FORUM Gesellschaft für Informations-sicherheit mbH, Dresden

Dresden, 25. Mai 2023

Henning Riediger

Aktuelle Anforderungen der Bankenaufsicht

- ***Aktualisierung***
- ***Prüfungsthemen***
- ***Fallstudien***

DISCLAIMER

- Dieser Vortrag spiegelt ausschließlich die persönliche Meinung des Referenten und nicht notwendigerweise die der Deutschen Bundesbank wider.

Angaben zur Person

- **Henning Riediger**
  Diplom-Betriebswirt (FH)
- 2001 Deutsche Bundesbank,
  Studium an der Hochschule Hachenburg
- 2004 **Deutsche Bundesbank**
  2014 **Prüfungsleiter** im Referat
  Bankgeschäftliche Prüfungen, Hannover
- **Schwerpunkte**
  Gesamtbanksteuerung/Risiko-Controlling
  Internes Kontrollsystem
  Informationstechnologie
  Outsourcing

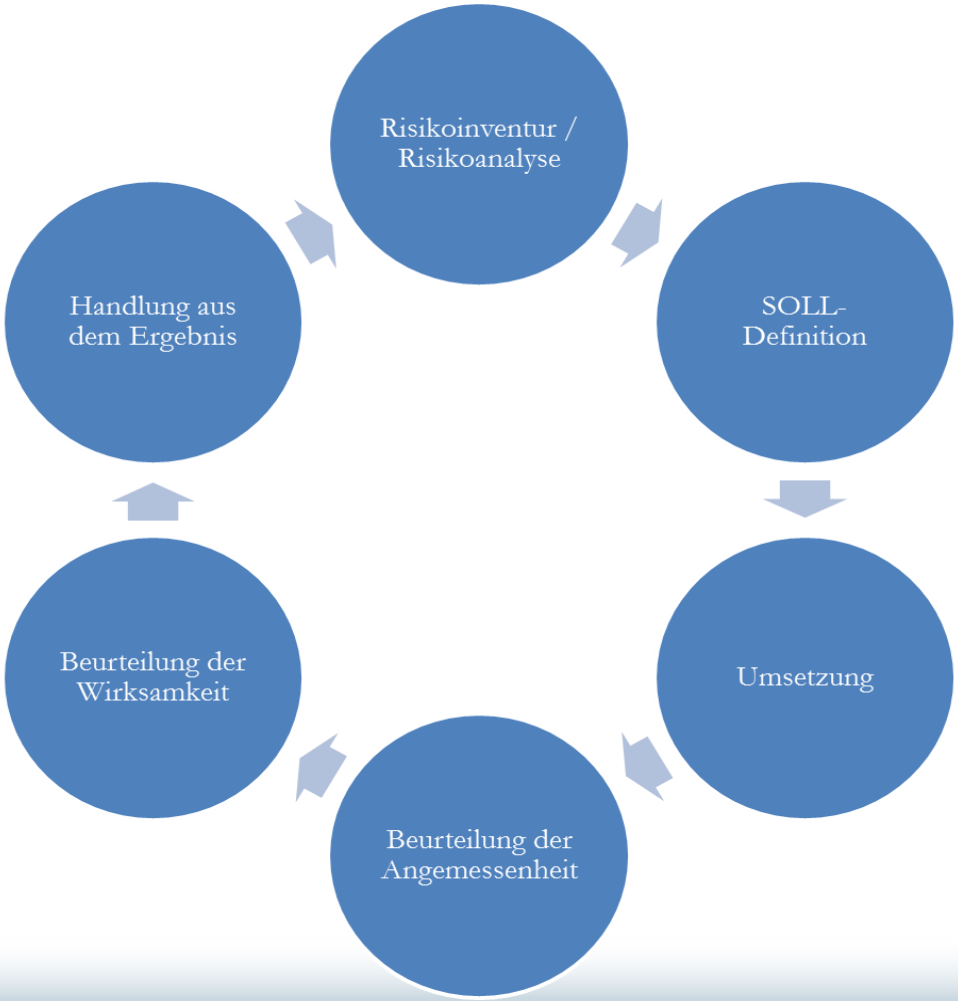
AGENDA

- Risikomanagement und Risikokultur
- Aktuelle Aufsichtsschwerpunkte
- Aktuelle Prüfungserfahrungen
- Teilnehmer-Themen

RISIKOMANAGEMENT UND RISIKOKULTUR

Risikomanagement und Risikokultur

Steuerungs- und Überwachungsprozess



Aufsichtliche Prüfgebiete

- Kontrollzweck
- Vollständigkeit versus Risiko
- **Funktionsfähigkeit**

Handlungserfordernisse

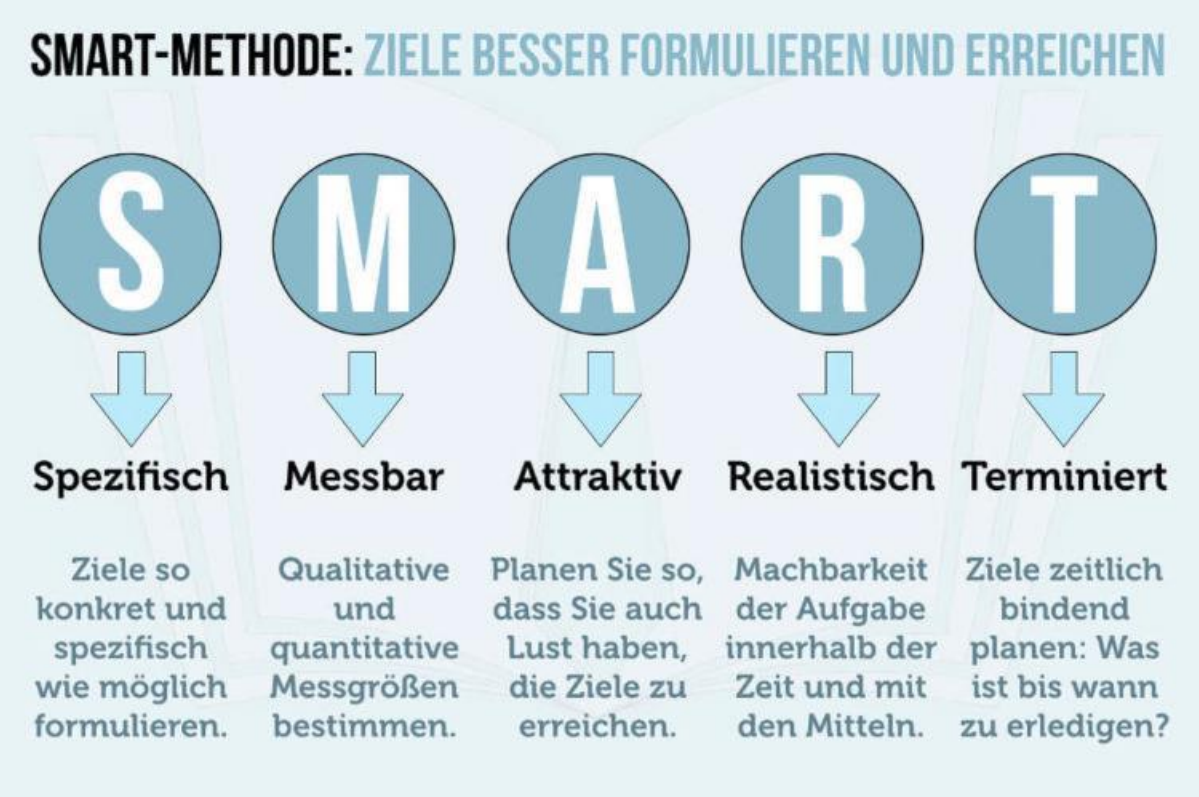
- Frequenz festlegen
- Zuständigkeiten definieren
- Berichtswege festlegen
- Toleranzen definieren
- Ergebnisse festhalten

