Die Relevanz von IT-Compliance Prüfungsstandards bei IT-Auslagerungen im deutschen Bankensektor

Benjamin Schwering

Technische Universität München
Chair for Information Systems, Prof. Dr. Krcmar
Boltzmannstr. 3
85748 Garching
benjamin.schwering@in.tum.de

Abstract: Dieser Forschungsbeitrag soll die Relevanz von Prüfungsstandards auf die Gestaltung von Informationssystemen und der IT Landschaft von IT-Dienstleistern im deutschen Bankensektor aufzeigen. Zu diesem Zweck wurde ein empirisch-qualitativer Forschungsansatz gewählt. Es wurde ein Fragebogen konstruiert und an zirka 600 deutsche Banken versendet. Aus den Ergebnissen kann geschlossen werden, dass Banken tatsächlich eine große Nachfrage nach entsprechenden Prüfungsleistungen besitzen und damit weitreichende Anforderungen an die Gestaltung der IT Landschaft ihrer IT-Dienstleister stellen. In diesem Beitrag werden damit die Anforderungen deutscher Banken dargestellt und belegt. Aufbauend auf diesen Beitrag sollte sich weitere Forschung mit den genauen Konsequenzen für IT-Dienstleister und deren IT Landschaft beschäftigen.

1 Einleitung

Im deutschen Bankenumfeld ist eine Auslagerung der IT-Landschaft nicht unüblich und hat in mehreren Beispielen zu großen Erfolgen geführt ([SS08] S. 120 f.). So hat die Deutsche Bank 2007 ihr Rechenzentrum erfolgreich an Dritte ausgelagert. Auch die Stadtsparkassen und Genossenschaften haben seit den siebziger Jahren bereits ihre EDV ausgelagert. Dass das bis heute Bestand hat, spricht ebenfalls dafür, dass die Auslagerung im deutschen Bankenbereich durchaus üblich und erfolgversprechend ist. In diesem Umfeld stellen Banken umfangreiche Anforderungen an ihre IT-Dienstleister. Diese sind insbesondere durch gesetzliche Anforderungen begründet, denen die Banken selbst unterworfen sind. Denn der Bankensektor ist wie kein anderer Wirtschaftszweig einer umfassenden staatlichen Regulierung unterworfen ([HPW07] S. 355; [Ge96])

In der Literatur lassen sich relevante Gesetze finden, die besondere Anforderungen an operationelle Risiken definieren und damit Auswirkung auf die IT im deutschen Bankensystem stellen. (Vgl. dazu im Folgenden [LS06], [GRB04] Kapitel 4.5 und [HPW07] Kapitel L2). Gesetze mit allgemeiner Bedeutung sind im Aktiengesetz (AktG), dem Handelsgesetzbuch (HGB) und den Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme (GoBS) zu finden. In vielen Gesetzen findet sich die Forderung nach einem internen Kontrollsystem, um operationellen Risiken entgegen zu wirken. So fordern § 91 Abs. 2 AktG und § 317 Abs. 4 HGB die Einrichtung und Prüfung eines internen Kontroll- bzw. Überwachungssystems. Außerdem ist der Abschlussprüfer laut § 289 Abs. 1 HGB (für Konzerne gilt § 317 Abs. 2 HGB) dazu verpflichtet, im Lagebericht des Unternehmens, auf die Risiken der künftigen Entwicklung einzugehen.

Für Banken sind zudem das Kreditwesengesetz (KGW) und die Mindestanforderungen an das Risikomanagement (MaRisk) von besonderer Bedeutung. Insbesondere werden restriktive Anforderungen an ein internes Kontollsystem in den MaRisk (MaRisk BT1) definiert. So wird von dem internen Kontrollsystem insbesondere verlangt, dass es „Regelungen zur Aufbau- und Ablauforganisation und; Prozesse zur Identifizierung, Beurteilung, Steuerung, Überwachung sowie Kommunikation der Risiken (Risikosteuerungs- und -controllingprozesse)“ (MaRisk AT1) umfasst. Sollten Teile der Unternehmens-IT, die für das interne Kontrollsystems eines Unternehmens relevant sind, an externe IT-Dienstleister ausgelagert sein, darf das auslagernde Unternehmen unter keinen Umständen die Verantwortung für die internen Kontrollen der ausgelagerten Bereiche abgeben (MaRisk AT 9). Das Unternehmen muss entweder selber die Prozesse in dem Dienstleistungsunternehmen prüfen oder von dem Dienstleistungsunternehmen eine Prüfung der ausgelagerten Prozessteile bzw. der implementierten internen Kontrollen durch einen unabhängigen Wirtschaftsprüfer verlangen. Abbildung 1 verdeutlicht den dargestellten Zusammenhang zwischen Bank und IT-Dienstleister.

