IT-Sicherheit in Banken (IS-Management)

Zusammenstellung der erforderlichen Aufgabenbereiche für ein integriertes Werkzeug zu den Bereichen: IT-Betrieb, IT-Sicherheit und IT-Revision

Bei der Zusammenstellung wird von der Struktur des IDW PS 330 ausgegangen.

Bei der folgenden Unterteilung werden die Begriffe Information, Kontrollaktivität und Prüfung benutzt. Hierdurch soll die sich aus dem Risikogegenstand ergebende Aktivität dargestellt werden.

Information: Die Angaben dienen der Darstellung und Dokumentation der Informationssysteme. Es handelt sich um Informationen, die grundsätzlich in der Anweisung beschreiben wurden (Organisationsrichtlinien gem. MaRisk) bzw. diese ergänzen oder näher ausführen. Aus diesen Informationen können sich für den IT-Betrieb und damit für die IT-Abteilung (z.B. Systemadministration) Arbeitspflichten ergeben, die dann gleichzeitig im Tool aufgezeigt und dokumentiert werden. Darauf wird in der Tabelle nicht ausdrücklich daraufhingewiesen. Dort wird nur der Begriff Information genannt.

Kontrollaktivität: Entsprechend dem IKS werden hier mögliche Kontrollaktivitäten aufgezeigt. Diese sollten im Tool entsprechend vermerkt werden können.

Prüfung: Prüfung entsprechend der MaRisk, dem IDW EPS 261 und 300 n.F.. Grundlage ist nicht das Tool für die IR, sondern der Prüfungsplan der IR. Zur Transparenz sollte hier das Datum der letzten Prüfung angegeben werden

Beim Punkt IT-Betrieb ist entsprechend nach Verfügbarkeit, Authentizität, Vertraulichkeit und Datenintegrität im Einzelfall abzustellen.
Das Tool sollte als „Arbeitswerkzeug angesehen werden, dass bestimmte Dokumentationspflichten,z.B. nach einer Kontrolle von Logdateien kann darstellt und dokumentiert.

IT-Sicherheitsbeauftragter: Darstellung der Kontrollaktivitäten und damit auch Risikobeurteilungen des IT-Sicherheitsbeauftragten.

IT-Revision: Darstellung möglicher Prüfungshandlungen, um die Historie der risikoorientierten Prüfungshandlungen festhalten zu können.

Geschäftsprozess: IT z.B. Software wird innerhalb eines Geschäftsprozesses eingesetzt und z.B. parametrisiert. Insoweit ist der Schutzbedarf des Prozesses maßgebend.

Nachfolgend werden einzelne Prüfungsfelder dargestellt. Es handelt sich nur um eine Auswahl. Entscheidend ist die eingesetzte Methode/Standard der Bank!

Risikogegenstand	IT-Betrieb	IT-Sicherheit(sbeauftragter)	IT-Revision
	Im Tool Darstellung nach Verfügbarkeit, Authentizität, Vertraulichkeit und Datenintegrität		
IT-Umfeld			
Hinweise zum IT-Sicherheitskonzept Geschäfts-/Risikostrategie IT	**Information**[1]	**Information**	**Information (=Informationsbeschaffung entsprechend IDW Standard IDW EPS 261)**
IT-Organisation			
Organigramm und Anweisung Regelungen zur Systemadministration	**Information**	**Information**	**Information/Aufbauprüfung**
Verantwortlichkeiten und Kompetenzen	**Information**	**Information**	**Information/Aufbauprüfung**
Sonstige Regelungen (z.B. Verweis zu operationellen Risiken)	**Information**	**Information**	**Information/Aufbauprüfung**
Risikoinventur z.B. Vermerk zur letzten Risikoinventur Die Inventur erfolgt letztlich über ein anderes Tool	**Information**	**Information**	**Information/Prüfung**
IT-Infrastruktur			
Übersicht über die Systemkomponenten z.B. auch Hinweise zu den Regelungen bei mobilen Arbeitsplätzen und Übersicht der zugeordneten mobilen Arbeitsplätze (bzw. Verweis auf ein anderes Tool)	**Information**	**Information/Kontrollaktivitäten**	**Information/Prüfung**

[1] Information beinhaltet auch Arbeitspflichten/Aufgaben der Systemadministration bzw. weiterer IT-Mitarbeiter