IT-Governance …

- ... ist die Struktur zur Steuerung sowie Überwachung des Betriebs und der Weiterentwicklung der IT-Systeme und IT-Prozesse
  - Elementarer Bestandteil des **Internen Kontrollsystems** eines Instituts (IKS!)
- für wirksame Umsetzung ist der Vorstand verantwortlich
- Angemessene Personalausstattung im IT-IKS
- Vermeidung von Interessenskonflikten und mit einander unvereinbaren Tätigkeiten (analog MaRisk)
  - Funktionstrennung umsetzen!!!

Strategien

- **Anforderungen an strategische Vorgaben – auch in der IT-Strategie**



Berichtswesen

- **BAIT Tz. 3.11**
  - „Die Geschäftsleitung ist regelmäßig, mindestens jedoch vierteljährlich, insbesondere über die Ergebnisse der Risikoanalyse sowie Veränderungen an der Risikosituation zu unterrichten.”
    - Damit die Geschäftsleitung die richtigen Entscheidungen bei der Steuerung und Lenkung des IRM-Prozesses treffen kann, benötigt sie Informationen über den aktuellen Stand und die Entwicklung des IRM.
    - Die Leitungsebene muss in angemessener Form über die Ergebnisse der Überprüfungen und den Status des IRM informiert werden. Dabei sollten **Probleme, Erfolge und Verbesserungsmöglichkeiten** aufgezeigt werden.
    - U. a. sollten hierbei die folgenden Aspekte berücksichtigt werden:
      - Status der Risikoanalysen (ausstehend, durchgeführt)
      - Maßnahmenstatus (Grad der umgesetzten Soll-Maßnahmen auf Informationsverbund)
      - Risiken (Restrisiken, akzeptierte Risiken, nicht berücksichtigte Bedro-hungen und Schwachstellen)
      - alle Veränderungen, die Einfluss auf das IRM haben könnten
      - Die Risikosituation enthält auch externe potenzielle Bedrohungen.
      - Projektstatus

AKTUELLE AUFSICHTS-SCHWERPUNKTE

Prüfungsthemen

- IT-Organisation
  - IT-Aufbauorganisation
  - IT-Ablauforganisation
- IT-Strategien
- Informationsrisiko- und Informationssicherheitsmanagement
  - Netzwerksicherheit
  - Kryptografie
  - Sonstige Operative Informationssicherheit
  - Informationssicherheitsvorfallmanagement und IT-Forensik
- Identitäts- und Benutzerberechtigungsmanagement
- SIEM
- Projektmanagement
- Anwendungsentwicklung (inklusive IDV)
- Physische Sicherheit
- Incident- und Problemmanagement
- Change-, Release- und Deploymentmanagement
- Konfigurationsmanagement
- Auslagerungen, sonstiger Fremdbezug von IT-Dienstleistungen
- Buiseness Continuity Management
- IT-Revision

Informationsrisikomanagement - Risikoübernahme und -steuerung

- **Risikobehandlungsoptionen (TARA-Prinzip) ... Risiken ...**
  - vermieden werden, indem beispielsweise die Risikoursache ausgeschlossen wird,
  - reduziert werden, indem die Rahmenbedingungen, die zur Risikoeinstufung beigetragen haben, modifiziert werden (Risikominimierende Maßnahmen),
  - transferiert werden, indem die Risiken mit anderen Parteien geteilt werden,
  - akzeptiert werden, beispielsweise weil die mit dem Risiko einhergehenden Chancen wahrgenommen werden sollen.
- **Risikovermeidung**
  - Ist es sinnvoll, das Risiko durch eine Umstrukturierung des Geschäftsprozesses oder des Informationsverbunds zu vermeiden? Gründe für diesen Ansatz können beispielsweise sein:
    - Alle wirksamen Gegenmaßnahmen sind mit hohem Aufwand verbunden und damit sehr teuer, die verbleibende Gefährdung kann aber trotzdem nicht hingenommen werden.
    - Die Umstrukturierung bietet sich ohnehin aus anderen Gründen an, z. B. zur Kostensenkung.
    - Es kann einfacher und eleganter sein, die vorhandenen Abläufe zu ändern, als sie durch Hinzufügen von Sicherheitsmaßnahmen komplexer zu machen.
    - Alle wirksamen Gegenmaßnahmen würden erhebliche Einschränkungen für die Funktion oder den Komfort des Systems mit sich bringen.