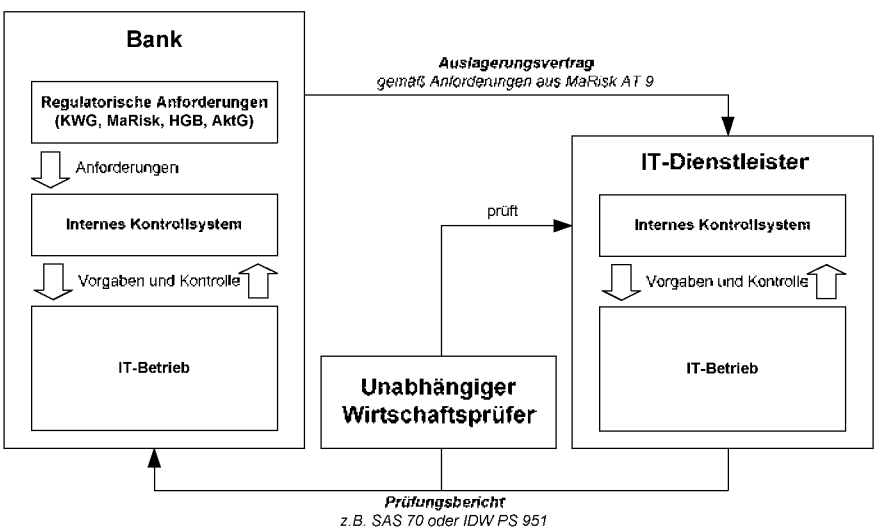

Abbildung 1 Beziehung zwischen Bank und IT-Dienstleister

Für den Zweck gibt es den internationale Prüfungsstandard SAS 70 sowie den deutschen Prüfungsstandard IDW PS 951. Beide beschreiben nicht etwa eine Checkliste mit Kontrollen vor, die der Wirtschaftsprüfer zu testen hat. Der Prüfumfang muss je nach Art der ausgelagerten Dienstleistungen für jeden Bericht definiert werden. Orientieren können sich IT-Dienstleister bei der Einführung der Kontrollen an weit verbreiteten Kontrollziel-Frameworks, wie COSO oder CobiT. Sowohl der IDW PS 951 als auch der SAS 70 definieren zwei unterschiedliche Typen von Prüfberichten, von denen der Typ B bzw. Type II deutlich restriktiver ist. Dieser bewertet im Gegensatz zum einfachen Bericht, der lediglich eine Zeitpunktbetrachtung darstellt, eine Zeitraumbetrachtung. Im Gegensatz zum internationalen Standard SAS 70, der einen hohen Freiheitsgrad bei der Gestaltung zulässt, werden in einem IDW PS 951 Bericht Hinweise auf nicht durchgeführte Kontrollen gegeben.

Das Ziel dieses Forschungsbeitrags ist es, vor diesem Hintergrund, den tatsächlichen Bedarf deutscher Banken an solchen Prüfungsleistungen zu ermitteln, um eine Aussage über deren Relevanz in diesem Bereich treffen z können.

2 Forschungsmethode

Zum beantworten der Forschungsfrage wurde ein empirisch quantitativer Ansatz gewählt. Es wurde ein Fragebogen entwickelt. Dieser Fragebogen wurde erstellt, um die oben erwähnte Fragestellung nach den Anforderungen deutscher Banken an IT-Dienstleister zu beantworten. Es sollte damit auf empirisch-quantitativer Weise belegt werden, wie relevant IT-Compliance Prüfungsstandards im deutschen Bankensektor sind und welche Prüfungsleistungen bzw. Zertifikate besonders wichtig sind. Folgende Fragestellungen sollen daher überprüft werden:

- Ist der Umgang mit operationellen Risiken für Banken besonders wichtig?
- Welche Prüfungsstandards für das interne Kontrollsystem des IT-Dienstleisters sind für deutsche Banken besonders wichtig?

Der Fragebogen ist in drei Bereiche untergliedert: Der erste Teil enthält Fragen zu dem allgemeinen Umgang mit operationellen Risiken in der Bank. Der zweite Teil beinhaltet Fragen zu den Prüfungen des internen Kontrollsystems von IT-Dienstleistern. Abschließend sollte im letzten Teil eine Selbsteinordnung der Banken in verschiedene Kategorien geschehen.