Beispiel: mobile Arbeitsplätze: Verbindungsprofile darstellen, Sicherheitsfunktionen getroffene Vereinbarungen mit dem MA, Festplattenverschlüsselung)			
Übersicht über die Systemkomponenten/ Fremdsysteme z.B. Clustersysteme, Server mit Spezialfunktionen(z.B.Tivoli Gateway,Citrix)	**Information**	**Information**	**Information/Prüfung**
Darstellung der Veränderungen ‚Stand der Systeme[2]	**Information**	**Kontrollaktivität**	**Prüfung**
Unterteilt nach Hardware, Betriebssystem und Netzwerk(Domänenkonzept, Datenhaltung und Replikation, Gruppen im Netzwerk,…)	**Information**	**Information**	**Prüfung**
Regelungen und Dokumentation von Aktivitäten zu z.B. webmin Darstellung der Standardaufgaben bzw. Verweis auf die Anweisung	**Prozessbearbeitung nachweisen Risikobetrachtung und Kontrolle**	**Kontrollaktivität**	**Prüfung**
Darstellung des Datensicherungskonzeptes[3]	**Aktivitätensteuerung**	**Kontrollaktivitäten**	**Prüfung**
Darstellung Verschlüsselungsverfahren für Notebooks	**Information**	**Kontrollaktivitäten**	**Prüfung**
Weitere externe Komponenten, wie. usb-Sticks, Brenner,usw.	**Information**	**Kontrollaktivitäten**	**Prüfung**
Darstellung der Zugriffskontrollen z.B. Linuxrechte usw.)	**Information**	**Information und Kontrollaktivität**	**Prüfung**
Hinweise und Dokumentation zur Fernwartungsmaßnahmen außerhalb eines Standards (z.B. bei Bündelwechsel keine	**Prozessbearbeitung nachweisen**	**Information und Kontrollaktivität**	**Prüfung**

[2] erledigte Projekte oder **wichtige** Installationen könnten hier mit Datum dokumentiert werden.
[3] Rücksicherungen und Tests können hier dokumentiert werden.

Dokumentation, da dies als genereller Prozess angesehen wird, evtl. Datumsangabe des letzten Bündelwechsels,…)			
Darstellung der physischen Sicherungsmaßnahmen	**Information**	**Kontrollaktivitäten**	**Prüfung**
Regelungen für den Notfallbetrieb bzw. Verweis auf gesondertes Tool Darstellung des Prozesses gem. MaRisk AT 7.3	**Information**	**Kontrollaktivität bzw. Szenariobetrachtung/Tests**	**Prüfung**
Regelungen zur räumlichen Sicherheit z.B. Übersicht der Komponenten im Raum, Risikodarstellung aufgrund der räumlichen Gegebenheiten, Zugriffskontrollen darstellen	**Information**	**Kontrollaktivitäten**	**Prüfung**
IT- Anwendungen			
Hinweise zur eingesetzten Software und den Eigenprogrammierungen Klassifizierung der Software –auch im Hinblick auf ihre Sensibilität	**Information**	**Information**	**Information**
Einstellungen unter Windows z.B. Group Policies Darstellung wesentlicher Abweichungen	**Information**	**Kontrollaktivität**	**Prüfung**
Darstellung des Prozesses entsprechend der MaRisk für Eigenentwicklungen, usw. AT 7.2	**Prozessbearbeitung nachweisen**	**Kontrollaktivität**	**Prüfung**
IT-Geschäftsprozesse			
Darstellung von wesentlichen Standardabweichungen bei den Prozessen	**Information**	**Information und Kontrollaktivität**	**Prüfung**
Prüfung der Logdateien unter z.B.webmin	**Information/Kontrollen**	**Kontrollaktivitäten**	**Prüfung**

Zusätzliche Themenbereiche			
IT-Outsourcing			
Hinweise zum IT- Outsourcing in der Zusammenfassung auch zu den obigen Punkten	**Information**	**Information**	**Information/Auswertung**
Möglichkeit um Hinweise zu erhaltenen Prüfungsberichten zu geben	**Information**	**Information**	**Auswertung der externen Prüfungsberichte und Hinweise dazu im Tool**
Hinweise zu den Regelungen der MaRisk	**Information**	**Information/Kontrollaktivitäten**	**Information/Kontrollaktivitäten**
Internet und E-Mail			
Darstellung der Regelungen für die Nutzung z.B. Mail-Archivierung Regelungen Internetseite (Uhrheberrecht, Impressum, Nennung der Verantwortliche für die Seite)	**Information**	**Kontrollaktivitäten**	**Prüfung**