation unumkehrbar. Um handlungsfähig zu bleiben und die eigenen Ressourcen zu schonen, befreien sich die Unternehmen immer stärker von Ballast abseits ihres Kerngeschäfts. Entsprechend rückt IT-Outsourcing in den Fokus der Finanzinstitute. Unter Beachtung der regulatorischen Auflagen ist dieser Weg in der Regel gangbar – aber es gibt Stolperfallen. Eine grundsätzliche Betrachtung der wichtigsten Vertragserfordernisse und Prüfungsverpflichtungen beim Cloud Sourcing.

T? Nicht jetzt, das ist ein Thema für die Fachabteilung!“ Diese Haltung ist noch gar nicht so lange her. Heute haben digitale Aspekte bei Finanzinstituten aber eine enorme unternehmensstrategische Bedeutung erlangt. Sowohl für Innovationen als auch für kundennahe Angebote oder beim Thema Effizienzsteigerung führt kein Weg mehr an IT-gestützten Prozessen vorbei.

Ob ein Unternehmen aber alles selbst machen muss? Oft haben Verfügbarkeit, Sicherheit und Compliance gerade in der Finanzbranche dazu geführt, dass Inhouse-Lösungen vorgezogen wurden. Dieser Trend kehrt sich derzeit um. Grund dafür sind immer kürzere Innovations- und Produktzyklen und der gleichzeitig steigende Kostendruck.

Das Thema Outsourcing ist daher virulenter denn je. Die Vorteile sind verlockend: Kosteneinsparungen, Produktivitätssteigerungen infolge von Arbeitsteilung und Spezialisierung sowie mehr Flexibilität durch hohe Skalierbarkeit. Schließlich ist eine Verlagerung auch ein Impuls, die eigenen Geschäftsabläufe zu überdenken und gegebenenfalls zu reorganisieren.

Ganz ohne Nachteile ist ein Outsourcing allerdings nicht: Es kann zu erhöhten Kommunikationsaufwänden kommen, zudem droht eine Abhängigkeit vom gewählten Cloud-Partner. Ein Teil der Steuerungshoheit geht in jedem Fall verloren. Beim Thema Sicherheit ist Vertrauen zwar gut, sind aber Kontrolle und exakte Festlegungen ein Muss. Denn es existieren eine Vielzahl von Gesetzen, Regularien und IT-Standards, die Rechte und Pflichten von Finanzinstituten und Dienstleistern festlegen, vgl. dazu die Abbildung ▸ **1**.

Keine Auslagerung ohne Klarheit über den Prozess

Das Finanzwesen gehört zu den hoch reglementierten Branchen. Bei Auslagerungsprojekten, derzeit verstärkt in Richtung Cloud Computing, mischen viele Akteure mit, deren Vorgaben teils erst in nationales Bankenaufsichtsrecht umgewandelt werden müssen. Selbst für Experten ist der Regularien-Dschungel eine Herausforderung. Zumal sich durch die Vielzahl an Vorschriften Ermessensspielräume auftun, die von der Aufsicht nicht immer konsistent genutzt werden. Eine gute Orientierung bieten die EBA Guideline Outsourcing und die Mindestanforderungen an das Risikomanagement (MaRisk).

Ergibt sich aus Rechtsvorschriften kein genereller Hinderungsgrund für die Auslagerung eines Prozesses, empfiehlt es sich, das Outsourcing mit einer initialen Wesentlichkeitsprüfung samt Dokumentation zu starten. Diese Analyse ist kein einmaliger Vorgang. Sie sollte während der Vertragslaufzeit regelmäßig und auch anlassbezogen durchgeführt werden. Für die Einstufung als relevant gelten dabei vorher selbst erbrachte Leistungen, die künftig laufend oder wiederkehrend vom Dienstleister ausgeübt werden.

Neben dem Aspekt „wesentlich“ muss auch die Kritikalität bewertet werden. Kritisch ist beispielsweise alles, was die Erledigung der Geschäftsverpflichtungen beeinträchtigt, Auswirkungen auf die Zulassungsvoraussetzungen hat oder die Bereitstellung von Bank-Services unterbrechen könnte.

