Übersicht der grundlegenden Anpassungen in den Musterarbeitsanweisungen der GBC im IT-Bereich zum Update 06/2017

Informationssicherheitsleitlinie

- Alle Kapitel
  - Anpassung der AAW auf die Namensgebungen im SOIT
- Kapitel 4.1
  - Definition einer Beziehung der Schutzziele zu (Geschäfts-)zielen der Bank
  - Aufnahme eines Verweises auf die AAW IT-Risikomanagement hinsichtlich der Definition des angestrebten Schutzniveaus
- Kapitel 5
  - Aufnahme einer Passage zur Bewusstseinsbildung / Einbeziehung sämtlicher Mitarbeiter
- Kapitel 6.3
  - Aufnahme des Begriffes „Bewusstseinsbildung (Awareness)“

IT-Risikomanagement

- Alle Kapitel
  - Anpassung der AAW auf die Namensgebungen im SOIT
- Kapitel 1.1
  - Aufnahme eines Hinweises, dass die Aufnahme in die Risikoinventur für die operationellen Risiken durch das Risikomanagement/Risikocontrolling erfolgt.
  - Aufnahme des Proportionalitätsprinzips
  - Aufnahme eines Bearbeitungshinweises zur Quantifizierung der IT-Risiken
- Kapitel 1.2:
  - Ergänzung der Änderungsbedarfe im Rahmen des PDCA-Zyklus im Hinblick auf Organisationsänderungen und den Einsatz neuer IT-Schutzobjekte
  - Aufnahme eines Hinweises auf die AAW Informationssicherheitsvorfälle
- Kapitel 2.3
  - In den SOIT haben sich verschiedene Definitionen geändert. Diese sollten – nach einer bankinternen Überprüfung inkl. Dokumentation - nach ForumISM und damit in den bankinternen IT-Risikomanagementprozess überführt werden
- Kapitel 2.5.3
  - Aufnahme der Anforderungen und Maßnahmen für die Behandlung von Schutzzielen
- Kapitel 2.6.1
  - Aufnahme eines Hinweises,(Text + Ablaufbild), dass für zeitkritische Prozesse notwendige IT ebenfalls in dem Notfallhandbuch zu berücksichtigen ist
- Kapitel 2.6.2
  - Aufnahme von weiteren gem. SOIT möglichen Kriterien zur Bewertung der Geschäftsprozesse
- Kapitel 2.7.2

    - Darstellung, dass sich die Wesentlichkeit eines IT-Schutzobjektes direkt aus der Wesentlichkeit des Prozesses und die Einbindung des Schutzobjektes in den Prozess ergibt. Somit wird nur in wenigen Fällen eine Wesentlichkeitsermittlung auf Schutzobjektebene erforderlich sein.
    - Aufnahme des Begriffes „schützenswert“ aus den SOIT bei der Ermittlung der Wesentlichkeit
- Kapitel 2.7.5.1
    - Aufführung des Bedrohungskatalogs nebst der Zuordnung der Risikokategorien des RZ
- Kapitel 2.7.5.2
    - Aufnahme von Hilfestellungen für die Bewertung der Bedrohungen
    - Aufnahme von Begrifflichkeiten aus den SOIT zur Konkretisierung der Auswirkungen bei der Analyse der Bedrohungen
    - Aufnahme von Begrifflichkeiten aus den SOIT zur Konkretisierung der Aufnahme von Hilfestellungen für die Bewertung der Schwachstellen
    - Aufnahmen eines Hinweises, dass im Rahmen der Risikoanalyse bestehende über die BSI-Checkliste hinaus gehende Maßnahmen (risikomindernd) berücksichtigt werden
    - Konkretisierung der Beziehung von Restrisiko zum Risiko bei den einzelnen Bewertungsstufen
- Kapitel 2.9
    - Neuaufnahme zur Darstellung des Umgangs mit bedeutenden Schadensfällen im IT-Bereich
- Kapitel 2.10
    - Anpassung der Bedrohungen in den MaSi-relevanten Risiken auf die Bedrohungen des SOIT

Notfallhandbuch

- Alle Kapitel
    - Anpassung der AAW auf die Namensgebungen im SOIT
- Kapitel 1
    - Anpassung der Definitionen an die Begrifflichkeiten des SOIT sowie Aufnahme zusätzlicher Begrifflichkeiten. Trennung in verschiedene Unterkapitel wg. der Aufnahme von Regelungen für die Aufrechterhaltung und Verbesserung des Notfallmanagements
- Kapitel 2
    - Ergänzung der Zuständigkeit des Notfallteams auch für vorhersehbare (Schadens-) Ereignisse
- Kapitel 5
    - Die Bedrohungen wurden an den SOIT angepasst und mit typischen Notfallszenarien verknüpft
- Kapitel 6
    - Verschiedene Ergänzungen aufgrund der Änderungen in Kapitel 5
- Kapitel 7
    - Verschiedene Ergänzungen aufgrund der Änderungen in Kapitel 5

- Kapitel 9.2
  - Darstellung des Verzichts von Wiederherstellungsplänen (bzw. Wiederanlaufplan gem. MaRisk = Wiederherstellungsplan gem. SOIT)
- Kapitel 9.2.1.2
  - Anpassung des Notfallkonzeptes an den Notfall- und Störungsprozess der DZ Bank AG
- Kapitel 9.2.5.1
  - Erweiterung des Geschäftsfortführungsplans für den Prozess „Eigengeschäft und Refinanzierung“ im Hinblick auf den Bereich Offenmarktgeschäfte (OMTOS); Anpassung der Vorgehensweise an den Notfallprozess der Deutschen Bundesbank
- Kapitel 10
  - Aufnahme eines Hinweises, dass IT-Systeme, die für zeitkritische Prozesse notwendig sind, gem. SOIT im Notfallhandbuch zu berücksichtigen sind
- Anlage 4
  - Erweiterung der Notkassenbestände um Münzgeld
- Neue Anlage 6
  - Notfallkonzept Offenmarktgeschäfte

Softwareeinsatz

- Alle Kapitel
  - Anpassung der AAW auf die Namensgebungen im SOIT
- Kapitel 2.2
  - Gleichstellungen der Regelungen zur Beschaffung unabhängig von Beschaffungsart (Kauf / Miete / Leasing)
  - Anpassung des Releasebearbeitungsprozesses an den SOIT

Operativer IT-Betrieb, Paket 1: Grundlagen, Datensicherung, Laufwerke, Entsorgung, Fremdpersonal

- Alle Kapitel
  - Anpassung der AAW auf die Namensgebungen im SOIT
  - Redaktionelle Anpassungen GenoBankSafe-IT ➔ ForumISM
- Kapitel 3
  - Kontrolle der Datensicherung im RZ erforderlich (gem. SOIT)

Operativer IT-Betrieb, Paket 4: Virenschutz, Internetzzugang, Elektronische Kommunikation

- Alle Kapitel
  - Anpassung der AAW auf die Namensgebungen im SOIT
- Kapitel 3.1
  - Detaillierung der Aufbewahrungsfristen für E-Mails

- Definition besonders schutzbedürftiger Mailboxen und Sonderregelungen für den Zugriff Dritter darauf

Operativer IT-Betrieb, Paket 8 - IT-Kontrollen

- Alle Kapitel
  - Anpassung der AAW auf die Namensgebungen im SOIT
- Anlage: 1:
  - Diverse Anpassungen der Detailkontrollen bezüglich von Änderungen an den IT-Schutzobjekten und ihren Funktionen
    - Funktionsgruppenkonzept in Foconis ZAK
    - neue Kontrollen für VR-Control
    - usw.