Version	Veränderung
1.4.3	Übergreifend: • Anpassung der Bezeichnung auf die Anforderungen der BAIT (Informationsrisikomanagement). Kapitel 1.2: Aufnahme eines Verweises auf die Einbindung der Mitarbeiter der Fachbereiche im Hinblick auf einen notwendigen Austausch wg. Veralterung. Kapitel 2.3: Anpassung der Parameterbeschreibungen an den SOIT Kapitel 2.7.5.2 Aufnahme eines Hinweises, dass ein zusätzliches Risiko bei der Überalterung des zu bewertenden Schutzobjektes anzulegen ist.
1.4.2	Anpassung der AAW auf die Anforderungen des SOIT Kapitel 1.1: • Aufnahmen eines Hinweises, dass die Aufnahme in die Risikoinventur opRisk 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 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 Informationsrisikomanagementprozess überführt werden. In diesem Kapitel sind die (alten) Einstellungen in ForumISM und darunter in Textform die neuen Einstellungen gem. SOIT aufgeführt. Es sollte bankseitig eine Anpassung in ForumISM (und dann neue Hardcopy in die AAW einfügen und die Texte zu den SOIT Einstellungen entfernen) 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 Kapitel 2.7.5.2 • 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
1.4.1	Kapitel 2.7.1 und Kapitel 2.7.4 • Erweiterung des Prozesses für die Bearbeitung von IT-Schutzobjekten: Verpflichtende Berücksichtigung im Notfallhandbuch, sofern ein IT-Schutzobjekt erhöhte Verfügbarkeitsanforderungen besitzt (Vf3 oder Vf4).
1.4	Alle Kapitel: • Redaktionelle Anpassungen bezogen auf die Erweiterung des Kapitels 2.3. • Aktualisierung sämtlicher Screenshots auf Basis der Version 3.6 von ForumISM. Kapitel 2.1: • Aufnahme eines Hinweises, dass Datenbankabfragen nicht mit anderen Objekten verknüpft werden. Kapitel 2.2: • Erweiterung der Beschreibung des Datenklassenmodells. • Begriffsdefinition von Anwendung, Datenbankabfrage, System und Infrastruktur sowie Verknüpfung zu hierzu relevanten AAW. Kapitel 2.3: • Umfangreiche Erweiterung bei der Beschreibung der Parameter. • Verknüpfung der Parameter mit dem SOIT und Dokumentation etwaiger Abweichungen hiervon. Kapitel 2.7.2: • Integration von selbsterstellten wesentlichen Datenbank-/Reportingabfragen in das Risikomanagement.

	Kapitel 2.7.4: • Definition des Umgangs mit Datenbankabfragen im Rahmen der Schutzbedarfs-/Schutzniveauanalyse (Erleichterungen). • Darstellung der Vorgehensweise zur Erstellung bankinterner Sicherheitskonzepte. Kapitel 2.7.5: • Definition des Umgangs mit Datenbankabfragen im Rahmen der Risikoanalyse / Erstellung von IT-Sicherheitskonzepten (Erleichterungen). Kapitel 5: • Löschen der Anlage 1. • Inhalte der alten Anlage 1 sind nun Gegenstand des Kapitels 2.3. Anlage 2: • Neuerstellung der Anlage 2 (Muster zur Erstellung bankeigener Sicherheitskonzepte)
1.3	Kapitel 2.9: Bearbeitungshinweis für die Risikoanalyse von Kreditkarten gemäß MaSI.
1.2	Kapitel 2.8: Verknüpfung mit der AAW operativer IT-Betrieb – IT-Kontrollen: Hinweis auf die Definition von IT-Kontrollen zur Minderung des Restrisikos für meldepflichtige und genehmigungspflichtige Risiken.
1.1	Implementierung des Kapitels 2.9 zur Umsetzung der von den MaSI geforderten Risikoanalysen.
1.0	Neugliederung der AAW auf Basis neuer Versionen von ForumISM und Aktualisierungen im SOIT.