Die Verantwortung bleibt

In der Finanzindustrie eigentlich eine Binse, aber dennoch wert, erwähnt zu werden: Beim Outsourcing kann ein Institut die Abläufe delegieren, aber nie die Verantwortung. Daher ist es unverzichtbar, dass das IT-Outsourcing beim Risikomanagement entsprechende Berücksichtigung findet. Die ausgelagerten Prozesse dürfen nicht zur Blackbox mutieren. Die Verantwortlichkeiten müssen klar geregelt sein.

Das auslagernde Institut muss zudem über ausreichende Ressourcen verfügen, die eine Überwachung der ausgelagerten Funktionen und die Erfüllung der regulatorischen Anforderungen gewährleisten. Weiterhin muss Vorsorge für den Fall eines plötzlich notwendigen Wechsels des Serviceproviders getroffen werden, alternativ für eine rasche Re-Integration der betroffenen Prozesse in die bankeigene IT.

Da die Position ohnehin bald verpflichtend zu besetzen ist, sollte bereits jetzt ein Auslagerungsbeauftragter ernannt werden.

Eine Auslagerung hat mit hoher Wahrscheinlichkeit Auswirkungen auf die operati-

1 | Vorschriften, Normen und Standards im Bereich Bankenregulatorik

Zivilrecht	Aufsichtsrecht	ISO-Normen	Prüfstandards vom Institut für Wirtschaftsprüfer (IDW)	Sonstige Standards
» **BGB** Bürgerliches Gesetzbuch » **HGB** Handelsgesetzbuch » **UrhR** Urheberrecht » **DSGVO** Datenschutz-Grundverordnung » **BDSG** Bundesdatenschutzgesetz » **BSIG** Gesetz für das Bundesamt für Sicherheit in der Informationstechnik » **BSI-Kritis** Verordnung zur Bestimmung kritischer Infrastrukturen nach dem BSI-Gesetz » **GeschGehG** Gesetz zum Schutz vor Geschäftsgeheimnissen	» **EBA/GL/2019/02** European Banking Authority Guideline Outsourcing » **DORA** Digital Operational Resilience Act » **KWG** Kreditwesengesetz » **MaRisk** Mindestanforderungen Risikomanagement » **BAIT** Bankaufsichtliche Anforderungen IT	» **ISO 9001** Qualitätsmanagement » **ISO 19011** Auditierung Managementsysteme » **ISO 19600** Compliance Managementsysteme » **ISO 200000** IT-Service-Management » **ISO 27001** Informationssicherheit » **ISO 27702** Informationssicherheitsmaßnahmen » **ISO 27017** Übertragung von Daten » **ISO 27701** Informationssicherheit/Datenschutz » **ISO 27018** Regulierung personenbezogener Daten	» **PS 321** Interne Revision und Abschlussprüfung » **PS 330** Abschlussprüfung Informationstechnologie » **PS 850** Projektbegleitende Prüfung IT » **PS 860** IT-Prüfung außerhalb Abschlussprüfung » **PS 880** Prüfung Software-Produkte » **PS 951** Prüfung IKS-Dienstleister » **PS 980** GoP Compliance-Managementsysteme » **PS 981** GoP Risikomanagementsysteme » **PS 983** GoP interne Revisionssysteme	» **ITIL** Information Technology Infrastructure Library » **COBIT** Control Objectives Information Related Technology

Quelle: PPI AG.

onelle Sicherheit. Daher ist eine Risikoanalyse angezeigt, die sich zum Beispiel auf Gefahren durch ausfallende oder minderwertige Serviceleistungen erstreckt sowie auch auf solche aus Systemen, Prozessen, menschlichen Fehlleistungen oder externen Effekten.

Kleinere und wenig verflochtene Organisationen können sich auf qualitative Ansätze der Risikobeurteilung beschränken. Größere Institute sind hingegen zu anspruchsvolleren quantitativen Ansätzen verpflichtet. Die Ergebnisse dieser Betrachtungen müssen dokumentiert werden und bei der finalen Entscheidungsfindung Berücksichtigung finden. Als Resultat ergibt sich eine fundierte Antwort auf die Frage: Werden Risiken durch die Auslagerung verringert oder erhöht? Was ändert sich?

