

Organisationshandbuch		Volksbank Musterstadt eG	
IT-Risikomanagement	Kapitel Nr. / Register Nr.:		
	Ausgabe Nr. / gültig ab:		
	Ersatz für:		
	Verfasser:		
	Mitarbeit:		

1	IT-Risikomanagement als Teilbereich des Managements operationeller Risiken	6
1.1	Einleitung und Anforderungen an das IT-Risikomanagement	6
1.2	PDCA-Zyklus und Einbindung der Fachbereiche in das IT-Risikomanagement.....	8
2	IT-Risikosteuerung in ForumISM	11
2.1	Grundlegende Hinweise	11
2.2	Ermittlung der zu betrachtenden Objekte im IT-Risikomanagement.....	13
2.3	Parametrisierung von ForumISM	15
2.4	Übergreifende Schutzmaßnahmen (BSI-Grundschutz)	39
2.4.1	Prozess für die Ermittlung und Bewertung der relevanten Maßnahmen.....	39
2.4.2	Analyse und Ermittlung des Umsetzungsstands	40
2.4.3	Qualitative Restrisikobetrachtung	40
2.5	Datenklassen.....	42
2.5.1	Prozess für die Ermittlung und Bewertung der Datenklassen	42
2.5.2	Schutzbedarfsanalyse.....	42
2.6	Geschäftsprozesse	44
2.6.1	Prozess für die Ermittlung und Bewertung der Geschäftsprozesse.....	44
2.6.2	Wesentlichkeitsermittlung.....	46
2.6.3	Business Impact Analyse	48
2.6.4	Schutzbedarfsanalyse.....	49
2.7	IT-Schutzobjekte	50
2.7.1	Prozess für die Ermittlung und Bewertung der IT-Schutzobjekte.....	50
2.7.2	Wesentlichkeitsermittlung.....	51
2.7.3	IT-Sicherheitskonzepte (externe und interne).....	52
2.7.4	Schutzbedarfs-/Schutzniveausermittlung	53
2.7.5	Risikoanalyse	55
2.7.5.1	Bedrohungskatalog	56
2.7.5.2	Objektspezifische Risiken (Risikoanalyse).....	57
2.7.5.3	Ermittlung der Risikokategorie und deren Auswirkungen.....	64
2.7.5.4	Maßnahmen zur Risikoreduktion.....	66
2.8	Wiedervorlageintervall	66
2.9	Behandlung von bedeutenden Schadensfällen im IT-Bereich	67

Organisationshandbuch	Volksbank Musterstadt eG		
IT-Risikomanagement	Kapitel Nr. / Register Nr.:		
	Ausgabe Nr. / gültig ab:		
	Ersatz für:		
	Verfasser:		
	Mitarbeit:		

2.10	Ergänzende / abändernde Hinweise für Schutzobjekte, die den MaSI unterliegen	68
3	Berichtswesen	73
4	Stresstests für IT-Risiken	74
5	Anlage 1: Vorstandsvorlage genehmigungspflichtige/signifikante Risiken	75
6	Anlage 2: Muster_Schutzniveauanalyse	75

Organisationshandbuch		Volksbank Musterstadt eG	
IT-Risikomanagement	Kapitel Nr. / Register Nr.:		
	Ausgabe Nr. / gültig ab:		
	Ersatz für:		
	Verfasser:		
	Mitarbeit:		