Um die Rücklaufquote der Fragebögen, die an die ca. 200 nicht-Kunden des IT-Dienstleisters gesendet wurden, zu erhöhen, wurden personalisierte Anfragen gesendet soweit es die vorhergehende Recherche zuließ. Adressiert wurde der Fragebogen an Personen innerhalb der Banken, die mit der Prüfung des Informationssystems betraut sind (Interne Revision), oder an der Auslagerung von IT-Aktivitäten mitwirken.

Der Fragebogen wurde so konzipiert, dass er im Internet ausgefüllt werden konnte. Da die Empfänger des Fragebogens von ihrem Arbeitsplatz aus generell Zugang zum Internet besitzen, erschien dieses Medium naheliegend. Zur Realisierung wurde die Freeware-Software Limesurvey® verwendet, die eine komfortable Konstruktion des Online-Fragebogens ermöglichte.

3 Ergebnisse der Umfrage

3.1 Allgemeine Anmerkungen zu der Studie

Von den insgesamt ca. 630 angeschrieben Finanzdienstleistern wurden 62 Fragebögen vollständig ausgefüllt. Damit beläuft sich die Rücklaufquote der Studie auf fast 10%

Obwohl der Fragebogen mit der Unterstützung des IT-Dienstleisters an mehr Banken aus seinen Kundenkreis versandt wurde als an sonstige deutsche Banken, lässt sich im Rücklauf der Fragebögen dieser Einfluss kaum erkennen. Es kann festgestellt werden, dass die Bankenverteilung in der Studie erstaunlich nahe an der tatsächlichen Verteilung von deutschen Banken heranreicht. Durch einen Homogenitätstest kann statistisch nachgewiesen werden, dass die empirische Verteilung der Banken in dieser Studie, repräsentativ für die tatsächliche Verteilung deutscher Banken ist. [1] So kann mit einem äußerst kleinen α-Fehler von 0,01% die Hypothese beibehalten werden, dass beide Verteilungen derselben Grundgesamtheit entstammen. Damit kann diese Studie Aussagen treffen, die auf alle deutschen Bankenarten selber maßen zutreffen.

Die Verteilung der Funktionen der Personen, die diesen Fragebogen ausgefüllt haben, lässt darauf schließen, dass der Fragebogen durchaus kompetent ausgefüllt wurde. So wurde der Großteil der Fragebögen entweder von Mitgliedern der Internen Revision, IT-Managern oder sogar von der Geschäftsleitung ausgefüllt. Nur 10% der Beteiligten erfüllten sonstige Aufgaben in Verbindung mit der Auslagerung von IT-Aufgaben. Davon gaben allerdings einige an, dass sie im Risikomanagement arbeiten oder direkt für die IT-Compliance in der Bank verantwortlich sind.

Um bei der Auswertung die Banken ihrer Größe nach kategorisieren zu können, wurde nach der Bilanzgröße gefragt. Diese wurde in 25%Perzentile gruppiert. Es wurden also vier Gruppen gebildet, die annähernd die gleiche Anzahl an Banken enthalten. Daraus sind folgende Gruppen entstanden:

- kleiner als 600.000
- von 600.000 bis 7,25 Mio.
- größer als 7,25 Mio. bis 480 Mio.
- größer als 480 Mio.

[1] Die Grundlage für die Verteilung von Universalbanken in Deutschland wurde Hartmann-Wendels, Pfingsten, Weber (2007), S. 28 entnommen.

3.2 Ist der Umgang mit operationellen Risiken für Banken besonders wichtig?

Auf die Frage nach den gesetzlichen Regelwerken, die für die Bank relevant sind, gaben alle Beteiligten an, dass sie den Regeln des KWG unterworfen sind. Für zirka 18% der beteiligten Banken ist ebenfalls das AktG von Bedeutung. Lediglich 2% fallen unter die Jurisdiktion des Sarbanes-Oxley Acts (SOA).

Wie bereits dargelegt, kommt dem verantwortungsvollen Umgang mit operationellen Risiken, aufgrund des KWG im Bankensektor, eine besondere Bedeutung zu. Den tatsächlichen Stellenwert dieses internen Kontrollsystems und damit die tatsächliche Relevanz von operationellen Risiken in den befragten Banken, wird im Folgenden dargestellt. So geben immerhin 5% der befragten Banken an, dass das Management operationeller Risiken in Ihrem Unternehmen nicht so relevant sei. Die Unternehmen, die das angegeben haben, fallen sogar alle in die Größenkategorie „größer als 7,25 Mio. bis 480 Mio. “. Allerdings lässt sich allgemein festhalten, dass zumindest bei 93% aller befragten Banken, das interne Kontrollsystem einen durchaus hohen Stellenwert besitzt. Anzumerken ist ebenfalls, dass es keinen besonderen Zusammenhang zwischen dem Stellenwert des internen Kontrollsystems und der Unternehmensgröße gibt. So weisen die beiden Variablen eine Spearman-Korrelation nahe 0 auf.

