Vorwort

Mit Konkretisierung des AT 7.2 MaRisk in Form der BAIT sind die Anforderungen für die IT-Organisation deutlich gestiegen. Im Rahmen dieser Anforderungen haben wir uns entschlossen, für die wesentlichen erforderlichen Arbeitsanweisungen für den operativen IT-Betrieb entsprechende Muster-Anweisungen zu erstellen. Diese Anweisungen ergänzen insofern die bereits durch unser Haus erstellten Arbeitsanweisungen zur Umsetzung der Anforderungen der MaRisk im IT-Bereich.

Ziel dieser Musterarbeitsanweisungen ist es, der Bank einen Überblick über zu regelnde Vorgehensweisen zu verschaffen und gleichzeitig ein Muster zur Verfügung zu stellen, mit der bankintern eine Umsetzung erfolgen kann. Die aufgeführten Regelungen müssen in der einzelnen Bank individuell bewertet und ggf. angepasst / ergänzt werden.

Die neuen Anforderungen des 2017 aktualisierten Standards für Ordnungsmäßigkeit der IT-Verfahren der Fiducia & GAD (SOIT) sind in diesen Arbeitsanweisungen bereits berücksichtigt. Ebenso sind die wesentlichen übergreifenden Maßnahmen aus ForumISM sowie die wesentlichen relevanten BSI-Grundschutzmaßnahmen in die Erstellung eingeflossen.

Mit Einführung der BAIT im Jahr 2017 sind die Anforderungen an die Bearbeitung von Störungen im IT-Betrieb erstmal aufsichtsrechtlich konkretisiert worden. Dies hat dazu geführt, diese ursprünglich nur für die Bearbeitung von (Informations-) Sicherheitsvorfällen definierte Arbeitsanweisung um Regelungen zum Management von Serviceanfragen sowie von Störungen im IT-Betrieb zu erweitern. Ein wirtschaftliches und aufsichtsrechtlich ordnungsgemäßes Management dieser drei Prozesse ist u.E. ohne ein (teil-) elektronisches Ticketsystem nur schwer darstellbar, weshalb der Einsatz eines solchen Ticketsystems die technische Basis für die hier definierten Prozesse bilden sollte.

Sofern für die Bank Bearbeitungshinweise gegeben wurden, sind diese in der Arbeitsanweisung in blauer Schrift kenntlich gemacht. Insbesondere diese Stellen sollten entsprechend auf die individuellen Belange und Gegebenheit in der Bank angepasst werden.

[Bearbeitungshinweis: Das Vorwort sollte nach Berücksichtigung der oben genannten Punkte bei Einführung der Arbeitsanweisung gestrichen werden].

Darstellung der wesentlichen Veränderungen:	
Version	**Veränderung**

2.0	• Übergreifend
	  ○ Anpassung (IT-) Sicherheitsvorfall in (Informations-) Sicherheitsvorfall
	  ○ Aufnahme der Abgrenzung zwischen „(Informations-) Sicherheitsvorfall“ und „Abweichung im Alltagsbetrieb“ (=Störung) (Anforderung der BAIT)
	• Kapitel 1 in Kapitel 3 verschoben
	• Neuerstellung von Kapitel 2 zur Bearbeitung von Serviceanfragen
	• Neuerstellung von Kapitel 2 zur Bearbeitung von Störungen (Incidents)
	• Umbenennung de Arbeitsanweisung hinsichtlich der neu hinzugekommenen Kapitel
	• Definition von Zuständigkeiten für die Prävention von Informationssicherheitsvorfällen

1.2	• Redaktionelle Anpassungen OHB -> SOIT
1.1.2	• Aufnahme „… in einem Landkreis bzw. einer kreisfreien Stadt …“ bei den GAA • Notfallkonzept → Notfallhandbuch

1.1.1	• Kapitel 1.2: Ergänzung der Definition für schwerwiegende MaSI-relevante (IT-) Sicherheitsvorfälle
	• Kapitel 1.3: Ergänzung der Meldepflicht für MaSI-relevante (IT-Sicherheitsvorfälle)
	  ○ Hinweise zur Durchführung der Meldung (insb. Mailadresse)
	  ○ Ergänzung von Hinweisen zur Meldung von Dienstleistern

1.1	• Aufnahme von Regelungen für die Umsetzung der MaSI.
	• Kapitel 1.1: Aufnahme der MaSI als Handlungsfeld für diese Arbeitsanweisung.
	• Kapitel 1.2:
	  ○ Aufnahme von Beispielen aus dem Zahlungsverkehrsumfeld
	  ○ Aufnahme der Definition für „schwerwiegende MaSI-relevanter (IT-) Sicherheitsvorfälle“
	• Kapitel 1.3:
	  ○ Ergänzung des Prozesses um die Weiterleitung von (IT-) Sicherheitsvorfällen an Dienstleister
	  ○ Ergänzung des Prozesses um die Meldung von schwerwiegenden MaSI-relevanten (IT-) Sicherheitsvorfällen
	  ○ Anpassung der Regelungen im Prozess für die Risikoermittlung und die Behandlung der Ergebnisse aus der Risikoermittlung
	• Kapitel 1.4:
	  ○ Aufnahme von Regelungen für Vorfälle mit Beteiligung eines Dienstleisters
	  ○ Aufnahme von Regelungen für Vorfälle mit Außen- / Kundenauswirkungen – insbesondere auf den (Internet-)Zahlungsverkehr

Inhaltsverzeichnis