Musterbericht – MC Banksoftware

Monat 20XX **Prüfungsplan**

Prüfungsbereich

IT Management

Prüfung der IKT Prozesse entsprechend der aufsichtsrechtlichen Anforderungen

Name

Inhaltsverzeichnis

Hinweis:
Anpassungen zur Version 1.0 sind in blau dargestellt. Neue Prüfungshinweise zur EBA Leitlinie für das Management von IKT- und Sicherheitsrisiken vom 28. November 2019 sind dabei jedoch grün gekennzeichnet.

Zentrale Entziehung nicht benötigter Rechte	
Erkennung und Definierung toxischer Rechtekombinationen ist erfolgt	
..	

4.5.2 Maßnahmen zur logischen Sicherheit

In Ergänzung der bisherigen Aussagen werden nachstehende Prüfungsergebnisse dargestellt:

Die Zugriffsrechte auf IT-Assets und deren Unterstützungssysteme sind nach dem Grundsatz „Need to know“ erstellt und verwaltet, dies gilt auch für den Fernzugang. Wir haben dies in einer Stichprobe geprüft……

Der Personalveränderungsbogen und die Regelungen sehen vor, dass nur Zugangsrechte, die zur Erfüllung der Aufgaben unbedingt erforderlich sind (nach dem Grundsatz „Least Privilege“) vergeben werden. Wir haben dies in einer Stichprobe geprüft……

Die Verwendung allgemeiner und gemeinsamer Nutzerkonten haben wir in folgendem Umfang festgestellt…….

Die Anzahl der Konten mit erhöhten Systemzugangsrechten sind begrenzt und werden genau überwacht.
Ein administrativer Fernzugriff auf kritische IKT-Systeme wird nur…… Personen zugeordnet. (Privilegierte Zugriffsrecht). Deren Aktivitäten werden überwacht und archiviert. Aufbewahrungsfristen werden beachtet.
Zugriffsrechte werden rechtzeitig gewährt, entzogen oder geändert. Für den Fall einer Beendigung des Beschäftigungsverhältnisses sollten die Zugriffsrechte unverzüglich entzogen werden. Dies haben wir in einer Stichprobe geprüft.

4.5.3 Gebäude und IT-Systeme (physische Sicherheit)

Der Zutritt in das Bankgebäude, die Serverräume…. erfolgt mittels eines Transponders. Ein Rechtssystem besteht. Geschützte Bereiche sind definiert. Ein Sollkonzept besteht. Zutrittsprofile sind definiert Der Zugang zu den Serverräumen und Verteilungssystemen ist IT gesteuert. Nur berechtigte Personen haben Zugriff. Die Rechtesysteme für die Zugangssteuerung basieren auf Profilen. Diese haben wir geprüft. Nachfolgende Erkenntnisse ergaben sich….

4.5.4 Rezertifizierung

Dieser Prozess ist Teil der logischen Sicherheit. Grundlagen ergeben sich in den MaRisk und den BAIT. Ein angewiesener Prozess besteht. Wir haben den Prozess, die Ergebnisse und Maßnahmen dazu in einer Stichprobe überprüft.

Nachfolgend ein Überblick der letzten 2 Rezertifizierungszeiträume für halbjährliche und jährliche Überprüfungen.

9. Qualitätsbeurteilung der gesamten Prüfung

Auf der Grundlage der erfolgten Prüfungshandlungen wird festgestellt, dass ein *grundsätzlich/insgesamt/nicht im vollen Umfang* angemessen angewiesenes Risikomanagementsystem und Internes Kontrollsystem vorgefunden wurde. In der Praxis haben wir *grundsätzlich/insgesamt/nicht im vollen Umfang* wirksame Prozesse festgestellt. Die Kontrollziele wurden *grundsätzlich/insgesamt/nicht im vollen Umfang erreicht*

Es ergaben sich nachstehende Feststellungen:

Anzahl der Feststellungen	
Anzahl der Hinweise	
Anzahl der Empfehlungen	

10. Ursachenanalyse

Sollten sich Feststellungen ergeben haben wird an dieser Stelle über die Ursachen der Feststellungen berichtet.

11. Erklärung zur Prüfung

Die Governance Systeme sowie Prozesse für die IKT- und Sicherheitsrisiken eines Finanzinstituts wurden im Rahmen dieser Prüfung geprüft. Der Prüfer hat sich intern und extern weitergebildet. Die Unabhängigkeit der Prüfer wird hiermit bestätigt. Interessenskonflikte ergaben sich nicht.

Die Häufigkeit und der Schwerpunkt ergibt sich aus der Risikoorientierung und ist entsprechend der IKT- und Sicherheitsrisiken angemessen.

Der vom Vorstand genehmigte Auditplan und seine Ausführung einschließlich der Häufigkeit der Audits berücksichtigen die IKT- und Sicherheitsrisiken im Finanzinstitut, stehen in einem angemessenen Verhältnis zu diesen und werden regelmäßig aktualisiert.

Ein formeller Prozess zur Nachverfolgung einschließlich Vorkehrungen für die rechtzeitige Überprüfung und Behebung kritischer Feststellungen der IKT-Prüfung sollte festgelegt werden.[29]

[29] EUROPEAN BANKING AUTHORITY (EBA): EBA/GL/2019/04 EBA Leitlinie für das Management von IKT- und Sicherheitsrisiken vom 28. November 2019:Rz 25 bis 27