BAIT

IT-Strategie: Bestens vernetzt

Die Einführung der neuen MaRisk und der BAIT liegt jetzt schon einige Monate hinter uns. Zeit für den Lackmustest: Welche Umsetzungsstrategie hat sich bewährt? Wie geht man es am besten an? Wie kann man sicherstellen, den Ansprüchen zu genügen?

Die Änderungen in der MaRisk (27. Oktober 2017), die die Anforderungen an die Informationstechnologie (IT) betreffen, sind nicht besonders umfangreich. Die meisten Neuerungen betreffen das Auslagerungsmanagement. Die Bankaufsichtlichen Anforderungen an die IT (BAIT, 3. November 2017) werden dagegen konkreter in den Forderungen.

Sie befassen sich mit acht Hauptthemen:

1. IT-Strategie,
2. IT-Governance,
3. Informationsrisikomanagement,
4. Informationssicherheitsmanagement,
5. Benutzerberechtigungsmanagement,
6. IT-Betrieb,
7. IT-Projekte/Anwendungsentwicklungen und
8. Auslagerung/sonstiger Fremdbezug.

Beschäftigt man sich näher mit den Themen der BAIT, wird der ‚große Wurf', das notwendige Zusammenspiel der einzelnen Themen, schnell sehr deutlich.

1. IT-Strategie

Am Anfang steht die Unternehmensstrategie. In ihr sollten Aussagen zur IT getroffen werden. Anders ausgedrückt: Die strategischen IT-Ziele müssen konsistent zur Geschäfts- und Risikostrategie des Unternehmens aufgebaut sein und sich an diesen ausrichten.

Die IT-Strategie sollte darüber hinaus Antworten auf alle sieben weiteren Themen der BAIT geben.

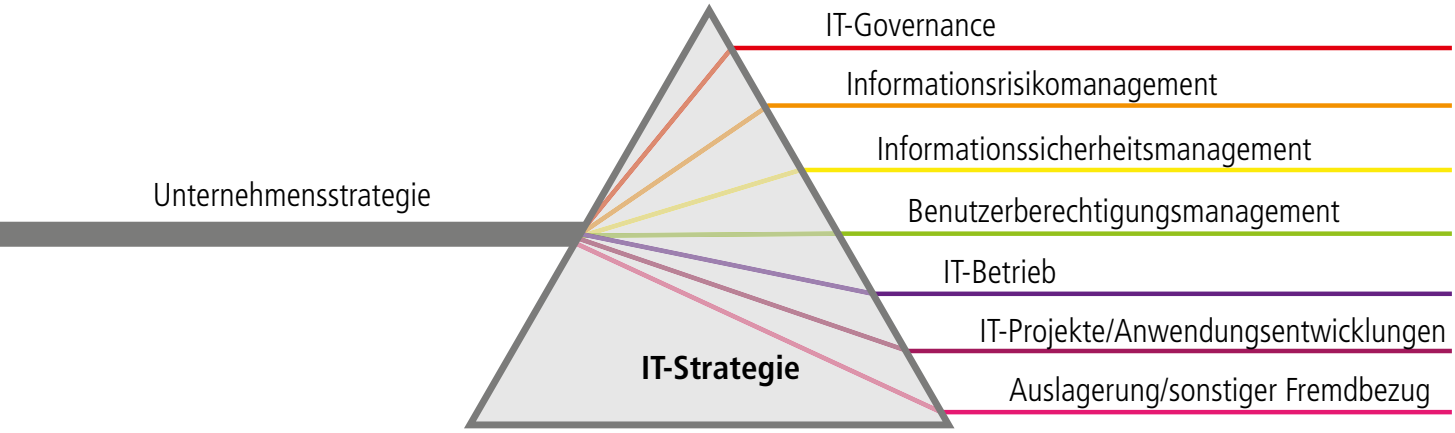
Sie beschreibt die strategische Entwicklung der IT-Aufbau- und IT-Ablauforganisation, der IT-Architektur sowie die dazugehörigen IT-Prozesse. Neben einer Aussage zu Sicherheitsstandards und Eckpunkten der Informationssicherheitsorganisation sollte sie das Notfallmanagement im IT-Betrieb berücksichtigen.

Wenn das Unternehmen auf eigenbetriebene und -entwickelte IT-Systeme oder auf Auslagerung setzt, sind in der IT-Strategie auch Aussagen zu diesen Themen aufzunehmen.

Die Messung und Erreichung der strategischen Ziele sollte mit Maßnahmen konkretisiert und die Erreichung der Ziele überprüft werden.

2. IT-Governance

Die in der IT-Strategie getroffenen Aussagen finden direkten Eingang in die IT-Governance. Hier wird geprüft, ob die Steuerung und Überwachung des Betriebs und der Weiterentwicklung der IT-Systeme einschließlich der IT-Prozesse auf Basis der IT-Strategie geschehen.



Zur Steuerung des Betriebs und der Entwicklung der IT-Systeme sollten quantitative und qualitative Kriterien festgelegt und überwacht werden. Bei Veränderungen an IT-Aufbau oder IT-Ablauf müssen Aktivitäten und Prozesse direkt angepasst werden.

Regelungen zum Informationsrisikomanagement und Informationssicherheitsmanagement sind zu treffen und schriftlich zu fixieren, ebenso wie Regelungen zu IT-Aufbau und IT-Ablauf.