Informationsrisikomanagement - Risikoübernahme und -steuerung

- **Risikoreduktion (Risikomodifikation)**
  - Ist es sinnvoll und möglich, das Risiko durch weitere Sicherheitsmaßnahmen zu reduzieren? => Risikominimierende Maßnahmen
  - Das Risiko durch die verbleibende Gefährdung kann möglicherweise gesenkt werden, indem eine oder mehrere ergänzende Sicherheitsmaßnahmen erarbeitet und umgesetzt werden, die der Gefährdung entgegenwirken. Als Informationsquellen über ergänzende Sicherheitsmaßnahmen kommen beispielsweise folgende infrage:
    - die Dokumentation und der Service des Herstellers, wenn es sich bei dem betroffenen Zielobjekt um ein Produkt handelt,
    - Standards und Best Practices, wie sie beispielsweise von Gremien im Bereich der Informationssicherheit erarbeitet werden,
    - andere Veröffentlichungen und Dienstleistungen, die beispielsweise im Internet oder von spezialisierten Unternehmen angeboten werden,
    - Erfahrungen, die innerhalb der eigenen Institution oder bei Kooperationspartnern gewonnen wurden. Der hypothetische Aufwand und mögliche Kosten für gegebenenfalls erforderliche Sicherheitsmaßnahmen und Informationen über bereits vorhandene Sicherheitsmechanismen sind wichtige Entscheidungshilfen.
  - **Die Wirksamkeit der Risikominimierenden Maßnahmen muss kontinuierlich überprüft werden.** Hierzu sollte es ein Übersicht der risikominimierenden Maßnahmen und deren aktuellen Umsetzungstand (Wirksamkeit) geben. Nur vollständig umgesetzte und auf Wirksamkeit geprüfte risikominimierenden Maßnahmen können auch risikominimierende bei der Risikobewertung angesetzt werden.

Informationsrisikomanagement - Risikoübernahme und -steuerung

- **Risikotransfer (Risikoteilung)**
  - Ist es sinnvoll, das Risiko an eine andere Institution zu übertragen, beispielsweise durch den Abschluss eines Versicherungsvertrags? Gründe für diesen Ansatz können beispielsweise sein:
    - Die möglichen Schäden sind rein finanzieller Art.
    - Es ist ohnehin aus anderen Gründen geplant, Teile der Geschäftsprozesse auszulagern.
    - Der Vertragspartner ist aus wirtschaftlichen oder technischen Gründen besser in der Lage, mit dem Risiko umzugehen.
  - Wenn im Rahmen der Risikobehandlung zusätzliche Sicherheitsanforderungen identifiziert werden, muss die Risikoeinstufung (siehe nachfolgende Beispiele) für die betroffenen Zielobjekte entsprechend angepasst werden. Zu beachten ist dabei, dass neue Anforderungen unter Umständen nicht nur Auswirkungen auf das jeweils analysierte Zielobjekt haben, sondern auch auf andere Zielobjekte. Die zusätzlichen Anforderungen und die daraus resultierenden Sicherheitsmaßnahmen werden im Sicherheitskonzept dokumentiert.

Informationsrisikomanagement - Risikoübernahme und -steuerung

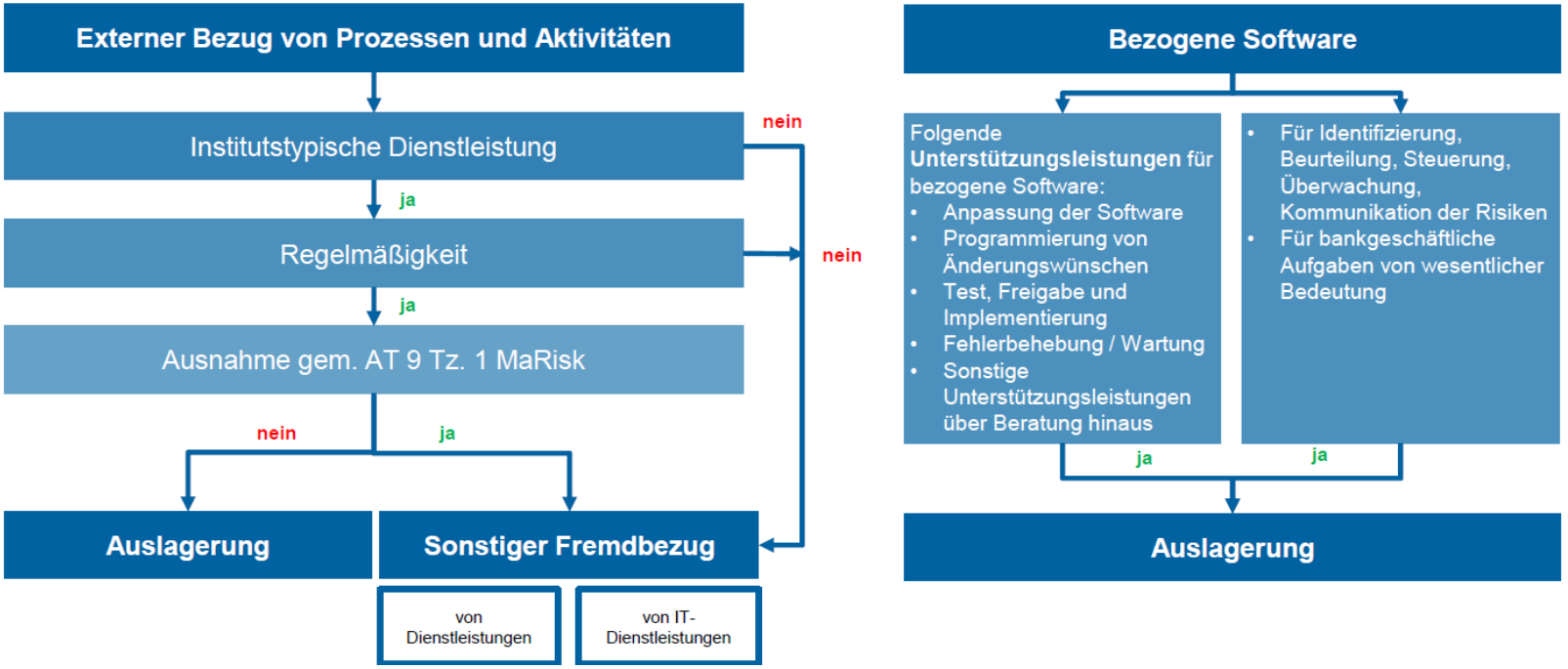
- **Risikoakzeptanz**
  - Können die Risiken auf Basis einer nachvollziehbaren Faktenlage akzeptiert werden? Die Schritte der Risikoeinstufung und Risikobehandlung werden so lange durchlaufen, bis die Risikoakzeptanzkriterien der Institution erreicht sind und das verbleibende Risiko („Restrisiko“) somit im Einklang mit den Zielen und Vorgaben der Institution steht.
  - Das Restrisiko muss anschließend der Leitungsebene zur Zustimmung vorgelegt werden (Risikoakzeptanz). Damit wird nachvollziehbar dokumentiert, dass die Institution sich des Restrisikos bewusst ist.
  - Idealerweise akzeptiert eine Institution nur Risiken der Stufe „gering“. In der Praxis ist dies aber nicht immer zweckmäßig. Gründe, auch höhere Risiken zu akzeptieren, können beispielsweise sein:
    - Die entsprechende Gefährdung führt nur unter ganz speziellen Voraussetzungen zu einem Schaden.
    - Gegen die entsprechende Gefährdung sind derzeit keine wirksamen Gegenmaßnahmen bekannt und sie lässt sich in der Praxis auch kaum vermeiden.
    - Aufwand und Kosten für wirksame Gegenmaßnahmen überschreiten den zu schützenden Wert.