Genau hinschauen ist Pflicht

Ein weiterer Aspekt, der nicht vernachlässigt werden sollte, ist die Tatsache, dass jeder Serviceprovider an sich auch ein Risiko darstellt. Grundsätzlich muss der künftige Vertragspartner im Rahmen der Sorgfaltsprüfung durch das Finanzinstitut zwingend eine Registrierung oder Zulassung bei einer zuständigen Behörde nachweisen. Dabei muss zwischen den jeweils für Auftraggeber und Provider zuständigen Institutionen eine Zusammenarbeitsvereinbarung bestehen.

Auch darf ein Finanzinstitut nicht als selbstverständlich voraussetzen, dass der künftige Vertragspartner zur Übernahme der Services geeignet ist und die Regulatory Compliance einhält. Hier ist grundsätzlich Kontrolle besser als Vertrauen. Das gilt in besonderem Maße, wenn personenbezogene Daten involviert sind.

Schließlich sollten die Verantwortlichen auch prüfen, ob das Handeln des Serviceproviders mit den Werten und dem Verhaltenskodex der eigenen Organisation kompatibel ist.

Nach der Analyse: Der Vertrag

Sämtliche dieser Vorarbeiten müssen am Ende in ein detailliertes Vertragswerk münden.[1] Darin sind die Verantwortlichkeiten und Belange des Outsourcings bis hin zu einer möglichen Exit-Strategie schriftlich zu fixieren.

Nicht vergessen werden darf in diesem Zusammenhang die genaue Führung des Auslagerungsregisters. Dieses sollte möglichst weitreichende und spezifische Angaben zum jeweiligen Arrangement enthalten. Auf Verlangen muss das Finanzinstitut in der Lage sein, den zuständigen Behörden diese Übersicht oder Teile davon in verarbeitbarer elektronischer Form zu übermitteln.

Zum normalen Informationsfluss kommt auch die Kommunikation bei Krisenlagen. So ist es geboten, die offiziellen Stellen bei maßgeblichen Veränderungen oder schwerwiegenden Vorfällen zu unterrichten, die substanziellen Einfluss auf die weitere Ausführung der Geschäftsaktivitäten haben könnten.

Das Vertragswerk profitiert in jedem Fall von einer guten Vorarbeit. Es enthält zunächst einmal Standards wie eine klare Benennung der Vertragspartner und eindeutige Regelungen zu Rechtswahl, Vergütung, Gewährleistung, Nutzungsrechten, Wettbewerbsverboten, Force Majeure und Change Request Management. Beim Cloud Sourcing gehören aber noch spezifische Absprachen in die Vereinbarung. Dazu zählen:

- Leistungsbeschreibung und Service Level Agreements,
- Bestimmungen zum Auditing,
- Aspekte von Datenschutz und Datenhaltung,
- Verlagerung an Subunternehmen,
- Informationspflichten,
- Beendigung des Vertrags,
- Notfallplanung.

Bereits in der einleitenden Leistungsbeschreibung sollte das Betriebsmodell festgelegt sein, also feststehen, ob es sich um Infrastructure as a Service (IaaS), Platform as a Service (PaaS) oder Software as a Service (SaaS) handelt. Ebenso gehört das Bereitstellungsmodell genannt: Wird in eine Public, Private oder Hybrid Cloud ausgelagert?