Auf die Frage nach der Einschätzung, wie sich regulatorische Anforderungen im Bezug auf operationelle Risiken in der Zukunft entwickeln werden, gaben 94% der Banken an, dass die Anforderungen steigen werden. 3% gaben an, dass die Anforderungen gleich bleiben und die restlichen 3% gaben an, dass die Anforderungen sinken werden. Es lässt sich daher feststellen, dass die Banken sich eher auf eine verstärkte Regulierung der operationellen Risiken einstellen.

3.3 Sind die einzelnen Prüfungsstandards für das interne Kontrollsystem des IT Dienstleisters für deutsche Banken wichtig?

Wie zuvor beschrieben, sind Banken bei der Auslagerung von wichtigen IT-Prozessen dazu verpflichtet, einen Nachweis der internen Kontrollen in diesen Prozessen zu erbringen (MaRisk AT9). Welche Prüfungsstandards, vor diesem Hintergrund, für Banken relevant sind, wird im Folgenden beschrieben. Dazu wurde erst grundlegend nach der Wichtigkeit einer solchen Prüfungsleistung gefragt. Danach werden 60%der Banken bei zukünftigen Ausschreibungen auf solche Prüfungsberichte bestehen. 45% der Banken werden solche Prüfungsleistungen auch für die bisher ausgelagerten Prozesse verlangen. Immerhin sehen 24%der Banken eine solche Prüfungsleistung zwar als wichtig an, jedoch nicht als Voraussetzung für eine Auslagerung. Den restlichen 16% ist eine solche Prüfung sogar vollkommen unwichtig oder nicht so wichtig, wie etwa andere Konditionen bei der Auslagerung. Auch an dieser Stelle besteht keine signifikante Korrelation zur Unternehmensgröße der Bank (eine Spearman-Korrelation von 0,161 deutet nicht auf einen signifikanten Zusammenhang hin). Was jedoch überrascht, das ebenfalls keine nennenswerte Korrelation zu dem, zuvor dargestellten Stellenwert des internen Kontrollsystems im eigenen Unternehmen besteht (auch an dieser Stelle deutet eine Spearman-Korrelation von 0,246 nicht auf einen signifikanten Zusammenhang hin). Allgemein lässt sich festhalten, dass Prüfungen des internen Kontrollsystems des IT-Dienstleisters, für Banken durchaus relevant sind.

Um herauszufinden, welche Prüfungsstandards für die Banken besonders relevant sind, wurde zunächst nach der Bekanntheit einzelner Prüfungsstandards gefragt. So ist der IDW PS 330 mit 76% am bekanntesten. Danach folgt der IDW PS 951 mit 53% Bekanntheitsgrad. Bei nur etwa 11% der Banken war der internationale Prüfungsstandard SAS 70 bekannt. Die besondere Bekanntheit des IDW PS 330 ist sicher damit zu erklären, dass die Banken ihr internes Kontrollsystem selbst danach prüfen lassen. Im Gegensatz zum IDW 330, der allgemein das interne Kontrollsystem in einem Unternehmen prüft, ist der IDW PS 951 speziell auf die Prüfung des internen Kontrollsystems bei Auslagerung ausgerichtet. An dieser Stelle sei noch darauf hingewiesen, dass nur ca. 58%der Banken, die den IDW PS 951 kennen, auch über den Unterschied zwischen dem einfachen Typ A und restriktiveren Typ B Bescheid wussten. Bei den wenigen Banken, bei denen der SAS 70 bekannt ist, ist zu 88% auch der Unterschied zwischen Typ I und Typ II des SAS 70 Berichts bekannt.

Weiterhin wurde gefragt, welcher Prüfungsstandard sich aus Sicht der Bank am besten eignet, um ihre Anforderungen, bezüglich der Testierung des internen Kontrollsystems, zu erfüllen. Dazu konnten die Banken auf einer Likert-Skalar von eins bis fünf wählen, für wie geeignet sie die einzelnen Prüfungsstandards halten. Dabei bedeutete eins komplett geeignet und fünf nicht geeignet. Für die Auswertung wird auf den Median zurückgegriffen, der als Maß für den Mittelwert bei einer ordinal-skalierten Variabel verwendet werden kann.[2] Im Ergebnis ist festzustellen, dass sowohl der IDW PS 951 Typ B als auch der IDW PS 330, aus Sicht der befragten Banken, als durchaus geeignet erscheint, ihre Anforderungen zu erfüllen. So besaßen beide Prüfungsstandards einen Median von 2 („gut geeignet"). Der internationale Prüfungsstandard SAS 70 besitzt selbst unter den Banken, die ihn überhaupt kennen, eine eher untergeordnete Bedeutung. Der Typ I besaß einen Median von 5 ("ungeeignet") und der Typ II mit einem Median von 3 ("bedingt geeignet").