Informationsrisikomanagement - Risikoübernahme und -steuerung

Quelle: Dr. Markus Held (Hrsg.), in: Schutzbedarfsfeststellungen und Risikoanalysen, Abb. 7, Seite 27, Heidelberg 202.0

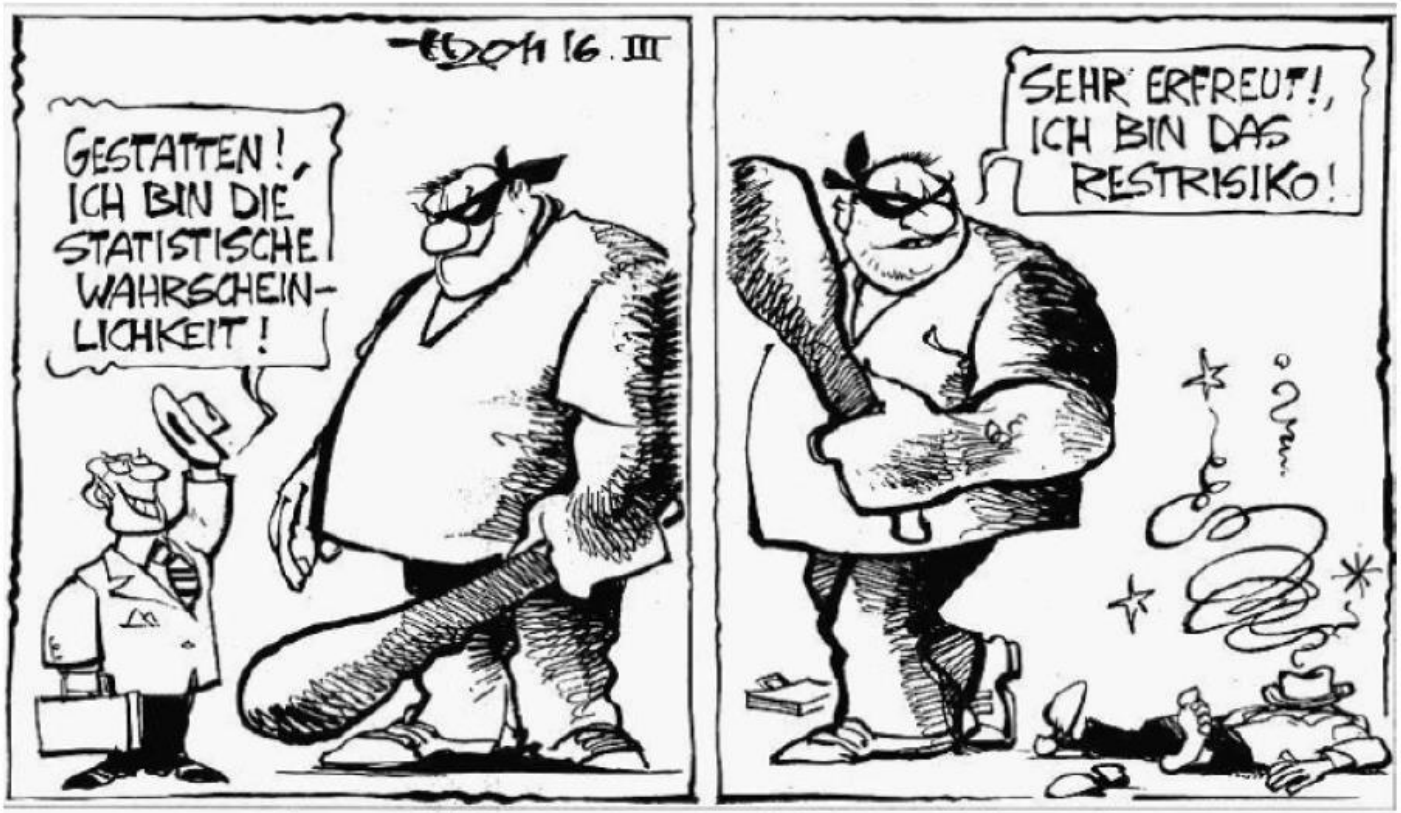
Auslagerungen

- **Identifikation und Zuordnungsentscheidung**



Für bankgeschäftliche Aufgaben von wesentlicher Bedeutung …

Beispiele:
- Kernbanksysteme
- Software, die im Rahmen des Kreditgeschäfts genutzt wird (inkl. Vertragserstellung, Sicherheitenbewertung, elektronische Aktenführung)
- Software im Liquiditätsmanagement / Treasury
- Software in Geldautomaten, Kontoauszugdruckern und Kundenterminals
- …