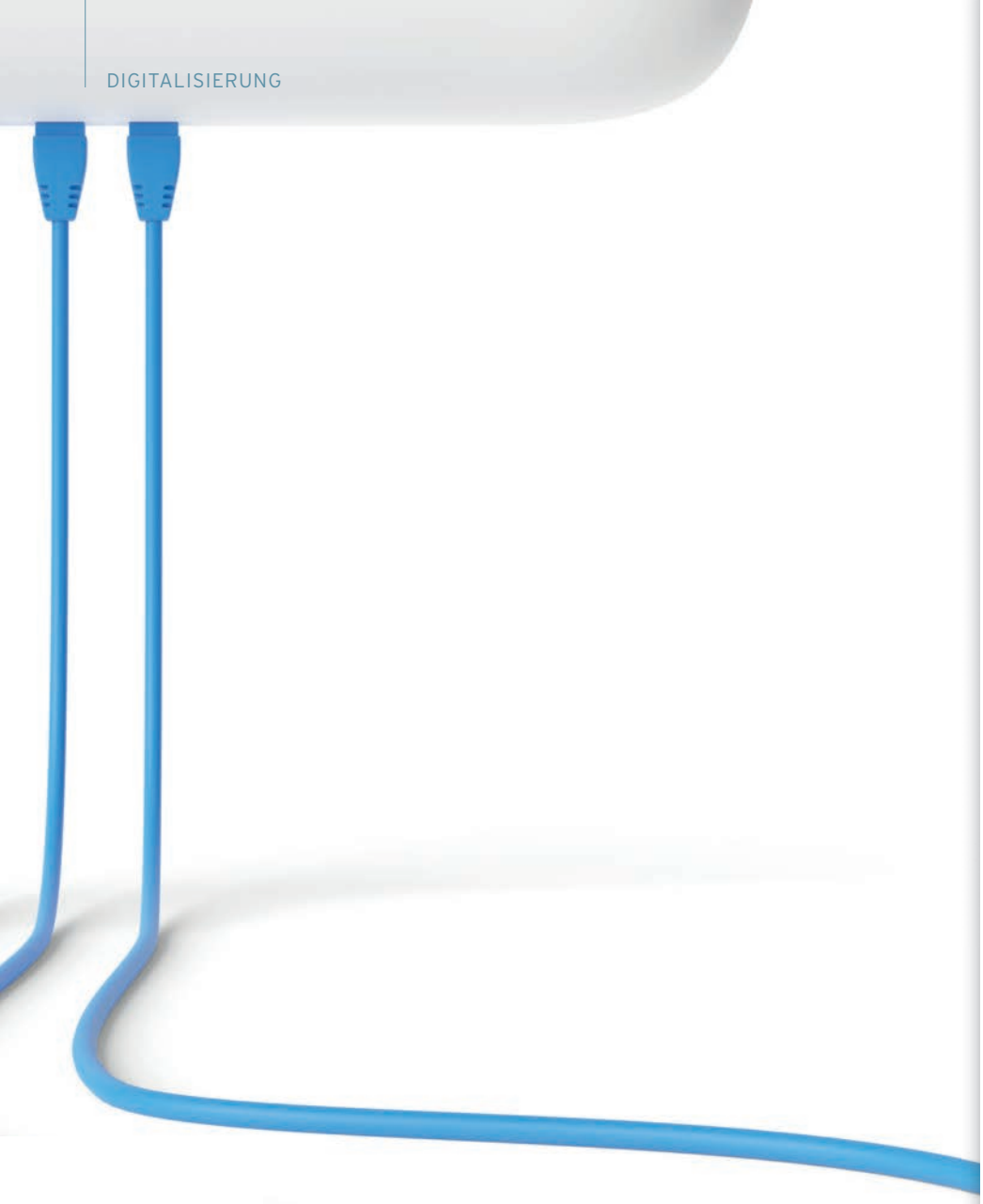
Unbedingt zum Vertragswerk gehören die Service-Level-Agreements (SLAs). Sie definieren die Dienstleistungen hinsichtlich des Niveaus von Performance und Sicherheit. Ein Outsourcing-Vertrag lässt den Auftraggeber natürlich auch nicht ohne Pflichten, etwa was personelle Ressourcen oder die Bereitstellung von Software angeht.

Kontrollen sorgen für Transparenz

Da die Verantwortung beim Finanzinstitut verbleibt, ist es natürlich nur recht und billig, dass sich dieses ausreichende Prüfungsrechte einräumen lässt. Daher muss ein Vertrag auch die Überprüfung der ausgelagerten Prozesse auf Einhaltung aller vereinbarten Parameter festschreiben. Den internen Kontrollinstanzen des Auftraggebers, einem beauftragten Dritten oder der internen Revision des Auftragnehmers muss eine Kontrolle auf Basis eines risikobasierten Ansatzes jederzeit möglich sein– auch vor Ort. Deshalb gehören die physischen Standorte aller mit dem Auftrag verbundenen Rechenzentren in den Vertrag. Der Cloud-Anbieter hat dem Finanzdienstleister dabei sehr weitgehende Rechte einzuräumen: uneingeschränkten Zugriff auf Informationen, Daten, Geräte, Systeme, Netzwerke sowie jederzeitige Einsicht in die durchgeführten Prozesse und Kontrollschritte.