4 Zusammenfassung und Ausblick

In der obigen Auswertung wurden die Anforderungen deutscher Banken an Prüfungsleistungen, nach denen sich IT-Dienstleister ausrichten können, vorgestellt. Es wurde gezeigt, dass das interne Kontrollsystem, unabhängig von der Unternehmensgröße, schon heute einen hohen Stellenwert für Banken besitzt. Auch in Zukunft werden entsprechende Regulierungen aus Sicht der Banken immer restriktiver werden. Die Prüfung des internen Kontrollsystems bei dem IT-Dienstleister ist für Banken durchaus relevant und viele Banken werden entsprechende Zertifikate bei zukünftigen Ausschreibungen verlangen. Unter den Prüfungsstandards sind insbesondere die Prüfung nach IDW PS 330 und IDW PS 951 Typ B von großer Bedeutung.

Als Konsequenz ergeben sich damit besondere Anforderungen an die Unternehmens-IT von IT-Dienstleistern im Bankensektor. Diese müssen ihre IT-Landschaft compliant zu den Anforderungen aus den entsprechenden Prüfungsstandards ausrichten. So wird z.B. im IDW PS 951 auf den COSO Framework (Committee of Sponsoring Organizations of the Treadway Commission) zum Aufbau eines internen Kontrollsystems verwiesen. Für die IT-Landschaft hat COSO allerdings eine geringere Bedeutung. So werden zwar Kontrollen für die Finanzberichtserstattung (die im allgemeine durch IT-Systeme realisiert wird) und die allgemeine Regeleinhaltung definiert, direkte IT bezogene Kontrollen gibt es jedoch nicht ([FG07] S. 76.). Ein gutes Framework für effektive IT-Kontrollen bietet dagegen CobiT (Control Objectives for Information and related Technology), das ein Referenzmodellrahmen für die Planung und Steuerung des Einsatzes von Informationstechnik ist ([Me04] S. 79). Damit stellt es eine gute Ergänzung zu COSO dar ([FG07] S. 77).

[2] Auf die Angabe eines Streuungsmaßes wird an dieser Stelle verzichtet, da es für ordinal-skalierte Daten kaum ein aussagekräftiges Streuungsmaß gibt. So bezieht die Spannweite z.B. nur die größten und die kleinste Ausprägung mit ein.

Um sich nach diesen Standards compliant auszurichten wird auf Seiten des IT-Dienstleisters ein nicht geringer Aufwand entstehen. Weitere Forschung sollte sich der Frage widmen wie dieser Aufwand genau aussieht bzw. aus welchen Bestandteilen dieser besteht und welchen Umfang er besitzt. Es sollte eine Abwägung zu den Nutzen solcher Prüfungen des internen Kontrollsystems stattfinden.

Literaturverzeichnis

[FG07] Fröhlich, M.; Glasner, K.: IT Governance: Leitfaden für eine praxisgerechte Implementierung. 1. Aufl., Gabler Verlag, Wiesbaden 2007.

[Ge96] Gerlach, R.: Deutsche Regulierungslust - Segen oder Fluch für das Kreditgewerbe? . In: Sparkasse, 09 (1996); S. 404 - 408.

[GRB04] Grob, H. L.; Reepmeyer, J.-A.; Bensberg, F.: Einführung in die Wirtschaftsinformatik. 5. Aufl., Vahlen Verlag, München 2004.

[HPW07] Hartmann-Wendels, T.; Pfingsten, A.; Weber, M.: Bankbetriebslehre. 4. Aufl., Springer-Verlag, Berlin Heidelberg New York 2007.

[LS06] Lensdorf, L.; Steger, U.: IT-Compliance im Unternehmen. In: Der IT-Rechtsberater, H. 8 (2006), S. 206-210.

[Me04] Menzies, C.: Sarbanes-Oxley Act: Professionelles Management interner Kontrollen. 1. Aufl., Schäffer-Poeschel Verlag, Stuttgart 2004.

[SS08] Schüller, B.; Simon, A.: Verbesserung des Unternehmensertrags durch Sourcing. In: Outsourcing in Banken: Mit zahlreichen aktuellen Beispielen. 2. Aufl., Gabler Verlag, Wiesbaden 2008.