Sehr geehrte Damen und Herren,

wie ich auf Ihrer Homepage gesehen habe, arbeiten Sie derzeit an einer Überarbeitung der MaRisk für Banken.

Erlauben Sie mir als Management Berater und Fachbuchautor hierzu folgende Anregungen, die sich ergeben haben, weil ich aus fachlichem Interesse AT 7.2 gelesen haben:

- Zur Unterscheidbarkeit von der "MaRisk VA" sollte der Titel analog in "MaRisk BA" verändert werden.

- In AT 7.2, Absatz 2, Erläuterungen, haben Sie die Angabe des internationalen Standards korrekt in ISO/IEC 27002 geändert. Im Hinblick auf das SIcherheitsmanagement empfehle ich Ihnen, hier zusätzlich die ISO/IEC 27001, Informationssicherheitsmanagementsysteme, anzugeben. Da die Sicherheit und Verfügbarkeit der IT außerdem wesentlich vom Zusammenspiel der IT-Sicherheitsprozesse bzw. des Informationssicherheitsmanagements mit den verschiedenen IT-Prozessen abhängt, empfehle ich Ihnen ferner, dort auch auf die ISO/IEC 20000, Teil 1 und Teil 2, zu verweisen. Sowohl die ISO/IEC 27001 als auch die ISO/IEC 20000 erlauben zudem eine Zertifizierung. Dies kann nicht zuletzt im Rahmen des Outsourcing der IT für Banken, aber auch für Versicherungen als Orientierung interessant sein.

- In AT 7.2, Absatz 2, haben Sie die MaRisk ergänzt um:
"... insbesondere sind Prozesse für eine angemessene IT-Berechtigungsvergabe einzurichten."
sowie in den Erläuterungen geschrieben:
"IT-Zugriffsrechte
Es ist sicherzustellen, dass jeder Mitarbeiter nur über die Rechte verfügt, die er für seine Tätigkeit benötigt (Prinzip der minimalen Rechtevergabe)."
Dies ist gegenüber der bisherigen Regelung ein Fortschritt und verfolgt die korrekte Zielsetzung. Die Erläuterung stellt zudem klar, dass der Nutzer im Betrieb (also nicht nur bei der Vergabe) auch nur die Rechte haben soll, die er für seine Tätigkeit benötigt. Die Erläuterung in Klammern hinsichtlich des "Prinzips der minimalen Rechtevergabe" würde meiner Meinung nach daher dementsprechend besser "Prinzip der minimalen Rechte" lauten.
Dies insbesondere auch deshalb, weil sich im operativen Geschäft oftmals die Situation ergibt, dass die Vergabe an sich korrekt ist, durch Wechsel in einen anderen Verantwortungsbereich jedoch bestehende Rechte nicht gelöscht werden.

Sollten sich Ihrerseits Fragen hierzu ergeben, stehe ich zu deren Beantwortung gerne zur Verfügung.

Ich freue mich, wenn diese Anregungen für Sie nützlich sind.

Mit freundlichen Grüßen
Dr.-Ing. Klaus-Rainer Müller