Möchte der beauftragte Dienstleister einzelne (Teil-)Aufgaben an Subunternehmer vergeben, gehört auch dieses vorab vertraglich geregelt. Hier sind grundsätzliche Festlegungen notwendig, welche Prozessschritte auf Dritte verlagert werden dürfen. Die Subunternehmen und die an sie vergebenen Aufgaben müssen benannt sein.

Für die Erfüllung der so weitergereichten Leistungen ist der Auftragnehmer als Vertragspartner des Instituts diesem gegenüber verantwortlich. Informations- und Prüfungsrechte sowie Kontrollmöglichkeiten des Auftraggebers und der Aufsicht gegenüber dem Dienstleister gelten in vollem Umfang auch gegenüber den Subunternehmen. Grundsätzlich sollten sich Finanzdienstleister hinsichtlich der Weitervergabe von Aufgaben an Dritte einen Zustimmungsvorbehalt einräumen lassen.



In der Not und wenn es zu Ende geht

Wenn der Ernstfall einer Störung trotz aller Vorkehrungen doch eintreten sollte, muss der Krisenplan in der Schublade liegen. Dienstleister und Auftraggeber sollten einen vertraglich festgelegten Business-Continuity-Plan vereinbaren. Dieser muss Vorkehrungen, Ressourcen und ausreichende Maßnahmen als Reaktion auf einen Notfall definieren. Der noch weitergehende Desaster-Recovery-Plan beschreibt schließlich die technischen Prozesse und Richtlinien zur Wiederherstellung im Katastrophenfall.

Kommt es beim Betrieb zu Störungen oder Gefahren für die Datensicherheit, ist der Auftraggeber unverzüglich zu informieren. Gleiches gilt bei Aktivitäten Dritter, etwa Datenanfragen, Pfändungen, Beschlagnahmen oder Insolvenz.

Selbstverständlich sollte der Dienstleistungsvertrag auch eine ordentliche Kündigungsfrist innerhalb der Laufzeit festlegen und einen geordneten Ausstiegsprozess fixieren. Der Serviceprovider hat die ausgelagerten Leistungen so lange zu erbringen, bis eine vollständige Übertragung erfolgt ist. Es sind auch Regelungen zur Übergabe von dokumentierten Anpassungen bei Datenformaten zu treffen. Nach Vertragsende und erfolgreicher Rückübertragung der Prozesshoheit hat der Serviceprovider alle Daten vollständig und unwiderruflich zu löschen.

Neben dem ordentlichen ist das außerordentliche Kündigungsrecht ein ganz normaler Vertragsbestandteil. Sie muss möglich sein, etwa wenn

- der Auftragnehmer seine Pflichten schwerwiegend verletzt,
- der Auftraggeber mit dem Bezahlen einer definierten Zahl von Rechnungen im Verzug ist, oder
- die Aufsichtsbehörden die Beendigung des Arrangements anordnen.

FAZIT

Cloud Sourcing liegt im Trend. Zu verlockend sind die Vorteile der Wolke wie Flexibilität, Kosteneinsparungen und IT-Entlastung. Das gilt trotz der Fallstricke in einer reglementierten Branche und der unteilbaren Verantwortung der Finanzinstitute. Eine entsprechend hohe Qualität müssen Projektvorbereitung und Vertragsgestaltung haben. Dazu gehören unbedingt Prüfungen auf Wesentlichkeit und Kritikalität. Dabei gilt: Je bedeutender der Prozess, desto größer sind die Anforderungen an den Dienstleister, seine Auswahl und seine Überwachung. Ein einwandfreier Dienstleistungsvertrag wird komplex sein. Treiber dafür sind vorwiegend die vielschichtigen Vorschriften und Zuständigkeiten seitens der Behörden.

Autoren

Frank Lohmeier ist Mitglied der Geschäftsleitung der auf Finanzdienstleister spezialisierten Unternehmensberatung PPI AG

Holger Bluhm ist Senior Consultant im gleichen Unternehmen und arbeitet in den Schwerpunkten Risikomanagement, Anforderungsmanagement, Prozessanalyse und Reporting.

1 Mehr Informationen dazu finden sich im Whitepaper „Cloud Sourcing und Regulatorik"; kostenloser Download auf der Website der PPI AG.