Geno Bank Consult

Geno Bank Consult GmbH • Postfach 7849 • 48042 Münster

An die
für die **IT-Organisation**
und die **Informationssicherheit**
verantwortlichen Mitarbeiter/-innen

Albersloher Weg 9
48155 Münster

Ansprechpartner:
Dirk Mertens
Telefon: 0151 15312317
E-Mail: dirk.mertens@genobc.de
http:// www.genobc.de

Münster, 20.02.2018

Anpassung unserer Musterarbeitsanweisungen für den IT-Bereich an die „Bankaufsichtlichen Anforderungen an die IT“ (BAIT)

Sehr geehrte Damen und Herren,

durch den hohen Grad der Unterstützung der bankgeschäftlichen Prozesse durch die IT und die dabei zu beachtenden bankaufsichtlichen Anforderungen stehen die für die IT-Organisation und die Informationssicherheit verantwortlichen Mitarbeiter/-innen regelmäßig vor neuen Aufgaben und Herausforderungen. Mit unserem breiten Angebot an fortlaufend aktualisierten Musterarbeitsanweisungen für den IT-Bereich unterstützen wir die IT-Verantwortlichen u.a. auch bei der Anpassung der IT-bezogenen Prozesse an Produktveränderungen der IT-Dienstleister sowie an neue externe Vorgaben für den IT-Betrieb.

Die **Anpassungen in den MaRisk** und die **Veröffentlichung der BAIT** haben wir zum Anlass genommen, einen Großteil unserer bewährten Musterarbeitsanweisungen für den IT-Bereich zu überarbeiten und das Angebot nochmals zu erweitern. Nach sorgfältiger Pilotierung freuen wir uns, Ihnen nun die überarbeiteten bzw. neuen Musterarbeitsanweisungen anbieten zu können.

Musterdokumente	Inhalte / wesentliche Anpassungen
BAIT-Check ***(NEU - kostenfrei)***	• Dokumentation der Art und des Umfangs, in dem die Anforderungen der BAIT in der Bank umgesetzt sind • Verweis auf Arbeitsanweisungen • Beschreibung der Nutzung von Öffnungsklauseln sowie der Auslegung von Anforderungen der BAIT • **Download: http://www.genobc.com/filemanager/fachinfos/it/aaw/Compliancecheck_BAIT_IT-Handbuch_20180215.docx**
Informationssicherheits-leitlinie	• Definition der BAIT als grundlegendes Regelwerk • Beschreibung der Aufgaben eines für alle Institute obligatorischen Informationssicherheitsbeauftragten (ISB) inkl. Ressourcenzuweisung • Überarbeitung der Aufgabenschreibung für den ISB

Informationsrisiko-management	• Umfangreiche redaktionelle Anpassungen auf Basis der BAIT • Berücksichtigung des Lebenszyklus bei der Risikoanalyse von IT-Schutzobjekten unter Hinzuziehung der Fachbereiche • Aktualisierung der Parameterbeschreibungen für ForumISM auf Basis des überarbeiteten SOIT
Notfallhandbuch	• Anpassung der Definitionen an die Begrifflichkeiten des SOIT sowie Aufnahme zusätzlicher Begrifflichkeiten • Ergänzung der Zuständigkeiten des Notfallteams um vorhersehbare (Schadens-)Ereignisse • Anpassung der Beschreibung von Bedrohungen auf Basis des überarbeiteten SOIT • Anpassung des Notfallkonzeptes an den Notfall- und Störungsprozess der DZ Bank AG • Anpassung der Vorgehensweise an den Notfallprozess der Deutschen Bundesbank • Erweiterung der Geschäftsfortführungspläne • Hinweise zur Berücksichtigung von zeitkritischen IT-Schutzobjekten • Erweiterung der Notkassenbestände um Münzgeld • Neue Anlage: Notfallkonzept Offenmarktgeschäfte
Berechtigungskonzepte	• Vorgaben zur Verhinderung von Selbstkontrolle bzw. Selbstüberprüfung durch Wechsel von Markt / Handel in die Marktfolge bzw. in Kontrollfunktionen • Definition des Sparsamkeitsbegriffs für die Erstellung von Sollkonzepten auf Basis Tz. 24 der BAIT mit schutzbedarfsabhängiger Einschränkung • Vorgaben für die Verwendung von nicht personalisierten oder technischen Benutzern gem. BAIT Tz. 25 • Vorgaben für die Korrektur von fehlerhaft vergebenen Kompetenzen gem. BAIT Tz. 27 • Hinweis zur elektronischen Auswertbarkeit von Ergebnissen aus Kompetenzvergabeprozessen gem. BAIT Tz. 28
Softwareeinsatz	• Berücksichtigung der Anforderungen der BAIT Tz. 48 • Verweis auf den Incident-Managementprozess für Abweichungen vom Regelbetrieb (=Störungen) nach der Produktivsetzung • Aufnahme eines Unterkapitels für die Darstellung des Prozesses zur Anpassung von eigenentwickelten Anwendungen • Regelungen für Eigenentwicklungen mit häufiger Änderungsfrequenz • Ausnahmen für RZ-Standardabfragen bei Test und Freigabe • Darstellung der Release-Datenbank als Verteilungsmedium im Verfahren 1 • Verknüpfung mit dem Informationsrisikomanagementprozess hinsichtlich der Steuerung des Lebenszyklus von Anwendungen • Erweiterung der Mindestangaben im Software-Register • Regelungen für Eigenentwicklungen hinsichtlich der Aufnahme in das Software-Register • Gleichstellung der Regelungen zur Beschaffung unabhängig von der Beschaffungsart (Kauf / Miete / Leasing) • Anpassung des Release-Bearbeitungsprozesses an den SOIT