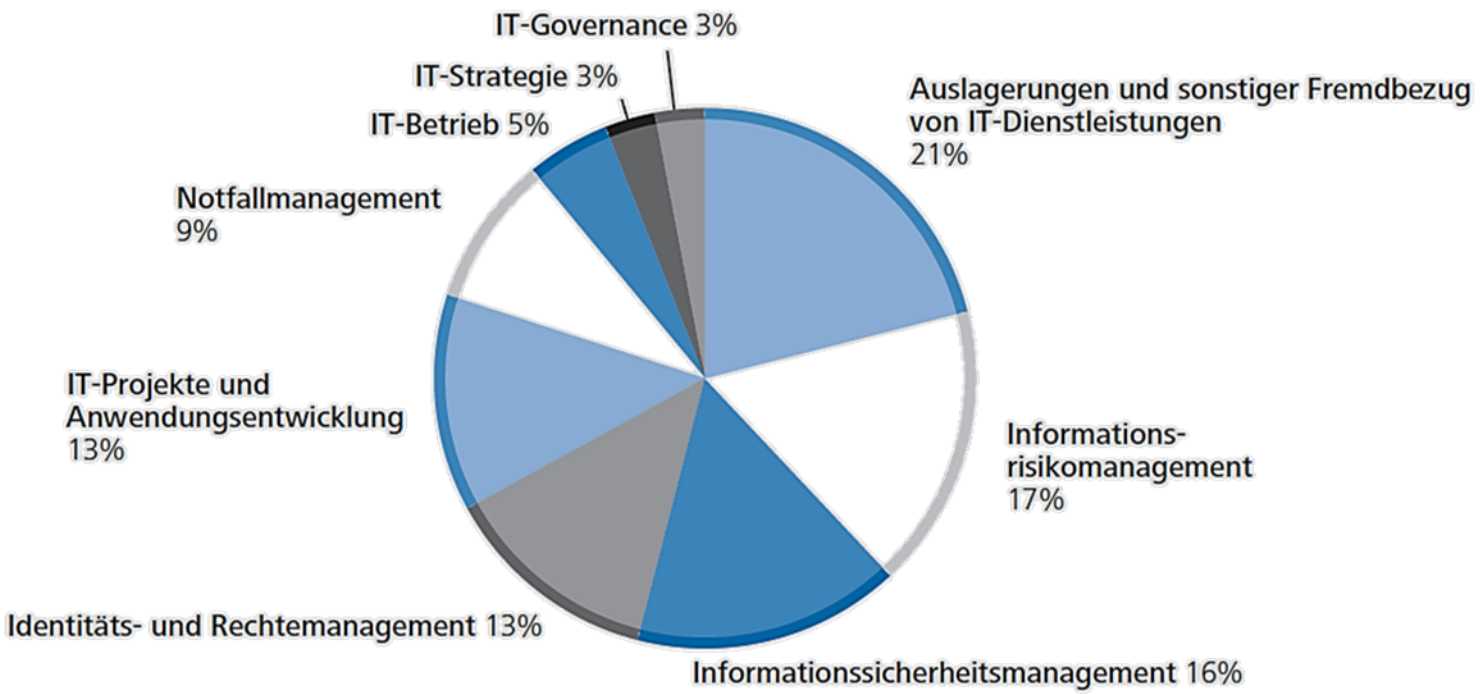


Zeichnung: Horst Haitzinger

AKTUELLE PRÜFUNGSERFAHRUNGEN

Feststellungen im IT-Bereich

- **Rückblick über die letzte Dekade**



Angaben ohne Gewähr

Informationssicherheitsmanagement - Zusammenfassung (= Baustellen)

- **Hauptkritikpunkte**
  - Der Informationssicherheitsbeauftragte ist nicht unabhängig.
  - Die Richtlinien/Sicherheitsrichtlinien/Konzepte sind nicht vollständig und/oder stehen im Widerspruch zur Informationssicherheitsleitlinie.
  - Es findet keine Überprüfung der Vorgaben in den Richtlinien und deren konkrete Ausformulierung in den Arbeitsanweisungen und technischen Konzepten der 1st-Line sowie deren Umsetzung in den IT-Systemen statt => Internes Kontrollsystem
  - Es werden keine bzw. nur unzureichenden Überprüfungen der Sicherheitsmaßnahmen durchgeführt.
  - Es finden keine bzw. unzureichende Schulungsmaßnahmen zum Thema Informationssicherheit statt.
  - Der Informationssicherheitsbeauftragte ist nicht bzw. nur unzureichende in den Managementprozess zu den Themen Auslagerung und Notfallmanagement eingebunden.

Informationsrisikomanagement - Zusammenfassung! (= Baustellen)

- Anforderungen an den Sollmaßnahmenkatalog
  - objektiv überprüfbar
    - Soll-Ist-Abgleich muss möglich sein
    - Sachkundige Dritte müssen sich in angemessener Zeit einlesen können
  - Institutsspezifisch!
  - Verprobung auf den (instituts)relevanten Standard (!)
  - Maßnahme muss umsetzbar sein / Einbindung Fachbereiche
  - Risikoorientierte Umsetzung möglich (Art, Umfang und Turnus)
    aber: Begründung muss nachvollziehbar und plausibel sein
    Stichwort: Expertenschätzung
  - [bei Auslagerung!] Detailausgestaltung muss bekannt sein und mit eigenen Anforderungen verprobt sein … Was macht mein DL?
  - Funktionsfähigkeit und Wirksamkeit der Kontrolle bzw. Schutzmaßnahme muss sichergestellt sein
  - Laufende Überwachung auf Sinnhaftigkeit bzw. Arbitrage
  - Papier ist geduldig! Umsetzung erforderlich

Security Information & Event Management - Zusammenfassung! (= Baustellen)

- **Hauptkritikpunkte**
  - Es ist nicht definiert, wann es sich um ein Sicherheitsrelevantes Ereignis handelt.
  - Es liegt keine vollständige und/oder qualitätsgesicherte Infrastrukturanalyse vor.
  - Es existieren keine Richtlinien, welche Informationen zu sammeln sind (Loggingkonzept).
  - Die Logdateien sind nicht manipulationssicher abgelegt.
  - Es erfolgt keine bzw. unvollständige Auswertung der Loginformationen.
  - Die Bewertung der Risiken (z. B.: noch nicht vorliegenden Auswertungsregeln, noch nicht angebunden Systemen) erfolgt nicht
  - Die Steuerung der Bearbeitung der sicherheitsrelevanten Ereignisse erfolgt nicht durch bzw. unter Beteiligung des Informationssicherheitsbeauftragten.
  - Eine korrelierte Auswertung von einzelnen sicherheitsrelevanten Ereignissen und /oder Incidents und Problems erfolgt nicht.
  - Es gibt keine Regelungen für die forensische Auswertung.

Beispielfeststellungen (Institut A - 1)

- Bei der Festlegung der Schutzbedarfe wurden **nicht die verarbeiteten Informationen zugrunde gelegt**, die **Begründung** für die finalen Einstufungen sind **nicht dokumentiert** und damit **nicht nachvollziehbar**. Außerdem existierte zum Prüfungszeitpunkt kein nachweisbar und strukturiert hergeleitetes Soll-Schutzniveau, welches über den Schutzbedarf für Prozesse hinausgeht, da die letztmalige Schutzbedarfsanalyse nicht beendet wurde. Die Bank hat zum Prüfungszeitpunkt keinen Soll-Ist-Abgleich, der eine strukturierte, systematische und vollständige Überprüfung der Umsetzung der Soll-Vorgaben aus dem Sollmaßnahmen-Katalog angemessen sicherstellen kann.
- Eine weitere schwerwiegende Feststellung trafen wir im Bereich **Identitäts- und Berechtigungsmanagement**. So können unternehmensweit nicht miteinander vereinbare Berechtigungskombinationen nicht systematisch erkannt und verhindert werden. Anwendungsberechtigungskonzepte fehlen oder lassen wichtige Regelungsinhalte vermissen.

