IT-Organisation

Analyse „wesentlicher Veränderungen" nach MaRisk AT 8.2

Aufgrund der MaRisk AT 8.2 sind wesentliche Veränderungen in der IT-Organisation gesondert zu beachten und zu dokumentieren. Doch wie kann der Nachweis erfolgen, dass nicht-wesentliche Veränderungen tatsächlich nicht wesentlich sind?

Die Norm des AT 8.2 MaRisk besagt, dass vor wesentlichen Änderungen in der IT-Organisation die Auswirkungen der geplanten Änderungen zu prüfen sind: „Vor wesentlichen Veränderungen in der Aufbau- und Ablauforganisation sowie in den IT-Systemen hat das Institut die Auswirkungen der geplanten Veränderungen auf die Kontrollverfahren und die Kontrollintensität zu analysieren. In diese Analysen sind die später in die Arbeitsabläufe eingebundenen Organisationseinheiten einzuschalten.

Im Rahmen ihrer Aufgaben sind auch die Risikocontrolling-Funktion, die Compliance-Funktion und die Interne Revision zu beteiligen."[1]

Doch was lässt sich unter einer „wesentlichen Veränderung" in der IT-Organisation verstehen und wie lässt sich die Norm in der Praxis umsetzen?

Eine „wesentliche Veränderung" setzt i.S. der MaRisk AT 8.2 voraus, dass die Veränderung unter anderem

- einen oder mehrere wesentliche Prozesse direkt betrifft,
- erhebliche Auswirkungen auf die Aufbau- und Ablauforganisation/das Gesamtunternehmen haben wird,
- erhebliche finanzielle sowie rechtliche Auswirkungen haben wird und folglich
- entsprechende Auswirkungen auf das interne Kontrollverfahren und die Kontrollintensität der Bank zu erwarten sind.

Des Weiteren sind zunächst grundlegende inhaltliche Fragen (Zeitpunkt, Aufbau und Inhalte der Analyse) zu klären.

Zeitpunkt und Ablage der Analyse

Die Analyse ist – wie in den MaRisk AT 8.2 deklariert – vor jeder Veränderung vorzunehmen. Doch was heißt das in der Praxis?

Die Analyse sollte zu Beginn eines jeden Projektes oder Einführungsprozesses erfolgen und kann idealerweise dort auch hinterlegt sein. Danach können weitere Schritte wie z. B. die Test- und Freigabephase erfolgen.

Dabei sind nicht nur die Fachabteilungen neben dem IT-Management involviert. Auch das Risikocontrolling, das Compliance-Beauftragtenwesen und die Interne Revision sind einzubinden und die Analyse/Dokumentation ist zur Kenntnis vorzulegen.

Aufbau und Inhalte der Analyse

Eine aussagekräftige Analyse setzt zunächst die Klärung der Analyse-Inhalte und des Analyse-Aufbaus voraus. Es empfiehlt sich, ein Musterformular zu erstellen bzw. zu verwenden, um eine einheitliche, standardisierte Vorgehensweise und Dokumentation sicherzustellen. Beispielhaft soll an dieser Stelle auf die Möglichkeit zur Nutzung einer Standard-Arbeitsanweisung des Genossenschaftsverbands (z. B. 100.04.07. Rahmenbedingungen zu wesentlichen Änderungen der IT und Organisation)hingewiesen werden.

Folgende Inhalte sind in der Analyse zu empfehlen:

- Welche Fachbereiche sind betroffen?
- Wer ist für die Analyse verantwortlich?
- Welche Veränderungen sind mit welchen Anwendungen geplant?
- Zu welchem Zeitpunkt ist die Veränderung geplant?
- Welche Zielsetzung ist mit der Veränderung verbunden?
- Welche Kriterien sprechen für eine wesentliche Veränderung nach MaRisk AT 8.2?
- Wird die Anwendung erstmalig eingesetzt?

>

[1] BaFin – Bundesanstalt für Finanzdienstleistungsaufsicht, https://www.bafin.de/SharedDocs/Downloads/DE/Rundschreiben/dl_rs0917_marisk_Endfassung_2017_pdf_ba.pdf?__blob=publicationFile&v=5 (Stand: 03.04.2019)

- Sind wesentliche und/oder unwesentliche Geschäftsprozesse betroffen?
- Liegt eine wesentliche oder nicht-wesentliche Veränderung vor? (mit kurzer Begründung)

Damit die Analyse den Anforderungen der MaRisk AT 8.2 entspricht, ist diese durch den Auftraggeber, den Freigeber sowie zur Kenntnis durch das Risikocontrolling, das Compliance-Beauftragtenwesen und durch die Interne Revision (digital) unterzeichnen zu lassen.

Kriterien der Wesentlichkeit und Auswirkungsanalyse

Zu den Kriterien der Wesentlichkeit zählt, ob sich die wesentlichen Veränderungen in der IT-Organisation auf die Stabilität/Funktionsfähigkeit des wesentlichen Geschäftsprozesses auswirken. Wenn beispielsweise die Einführung einer neuen Anwendung lediglich unterstützenden Charakter hat und bei einem möglichen Ausfall der Geschäftsprozess weiter nahezu uneingeschränkt fortgeführt werden kann, wäre dies ein Begründungsansatz für eine nicht-wesentliche Veränderung.

