

# Vorgelagerte Auditierung

Rating von Firmenkundenkrediten muss die IT-Compliance einschließen

In vielen Banken und Sparkassen stellt sich derzeit die Frage, ob hinsichtlich bestehender IT-Risiken der Blick hinter die Kulissen ihrer Firmenkunden lohnt. Immerhin gerät deren Bonität schnell ins Wanken, wenn hohe Haftungsforderungen auf die Geschäftsführung zukommen oder Industriespionage ihren Produktabsatz und damit ihre Wirtschaftlichkeit in Frage stellt.

Im Falle einer Kreditentscheidung hat ein Firmenkundenberater das Recht, sich von seinem Kunden Angaben über die in seinem Unternehmen definierten Standards zur Einhaltung der IT-Compliance offenlegen zu lassen. Was ohnehin ein Teil der Wirtschaftsprüfung (IDW Prüfungsstandards, Prüfungsstandard 330<sup>1</sup>) ist, macht im Sinne einer vorgelagerten Auditierung für Banken und Sparkassen durchaus Sinn. Immerhin entstehen in Folge der Wirtschaftsprüfung unter Umständen kostenintensive Auflagen, die im Businessplan berücksichtigt werden müssen. Je mehr die Institute im Rahmen der Kreditvergabeentscheidung wissen, um so besser lassen sich IT-Risiken und daraus resultierende Präventivmaßnahmen abschätzen. Darum ist es für Banken und Sparkassen im Vorfeld einer Kreditvergabe hilfreich, von ihren Firmenkunden Antworten beispielsweise auf die folgenden Fragen zu erhalten:

- Wie organisiere und überwache ich die Sicherheit digitaler Informationen in meinem Unternehmen?
- Ist meine Informationstechnik für das Unternehmen und auch für meine Kunden jederzeit verfügbar?
- Wie archiviere ich meine digitalen Daten?
- Wie gewährleiste ich einen ausreichenden Schutz meiner digitalen Daten?

## IT Compliance als Teil des Firmenkundenratings

Eine realistische Einschätzung der Risikolage ist nur mit einem tiefgreifenden IT- und auch Prozesswissen möglich, das niemand von einem Firmenkundenbetreuer erwarten kann. Darum sollen ihn entsprechende Standards

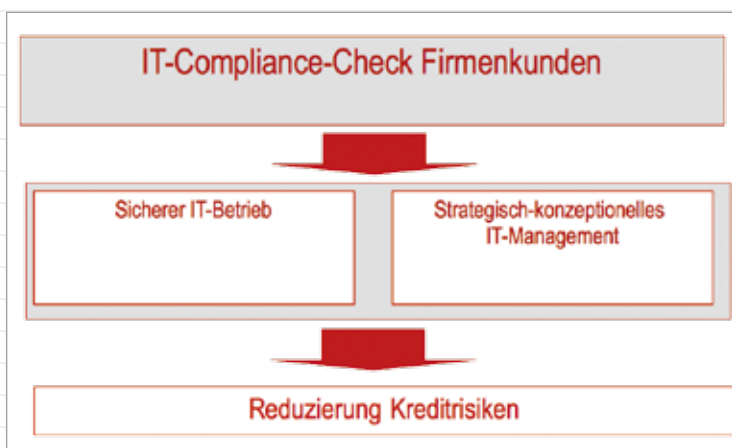


Abb. 1: IT-Compliance-Check Firmenkunden

(Quelle: P3N BERATUNGS GMBH)

darin unterstützen, die richtigen Fragen zu stellen und die Antworten den IT-Risiken und ihren möglichen (finanziell belastenden) Folgen entsprechend einzuordnen. Die P3N BERATUNGS GMBH begleitet Banken und Sparkassen dabei, jene Standards zu schaffen oder bestehende Vorgaben so zu adaptieren, dass sie für die Evaluierung der IT-Risiken ihrer Firmenkunden passen. Der IT-Compliance-Check (siehe Abb. 1) aus dem Zwickauer Beratungshaus orientiert sich an den IDW-Prüfungsstandards. Er schafft damit die Voraussetzungen für ein realistisches Rating von Firmenkundenkrediten unter Einbeziehung der IT-Compliance und gibt den Firmenkundenberatern das dafür notwendige Werkzeug in die Hand. Darüber hinaus modelliert P3N mit den Instituten nachgelagerte Prozesse, wie etwa die Bewertung und Gewichtung der IT-Risiken und daraus abzuleitende Maßnahmen. Von dieser Herangehensweise profitieren auch die Firmenkunden selbst. Die gewonnene Übersicht führt oft zu bilanzfreundlichen Korrekturen hinsichtlich der Rückstellungen für bestehende Risiken. Zum anderen ebnet die IT-Sicherheitsanalyse dem Firmenkunden den Weg hin zu zielführenden Präventivmaßnahmen und der Gestaltung einer funktionierenden IT-Compliance.

## Fazit

Die Einschätzung der IT-Sicherheitslage muss Teil der Risikoanalyse im Firmenkundenkreditgeschäft sein. Mittels etablierter Standards schaffen Banken und Sparkassen ein einfaches, einheitliches und transparentes Vorgehen hinsichtlich der Evaluierung der Einhaltung von IT-Compliance-Richtlinien beim Kunden – ohne bankinterne Ressourcen zu binden. Wie auch immer die Ergebnisse der Analyse ausfallen: Sie sind sowohl für den Firmenkunden als auch für die Banken und Sparkassen ein Gewinn.

<sup>1</sup> vgl. [http://www.it-Audit.com/unterstuetzung\\_jahresabschlusspruefung\\_audit\\_support\\_nach\\_idw\\_ps\\_330\\_html](http://www.it-Audit.com/unterstuetzung_jahresabschlusspruefung_audit_support_nach_idw_ps_330_html)



Der Autor:  
**Frank Hummel,**  
Geschäftsführer, P3N BERATUNGS GMBH