Version	Veränderung
1.4.2	<p>Anpassung der AAW auf die Anforderungen der SOIT</p> <p>Kapitel 1.1</p> <ul style="list-style-type: none"> 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 <p>Kapitel 1.2:</p> <ul style="list-style-type: none"> Ergänzung der Änderungsbedarfe im Rahmen des PDCA-Zyklus auf Organisationsänderungen und den Einsatz neuer IT-Schutzobjekte Aufnahme eines Hinweises auf die AAW Informationssicherheitsvorfälle <p>Kapitel 2.3</p> <ul style="list-style-type: none"> 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. 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) <p>Kapitel 2.5.3</p> <ul style="list-style-type: none"> Aufnahme der Anforderungen und Maßnahmen für die Behandlung von Schutzzielen <p>Kapitel 2.6.1</p> <ul style="list-style-type: none"> Aufnahme eines Hinweises,(Text + Ablaufbild), dass für zeitkritische Prozesse notwendige IT ebenfalls in dem Notfallhandbuch zu berücksichtigen ist. <p>Kapitel 2.6.2</p> <ul style="list-style-type: none"> Aufnahme von weiteren gem. SOIT möglichen Kriterien zur Bewertung der Geschäftsprozesse <p>Kapitel 2.7.2</p> <ul style="list-style-type: none"> 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 <p>Kapitel 2.7.5.1</p> <ul style="list-style-type: none"> Aufführung des Bedrohungskatalogs nebst der Zuordnung der Risikokategorien des RZ <p>Kapitel 2.7.5.2</p> <ul style="list-style-type: none"> 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 <p>Kapitel 2.7.5.2</p>

Organisationshandbuch		Volksbank Musterstadt eG	
IT-Risikomanagement	Kapitel Nr. / Register Nr.:		
	Ausgabe Nr. / gültig ab:		
	Ersatz für:		
	Verfasser:		
	Mitarbeit:		

	<ul style="list-style-type: none"> 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 <p>Kapitel 2.9</p> <ul style="list-style-type: none"> Neuaufnahme zur Darstellung des Umgangs mit bedeutenden Schadensfällen im IT-Bereich <p>Kapitel 2.10</p> <ul style="list-style-type: none"> Anpassung der Bedrohungen in den MaSi-relevanten Risiken auf die Bedrohungen des SOIT
1.4.1	<p>Kapitel 2.7.1 und Kapitel 2.7.4</p> <ul style="list-style-type: none"> 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	<p>Alle Kapitel:</p> <ul style="list-style-type: none"> Redaktionelle Anpassungen bezogen auf die Erweiterung des Kapitels 2.3. Aktualisierung sämtlicher Screenshots auf Basis der Version 3.6 von ForumISM. <p>Kapitel 2.1:</p> <ul style="list-style-type: none"> Aufnahme eines Hinweises, dass Datenbankabfragen nicht mit anderen Objekten verknüpft werden. <p>Kapitel 2.2:</p> <ul style="list-style-type: none"> Erweiterung der Beschreibung des Datenklassenmodells. Begriffsdefinition von Anwendung, Datenbankabfrage, System und Infrastruktur sowie Verknüpfung zu hierzu relevanten AAW. <p>Kapitel 2.3:</p> <ul style="list-style-type: none"> Umfangreiche Erweiterung bei der Beschreibung der Parameter. Verknüpfung der Parameter mit dem SOIT und Dokumentation etwaiger Abweichungen hiervon. <p>Kapitel 2.7.2:</p> <ul style="list-style-type: none"> Integration von selbsterstellten wesentlichen Datenbank-/Reportingabfragen in das Risikomanagement. <p>Kapitel 2.7.4:</p> <ul style="list-style-type: none"> Definition des Umgangs mit Datenbankabfragen im Rahmen der Schutzbedarfs-/Schutzniveauanalyse (Erleichterungen). Darstellung der Vorgehensweise zur Erstellung bankinterner Sicherheitskonzepte. <p>Kapitel 2.7.5:</p> <ul style="list-style-type: none"> Definition des Umgangs mit Datenbankabfragen im Rahmen der Risikoanalyse / Erstellung von IT-Sicherheitskonzepten (Erleichterungen). <p>Kapitel 5:</p> <ul style="list-style-type: none"> Löschen der Anlage 1. Inhalte der alten Anlage 1 sind nun Gegenstand des Kapitels 2.3.

Organisationshandbuch		Volksbank Musterstadt eG	
IT-Risikomanagement	Kapitel Nr. / Register Nr.:		
	Ausgabe Nr. / gültig ab:		
	Ersatz für:		
	Verfasser:		
	Mitarbeit:		

	Anlage 2: <ul style="list-style-type: none"> • 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.