Darüber hinaus sind die Einhaltung der rechtlichen Anforderungen der Bank sowie mögliche finanzielle Risiken, aber auch der Schutzbedarf der Daten und die Gesamtauswirkung auf das Unternehmens in der Wesentlichkeitsprüfung einzubeziehen.

Kontrollverfahren und Kontrollintensität in der Praxis

Was ist mit Auswirkungen auf Kontrollverfahren und Kontrollintensität in den MaRisk AT 8.2 gemeint?

Gemäß MaRisk AT 1 Ziffer 1 setzt sich das interne Kontrollverfahren aus dem internen Kontrollsystem (kurz IKS) und der Internen Revision zusammen. In der Praxis können im Bereich der Informationssicherheit/des IT-Managements beispielsweise wiederkehrende Kontrollaufgaben (Rezertifizierung der Zugriffs- und Zutrittsberechtigungen, Überprüfung der IT-Arbeitsanweisungen, Test-Freigabe-Verfahren von Releases etc.) zu dem in der Bank implementierten Kontrollsystem zählen.

Die Kontrollintensität legt dabei fest, wie das Kontrollverfahren bzw. das interne Kontrollsystem konkret umgesetzt wird (z. B. Kontrollzeitpunkte/-intervalle).

Das Ergebnis der Wesentlichkeitsprüfung kann unter anderem sein, dass das IKS und somit auch das Kontrollverfahren der Bank nicht direkt betroffen sind. Dieses wäre ein weiteres Argument für eine nicht-wesentliche Veränderung.

AUTOR UND ANSPRECHPARTNER

Benjamin Wellnitz
Beauftragter Informationssicherheit & Datenschutz,
E-Mail: benjamin.wellnitz@dz-cp.de

Folglich ist immer die Analyse nach MaRisk AT 8.2 voranzustellen, um entsprechende Prüfungsergebnisse herleitbar aufbauen zu können.

Sofern eine wesentliche Veränderung festgestellt wurde, sollte eine detaillierte Auswirkungsanalyse erstellt werden. Die Auswirkungsanalyse sollte

- die Auswirkungsintensität (Grad der Betroffenheit),
- Auswirkungen auf die Verfügbarkeit von IT-Systemen,
- Auswirkungen auf die Risikosituation (z. B. Adressausfallrisiko, Marktpreisrisiko, Liquiditätsrisiko) sowie
- erhöhte Auswirkungen auf operationelle Risiken darstellen.

Zu empfehlen ist, dass die genannten Dimensionen in der Beurteilung über eine Skalierung/Klassifizierung (z.B. 1 = unwesentlich bis 4 = wesentlich) beantwortet werden.[2]

Die detaillierte Auswirkungsanalyse braucht beim Ergebnis einer nicht-wesentlichen Veränderung nicht vorgenommen zu werden.

Weitere Schritte nach der Analyse

Nach der Analyse sollte in der nächsten Phase die Konzeption und Implementierung der erforderlichen organisatorischen Maßnahmen festgelegt und umgesetzt werden.

In der Regel wird eine Risikoanalyse gemäß MaRisk AT 7.2 losgelöst vom Ergebnis der Analyse nach MaRisk AT 8.2 vorgenommen. Hierbei werden mögliche Bedrohungsszenarien durch die identifizierten Risiken betrachtet. Um die Risiken (Bruttorisiko) zu minimieren, sind entsprechend Maßnahmen umzusetzen (z. B. Schulungen, um die Risiken einer fehlerhaften Erfassung/Konfiguration des neuen Systems zu minimieren). Dabei ist der Anpassungsbedarf an das interne Kontrollsystem, aber auch der Veränderungsbedarf in der Aufbau- und Ablauforganisation (z. B. Stellenbeschreibungen, Arbeitsanweisungen, Kompetenzen, Prozesse) zu überprüfen.

Im Anschluss erfolgt eine für Dritte nachvollziehbare Dokumentation.

Fazit

Grundsätzlich sind alle Veränderungen in der IT-Organisation auf die Wesentlichkeit vor der geplanten Veränderung in der IT-Organisation zu überprüfen. Das Ergebnis kann sowohl eine wesentliche als auch eine nicht-wesentliche Veränderung sein.

Bei einer fundiert begründeten Feststellung einer nicht-wesentlichen Veränderung kann auf eine Detailanalyse verzichtet werden.

Zu beachten ist, dass eine Wesentlichkeitsfeststellung einen erhöhen Maßnahmen- sowie Dokumentationsaufwand nach sich zieht und gut überlegt sein sollte. ▬

[2] vgl. Geiersbach, Karsten, Prüfungserfahrung zu AT 8.2 MaRisk, https://www.fc-heidelberg.de/pruefungserfahrungen-zu-8-2-marisk-2/ (Stand: 03.04.2019)