Hardwareeinsatz	• Berücksichtigung der Anforderungen der BAIT Tz. 48 • Verweis auf den Incident-Managementprozess für Abweichungen vom Regelbetrieb (=Störungen) nach der Produktivsetzung • Verknüpfung mit dem Informationsrisikomanagementprozess hinsichtlich der Steuerung des Lebenszyklus von Hardware • Anpassung des Bestandsverzeichnisses um die Mindestinhalte der BAIT Tz. 46
Serviceanfragen, Störungen und (Informations-) Sicherheitsvorfälle ***(Operativer IT-Betrieb: Paket 6)***	• Abgrenzung zwischen „(Informations-) Sicherheitsvorfall“ und „Abweichung im Alltagsbetrieb“(=Störung) *[Anforderung der BAIT]* • Neuerstellung von Kapitel 2 zur Bearbeitung von Serviceanfragen • Neuerstellung von Kapitel 3 zur Bearbeitung von Störungen (Incidents) und Informationssicherheitsvorfällen • Definition von Zuständigkeiten für die Prävention von Informationssicherheitsvorfällen
Auslagerungsmanagement ***(NEU)***	• Umfangreiche Regelungen zum Management von Auslagerungen (MaRisk) sowie zum Fremdbezug von IT-Dienstleistungen (BAIT)
Projektmanagement ***(NEU)***	• Initiale Definition von Regelungen zum Projektmanagement unter Berücksichtigung der Vorgaben der BAIT sowie zu Best-Practice-Ansätzen für das Projektmanagement (PMI) • Umfangreiche Anlagen: Vorlagen zur Projektrisikoanalyse, Dokumentation von Entscheidungen im Projekt, Projektantrag, Projektauftrag, etc.

Für Ihre Bestellung verwenden Sie bitte das beigefügte Bestellformular. Die Auslieferung der Musterdokumente erfolgt in Form von MS-Word-Dateien an die von Ihnen angegebene E-Mail-Adresse.

Gerne unterstützen wir Sie auch bei der Individualisierung der Musterarbeitsanweisungen sowie bei der Anpassung Ihrer bestehenden organisatorischen Regelungen für den IT-Bereich an die BAIT. Dabei bringen wir unsere Erfahrungen aus zahlreichen Projekten zur Optimierung von IT-Prozessen in Volksbanken und Raiffeisenbanken mit ein.

Als **Ansprechpartner** stehen Ihnen unsere IT- und Organisationsspezialisten

- Herr Dirk Mertens (Tel. 0151 15312317 | E-Mail: dirk.mertens@genobc.de) und
- Herr Björn Scherer (Tel. 0151 14827873 | E-Mail: bjoern.scherer@genobc.de)

gern zur Verfügung.

Freundliche Grüße

Geno Bank Consult GmbH

Anlage