Beispielfeststellungen (Institut A - 2)

- Abteilungsberechtigungskonzepte lassen **wichtige Inhalte vermissen**, wurden teils **nicht sachgerecht freigegeben** oder ihre Freigabe ist unzureichend dokumentiert. Dadurch sind die Soll-Berechtigungen nicht klar und kompetenzgerecht geregelt. Weiterhin fehlen **notwendige, zeitnahe Kontrollprozesse hinsichtlich der Rollenadministration und der Berechtigungs-administration** sowie Kontrollprozesse zur Vollständigkeit der Anwendungsberechtigungskonzepte, zur Nutzung unpersönlicher Benutzerkonten und zur Nutzung der Blacklist für die Sperre von Anwendungen. Außerdem können wichtige Kontrollhandlungen, die angabegemäß durchgeführt werden, mangels systematischer Dokumentation nicht nachvollzogen werden. Transparenz über das Berechtigungsmanagement der Weiterverlagerungsnehmer besteht nicht, wodurch unklar ist, in welchem Umfang dort Berechtigungen auf Informationen oder von der Bank benötigte Ressourcen bestehen und ggf. die Schutzbedarfsanforderungen der Bank kompromittieren.

Beispielfeststellungen (Institut A - 3)

- Die Rezertifizierung besteht lediglich aus einem teilweisen Soll-Ist-Abgleich eines **veralteten, nicht überprüften Berechtigungs-Soll** mit einem nicht qualitätsgesicherten Berechtigungs-Ist für einen Teilbestand der Berechtigungen. Die Nutzung **privilegierter Berechtigungen** wird nicht **systematisch, zeitnah und wirksam kontrolliert**. Schließlich ist eine zügige Bearbeitung berechtigungsrelevanter Tickets nicht sichergestellt, was seitens der Bank mit der Personalausstattung begründet wird

Beispielfeststellungen (Institut A - 4)

- Dann trafen wir eine schwerwiegende Feststellung zum Security Information and Event Management (SIEM). Die Prozessvorgaben der Bank sind widersprüchlich bezüglich des Geltungsbereichs, ihre Inhalte reichen nicht aus, um darauf aufbauend adäquat eine diesbezügliche Auslagerung zu definieren und zu kontrollieren. Definierte Prozesse sind weder in der Bank noch beim Auslagerungsnehmer vorhanden. Zum Prüfungszeitpunkt ist der Abdeckungsgrad der SIEM-Lösung nicht ausreichend, da nur ein geringer Anteil von vorgesehenen Anwendungen und System- bzw. Infrastruktur-komponenten zumindest teilweise angebunden sind und Logdaten zur Verfügung stellen. Von den angebundenen Datenquellen wird auch erst ein Teil über Regeln zur Bestimmung potenziell sicherheitsrelevanter Ereignisse überwacht. Eine zeitnahe Lieferung und Verarbeitung von Ereignissen durch die SIEM-Lösung ist nicht vollumfänglich gewährleistet, da Logdaten von verschiedenen Dienstleistern nur mit Verzögerungen geliefert werden.
-

Beispielfeststellungen (Institut A - 5)

- Auch eine zeitnahe Reaktion auf durch die SIEM-Lösung gemeldeten Alarme ist nicht gewährleistet, da das SOC nicht durchgängig besetzt ist und die Abdeckung der restlichen Zeiten durch ein spezielles Team nicht ausreichend ist. Die Analyse einer Stichprobe von Alarmmeldungen ergab, dass eine ordnungsgemäße und zeitgerechte Abarbeitung nicht sichergestellt ist. Die Bank hat keine Kontrollen bezüglich des SIEM-Prozesses definiert oder etabliert. Auch für Dienstleister ist keine wirksame Kontrollfunktion vorhanden und seitens des Dienstleisters selbst sind angemessene Prozesskontrollen weder formal definiert noch nachvollziehbar dokumentiert, was sowohl die Erweiterung und Pflege der SIEM-Infrastruktur als auch die Bearbeitung der SIEM-Alarmtickets betrifft. Schließlich beinhaltet das Berichtswesen der Bank keine konkreten SIEM-bezogenen Inhalte

Beispielfeststellungen (Institut A - 6)

- Eine weitere schwerwiegende Feststellung betrifft das Auslagerungsmanagement. In den Regelungen der Bank sind die Aufgaben des zentralen Auslagerungsmanagements, insbesondere zur Steuerung und Kontrolle, ob die Fachbereiche ihre Aufgaben im Auslagerungsmanagement angemessen erfüllen und Risiken ihrer ausgelagerten Dienstleistungen entsprechend steuern, nicht hinreichend festgelegt. Die Vertragsliste ist unvollständig, sodass nicht enthaltene Auslagerungen nicht erkannt werden können, wobei auch innerhalb der Vertragsliste diverse Auslagerungen nicht als solche identifiziert wurden. Der Prozess zur Klassifizierung von Fremdbezügen und zur Risikoanalyse weist diverse Schwächen auf. Vier Verträge für wesentliche Auslagerungen beinhalten Mängel bezüglich der Vereinbarung regulatorisch geforderter Mindestvertragsinhalte. Vor allem der maßgebliche IT-Dienstleiser erhält durch fehlende Leistungsspezifizierungen zu viel Entscheidungsspielraum in Bereichen, die originär die Bank zu verantworten hat. Weiterhin liegen für vier wesentliche Auslagerungen keine Handlungsoptionen für den Fall der unbeabsichtigten oder unerwarteten Beendigung vor, für drei weitere sind sie unvollständig.

Beispielfeststellungen (Institut A - 7)

- Die Umsetzung der Dienstleistersteuerung und -überwachung ist unzureichend, da z. B. Informationen und Berichte, welche die Bank von ihren Dienstleistern erhält, weder systematisch und dokumentiert ausgewertet noch Maßnahmen aus den gewonnenen Erkenntnissen abgeleitet werden. Schließlich ist das zentrale Auslagerungsmanagement mit Ausnahme der Berichterstattung nicht in die Identifizierung, Bewertung und Behandlung von Risiken im Zusammenhang mit Auslagerungen involviert. Darüber hinaus ist die Berichterstattung zu den Risiken im Zusammenhang mit Auslagerungen nicht aussagekräftig und somit nicht beurteilbar.