3. Informationsrisikomanagement

IT-Systeme und IT-Prozesse müssen Integrität, Verfügbarkeit, Authentizität und Vertraulichkeit sicherstellen.

Dafür sind klare Verantwortlichkeiten, Kontrollen, Kommunikationswege und Kompetenzen zu definieren. Um das Informationsrisikomanagement sauber zu betreiben, müssen zudem Überwachungs- und Steuerungsprozesse eingesetzt, Berichtspflichten eingehalten und Schutzbedarfe ermittelt werden.

4. Informationssicherheitsmanagement

Das Informationssicherheitsmanagement legt feste Aufgaben und Verantwortliche fest.

So hat der Informationssicherheitsbeauftragte die Aufgabe, eine Informationssicherheitsleitlinie zu erstellen. IT-Dienstleister werden nach den Vorgaben der Leitlinie überwacht. Jede Auslagerung ist im Rahmen eines IT-Projektes zu steuern und zu dokumentieren.

Darüber hinaus muss eine vierteljährliche Berichterstattung bei wesentlichen Auslagerungen vereinbart werden.

5. Benutzerberechtigungsmanagement

Im Rahmen des Benutzerberechtigungsmanagements werden die Kompetenzen definiert, aufeinander abgestimmt und gepflegt. Benutzerberechtigungen müssen regelmäßig und auch anlassbezogen überprüft werden. Das gilt auch bezüglich der Schnittstelle bei Auslagerungen. Technische User müssen jederzeit zweifelsfrei zuzuordnen sein.

Grundsätzlich dürfen Berechtigungen nur nach einer dokumentierten Genehmigung und Kontrolle vergeben werden. Die Vergabe, Änderung, Deaktivierung, Löschung und Rezertifizierung von Benutzerrechten sind nachvollziehbar zu dokumentieren. Dazu muss jedes Unternehmen außerdem einen Prozess etablieren, der den Soll-Ist Abgleich der Berechtigungen prüft.

Zudem muss sichergestellt werden, dass das Benutzerberechtigungskonzept eingehalten wird und nicht umgangen werden kann (technisch-organisatorische Maßnahmen).

6. IT-Betrieb

Nach den BAIT muss der IT-Betrieb zwingend mit den Anforderungen der IT-Strategie übereinstimmen.

Es muss dokumentiert werden, welche IT-Systeme eingesetzt werden und wie deren Beziehungen untereinander sind. Diese Aufstellung ist zu verwalten, zu erfassen und regelmäßig zu aktualisieren.

AUTORIN UND ANSPRECHPARTNERIN

Sandra Sitter
Leiterin IT & Projekte,
E-Mail: sandra.sitter@geno-tec.de

Die BAIT setzen weiter voraus, dass Prozesse zu Änderungen an IT-Systemen, abhängig von Art, Umfang, Komplexität und Risikogehalt, festgelegt sind und dann auch angewandt werden. Änderungen an IT-Systemen müssen dokumentiert, bewertet, priorisiert, genehmigt, koordiniert und sicher umgesetzt werden.

Die BAIT fordern zudem, dass Störungen und Ausfälle sauber dokumentiert, Ursachen analysiert, Maßnahmen eingeleitet und überwacht werden.

Nicht nur die DSGVO, sondern auch die BAIT fordern ein Datensicherungskonzept. Das Datensicherungskonzept muss Anforderungen zur Verfügbarkeit, Lesbarkeit, Aktualität der Kunden- und Geschäftsdaten sowie deren Verarbeitung ableiten. Datensicherungen müssen regelmäßig, mindestens jährlich getestet werden.

7. IT-Projekte und Anwendungsentwicklungen

Alle IT-Projekte und Anwendungsentwicklungen sind sauber und nachvollziehbar zu dokumentieren.

Aus einer Dokumentation müssen die Ziele und Anforderungen klar hervorgehen. Sowohl der Projektverlauf als auch die Umsetzung einer Entwicklung sind festzuhalten. Bei Entwicklungen liegt dabei insbesondere das Augenmerk auf einem zu installierenden Test- und Freigabeverfahren. Dabei ist zu dokumentieren, dass die Anforderungen an Funktion und Leistung richtig umgesetzt werden.

8. Auslagerung und sonstiger Fremdbezug von IT-Dienstleistungen

Als IT-Dienstleistungen werden alle Ausprägungen des IT-Bezugs definiert. In dieser Definition wird der AT 9 MaRisk nochmal konkreter gefasst.

Die Gesamtverantwortung der Auslagerung bleibt immer bei der Geschäftsleitung. Die BAIT fordern explizit Risikoanalysen. Änderungen müssen bewertet werden. Zu einer Auslagerung bedarf es regelmäßig auch einer Exit-Strategie. Zudem muss der Auslagerungsdienstleister überwacht werden.

Fazit

Um den Anforderungen der BAIT gerecht zu werden, müssen die einzelnen Punkte ineinandergreifen. Nur wenn sie aufeinander abgestimmt sind, erfüllt ein Unternehmen die gesetzlichen Anforderungen.

Zu ergänzen wäre, dass auch nur dann das Unternehmen mit Blick auf die IT sicher aufgestellt ist.

In der Praxis punktet langfristig eine ganzheitliche Herangehensweise ausgehend von der Unternehmensstrategie. Sie allein gewährleistet die erforderlichen Sicherheitsstandards und ermöglicht darüber hinaus die notwendige Flexibilität hinsichtlich einer künftigen Unternehmens(-IT-)entwicklung. ▬