Beispielfeststellungen (Institut A - 8)

- Die letzte schwerwiegende Feststellung trafen wir zum Notfallmanagement. Zum Prüfungszeitpunkt verfügte die Bank weder über Prozesslandkarte noch über eine Geschäftsauswirkungsanalyse (Business Impact Analyse), die aktuell, vollständig und qualitätsgesichert waren. Eine Gefährdungsanalyse (Risk Impact Analyse) wurde von der Bank weder durchgeführt noch ist sie überhaupt ein prozessualer Bestandteil des Notfallmanagements. Die Vorgaben für die Notfallkonzepte (Business Continuity Pläne) sowie die Notfallkonzepte selbst sind mangelhaft, die Übersichten über notfallrelevante Tools und Dienstleister nicht angemessen. Notfalltestpläne existieren nicht für alle relevanten Szenarien, die Notfalltestplanung ist nicht angemessen, die durchgeführten Notfalltests sind nicht ausreichend und deren Dokumentation ist unzureichend.

Beispielfeststellungen (Institut B - 1)

- Die folgende Tabelle zeigt, wie besonders schützenswerte Informationen mit Rechnungswesen-, Meldewesen-, Zahlungsverkehrs-, und Risikomanagementrelevanz definiert werden, sodass eine Einstufung in die höchste Schutzniveauklasse erfolgt:

Informationskategorien/ Informationscluster	Vertraulichkeit	Integrität	Verfügbarkeit
Daten des Rechnungswesens mit GoB-Relevanz	x	3	x
Daten zur Veröffentlichung mit oder ohne gesetzlicher Publizitätspflicht	x	3	x
Allgemeine Zahlungsverkehrsdaten	x	3	x
Sensible Zahlungsverkehrsdaten	x	3	3
Risikomanagement (inkl. Risikocontrolling)	x	3	x
Besonders personenbezogene Daten (z.B. Gesundheitsdaten, religiöse bzw. Gewerkschaftszugehörigkeit)	3	x	x

- Darüber hinaus bestehen keine weiteren objektiv überprüfbaren Kriterien zur Ableitung des Schutzbedarfs. Die Ableitung des Schutzbedarfs weist insofern Schwächen auf, als die vorgegebenen Kriterien nicht hin-reichend konkret definiert wurden. Es fehlen objektiv ausgearbeitete Richtlinien, an denen sich Mitarbeiter bei der Bestimmung des Schutzbedarfes orientieren können, um eine einheitliche Bewertung nach ein-schlägigen Kriterien zu ermöglichen. Zudem bestehen hinsichtlich der Verfügbarkeit keine weiteren Kriterien als die geschätzte Schadenshöhe bei einer Nicht-Verfügbarkeit oder dem Verlust von Daten. Die Berücksichtigung einer zeitkritischen Komponente fehlt hinsichtlich der Verfügbarkeit gänzlich.

Beispielfeststellungen (Institut B - 2)

- Feststellung (F2): Kriterien zur Ableitung des Schutzbedarfs (AT 7.2 Tzn. 4 und 5 MaRisk)
  - Die Kriterien zur Ableitung des Schutzbedarfs sind nicht hinreichend konkret definiert worden. Darüber hinaus ermöglichen die Kriterien keine eindeutige und ausreichend nachvollziehbare Bestimmung des Schutzbedarfs.
  - Gemäß AT 7.2 Tzn. 4 und 5 MaRisk sind angemessene Steuerungs- und Überwachungsprozesse, u. a. für die Festlegung des Schutzbedarfs und den daraus abgeleiteten Schutzmaßnahmen für den IT-Betrieb, insbesondere hinsichtlich der IDV-Anwendungen, einzurichten.

Beispielfeststellungen (Institut B - 3)

- Bei der Überführung einer IDV-Anwendung von der Entwicklungs- in die Testumgebung versendet der Business Architect die entsprechende Datei ohne Passwortschutz per E-Mail an die Testperson. Die Test-person vergibt daraufhin ein Passwort für die Datei und legt diese in der Testumgebung ab. Weitere Sicherheitsmaßnahmen oder Siegelungen bestehen nicht. Dieser Vorgang wird nicht dokumentiert und kann so-mit nicht nachvollzogen werden. Zudem wird nicht ausreichend sichergestellt, dass nur die Testperson schreibenden Zugriff auf die Testumgebung hat und der Entwickler keine Änderungen in der Testumgebung vornehmen kann.
- Die Mitarbeiter, die in der Doppelfunktion aus Anwender und Entwickler tätig sind, werden sensibilisiert, ausschließlich rollenadäquat auf Entwicklungs- und Produktivumgebung zuzugreifen. Dennoch ist es dem Entwickler möglich, nach der Freigabe der IDV-Anwendung weiterhin Änderungen an der Datei vorzunehmen und diese veränderte Datei dann in der Produktivumgebung einzusetzen.
- Die IDV-Anwendungen RTF-Rechnung und Kapitalplanung wurden beide am 15.05.2022 durch den FAO freigegeben. Beide IDV-Anwendungen haben sich aber bereits vor der eigentlichen Freigabe im Einsatz befunden.

Beispielfeststellungen (Institut B - 3)

- Weiterhin besteht hinsichtlich der Testung zu beiden IDV-Anwendungen keine Dokumentation. Diese soll im Rahmen der Verfahrensdokumentation bis zum Jahresende 2022 nachgeholt werden. Die Bestätigung über die ordnungsgemäße Durchführung der fachlichen Tests erfolgte zu beiden Anwendungen zudem erst am 13.05.2022. Somit wurden die IDV-Anwendungen RTF-Rechnung und Kapitalplanung ebenfalls eingesetzt, bevor die Durchführung der fachlichen Tests bestätigt wurde.
- Zudem wird das Kapitalplanungstool erst seit April 2022 als IDV-Anwendung im Inventar geführt. Davor wurde die IDV im Fachbereich selbstständig verwaltet. Die IDV-Anwendung Kapitalplanung wurde vom Fachbereich nicht als solche registriert, obwohl die entsprechende Anwendung bereits über einen längeren Zeitraum genutzt wird. Dadurch werden IDV-Anwendungen nicht fachgerecht überprüft und es fehlt etwa eine Übersicht hinsichtlich der Versionierung, da diese erst mit der Meldung einer IDV im Inventar in PlanningIT angefertigt wird.
- Die Versionierung einiger IDV-Anwendungen wird im Institut mithilfe einer Änderungs-historie in Word angelegt. Dabei besteht nur eine Anwendungsdatei über mehrere Versionen, die regelmäßig überschrieben wird. Die Versionierung ist hinsichtlich nachträglicher Änderungen nicht ausreichend geschützt. Zudem besteht durch die verschiedenen umgesetzten Versionierungsmethoden mithilfe von Word und PlanningIT keine zwingend konsistente Vorgehensweise im Institut, obwohl die Organisationsrichtlinien das entsprechende Vorgehen vorschreiben.

Beispielfeststellungen (Institut B - 4)

- Feststellung (F3): IDV-Anwendungen (AT 6 Tz.1 i. V. m. AT 7.2 Tzn. 2, 3 und 5 MaRisk)
  - Zusammenfassend ergeben sich hinsichtlich der IDV-Anwendungen folgende Schwächen:
    - Bei der IDV-Anwendung RTF-Rechnung weichen die Werte der Schutzbedarfsfeststellung zwischen Freigabedokument und IDV-Inventar zum Zeitpunkt der Freigabeerteilung voneinander ab.
    - Die Schutzbedarfe von den IDV-Anwendungen Kapitalplanung, Substanzwert und Risikoanalyse-Auslagerungen, die für das Institut eine maßgebliche Bedeutung haben, wurden zu niedrig eingestuft. Zudem wird die IDV Risikoanalyse-Auslagerungen aufgrund der zu niedrigen Schutzbedarfsermittlung hinsichtlich ihrer Tragweite für das Institut nicht angemessen überprüft.
    - Der Vorgang der Überführung einer IDV-Datei von der Entwicklungsumgebung in die Testumgebung wird nicht dokumentiert und ist somit nicht nachvollziehbar. Zudem haben Entwickler schreibende Zugriffe auf die Test- und Produktivumgebung. Weitere Maßnahmen zur Verhinderung von unberechtigten Änderungen an den IDV-Anwendungen in der Test- und Produktivumgebung sind nicht implementiert.
    - Die IDV-Anwendungen RTF-Rechnung und Kapitalplanung wurden bereits eingesetzt, ohne dass die An-wendungen freigegeben wurde.
    - Hinsichtlich der Testung der IDV-Anwendungen Substanzwert und Kapitalplanung besteht keine Dokumentation. Somit sind die Tests nicht nachvollziehbar. Zudem wurde die Durchführung der Tests erst bestätigt, als sich die Anwendungen bereits im Einsatz befunden haben.
    - …

Beispielfeststellungen (Institut B - 5)

- Feststellung (F3): IDV-Anwendungen (AT 6 Tz.1 i. V. m. AT 7.2 Tzn. 2, 3 und 5 MaRisk)
  - Zusammenfassend ergeben sich hinsichtlich der IDV-Anwendungen folgende Schwächen:
    - …
    - Die IDV-Anwendung Kapitalplanung wurde bis April 2022 im Fachbereich selbstständig verwaltet und nicht als IDV klassifiziert. Daher liegt für das Kapitalplanungstool keine Versionierung vor und die regelmäßige fachgerechte Überprüfung der IDV-Anwendung blieb aus.
    - Das Vorgehen hinsichtlich der Versionierung von IDV-Anwendungen ist inkonsistent. Zudem können innerhalb des Word-Dokuments, das für die Versionierung benutzt wird, nachträgliche Änderungen vor-genommen werden.
  - Die IDV-Anwendungen IDV sind angemessen zu dokumentieren und dabei muss insbesondere das Testvorgehen nachvollziehbar und plausibel sein. Die IDV-Anwendungen sind zudem in die Schutzbedarfsanalyse einzubeziehen und die Kritikalität der enthaltenen Daten in Bezug auf die Schutzziele angemessen abzuleiten. Vor Übergabe in den Linienprozess sind IDV-Anwendungen fachlich und technisch einer Abnahme zu unterziehen. Zudem ist bei der Abnahme bzw. den Tests sicherzustellen, dass der Entwickler keinen verändernden Zugriff auf die Test- und Abnahmeumgebung sowie die Produktivumgebung hat. Weiterhin ist gefordert, dass IDV-Anwendungen und deren Kritikalität rechtzeitig erkannt und klassifiziert respektive widerspruchsfrei versioniert wird. Somit sind die Anforderungen gemäß AT 6 Tz.1 i. V. m. AT 7.2 Tzn. 2, 3 und 5 MaRisk nicht erfüllt.

Beispielfeststellungen (Institut C - 1)

- Feststellung (F3): Informationsdatenverarbeitung (AT 6 Tz. 1 i. V. m. AT 7.2 Tzn. 1, 2 und 5 MaRisk):
  - Im Rahmen der Prüfungshandlung wurden im Institut hinsichtlich der IT-Themen die folgenden Schwächen festgestellt:
    - Die Institutsrechner besitzen trotz einer Clean Desk Policy keine technische Bildschirmsperre nach Zeitablauf.
    - Sämtliche IT-Schutzziele der Risikosteuerungs- und -überwachungsprozesse wurde lediglich entweder ein niedriger oder ein mittlerer Schutzbedarf zugeordnet. Zudem ist die IDV-Anwendung zur Festlegung der Schutzbedarfe als Datei ungeschützt und ohne Schutzvorrichtung veränderbar.
    - Innerhalb des Rezertifizierungsprozesses wird der Dateneigentümer nicht angemessen eingebunden.
    - Die abgenommene Version einer IDV-Anwendung ist nicht gegen nachträgliche Änderungen geschützt. Zudem ist das Vorgehen der Versionierung abhängig von dem für die IDV-Anwendung verwendeten Trägersystem (vgl. Tz. 198).
  - Aufgrund der oben genannten Schwächen sind die Anforderungen von AT 6 Tz. 1 i. V. m. AT 7.2 Tzn. 1, 2 und 5 MaRisk nicht vollumfänglich erfüllt.

Vielen Dank für IHRE Aufmerksamkeit!

Literaturempfehlung in eigener Sache ;-)

Strategiehandbuch Kreditwirtschaft
Herausgeber Henning Riediger, Autor u. a. Julian Mohr

- ISBN 978-3-95725-993-6 - 461 Seiten

„**MaRisk: Prüfungserkenntnisse aus Praxisfällen**“ –
Herausgeber: Henning Riediger

Inklusiver umfangreicher Fallstudien und Beispielfeststellungen zu Strategie, Informationsrisikomanagement, Informationssicherheitsmanagement, Auslagerungen, Benutzerberechtigung, Individuelle Datenverarbeitung usw.

- ISBN: 978-3-95725-164-0 - 482 Seiten