Praxisbericht zum Sollmaßnahmenkatalog

Westerwald Bank eG
Volks- und Raiffeisenbank

Vorstellung Referent

- Raphael Thewalt
- 28 Jahre alt
- Seit 08.2015 Mitarbeiter der Westerwald Bank eG
  - 10.2019-06.2021: Marketing & Digitalisierung mit Schwerpunkt Digitalisierung
  - 07.2021-12.2022: Betriebsorganisation Bereich Prozess- und Effizienzmanagement
  - Seit 01.2023: Beauftragter in den Bereichen Unternehmenssicherheit und Auslagerungsmanagement, sowie Schnittstellenperson zum ISB

Agenda

1. Ausgangssituation
2. Vorstellung Bankenindividueller SiMaKat (BASI)
3. Umsetzungsplan und wesentliche Meilensteine
4. Herausforderungen bei der Umsetzung
5. Ausblick DORA / BaSo

Ausgangssituation

Westerwald Bank eG
Volks- und Raiffeisenbank

Ausgangssituation

- BAIT Tz. 3.6:

  „ 3.6 Das Institut hat Anforderungen zu definieren, die zur Erreichung des jeweiligen Schutzbedarfs angemessen sind und diese in geeigneter Form zu dokumentieren (Sollmaßnahmenkatalog).“

  - Jedes Institut muss einen Sollmaßnahmenkatalog definieren, in dem die Anforderungen je Schutzziel und Schutzbedarfskategorie festgelegt sind.

- In Folge einer Prüfungsfeststellung in 2022 seit Anfang 2023 projektbegleitete Umsetzung des BASI

Vorstellung Bankenindividueller SiMaKat (BASI)

Westerwald Bank eG
Volks- und Raiffeisenbank

Bankenindividueller SiMaKat (BASI)

- In Zusammenarbeit von Genossenschaftlicher Finanzgruppe, Regionalverbänden und Primärbanken wurde der BASI als Arbeitshilfe entwickelt
  - bereitgestellt durch die AWADO
  - Definiert die gültigen Mindestanforderungen an das Informationssicherheitsmanagement nach ISO-Standard (ISO-Normenreihe 2700x)
- Grundlage zur Durchführung des Soll-/Ist-Vergleichs auf Schutzobjektebene ist durch vordefinierte Cluster und Sollmaßnahmenprofile gegeben

Bankenindividueller SiMaKat (BASI)

- Aufteilung der Sollmaßnahmen in 14 Cluster
  - Prinzipiell beinhaltet jedes Cluster die gleichen Maßnahmen
  - Cluster unterscheiden sich in der Relevanz verschiedener Maßnahmen

- Cluster 00 Organisation
  - Maßnahmen zielen hauptsächlich auf schriftlich fixierte Ordnung ab
  - Relevant für gesamten Informationsverbund

- Cluster 01-13
  - Servicespezifische Maßnahmen
  - Prinzipiell am Schutzobjekt zu beantworten

Clusterübersicht

00 Organisation	07 Ein- und Ausgabegeräte
01 Gebäude, Räume, Schränke	08 Netze, Netzwerkkomponenten
02 Wechseldatenträger	09 Arbeitsplatz
03 TK-Anlagen	10 IT-Cloud
04 IT-Sicherheitssysteme	11 Browseranwendungen
05 Server	12 Eigenentwicklungen IDV
06 SB-Systeme	13 IT-Anwendungen

Umsetzungsplan und wesentliche Meilensteine

Westerwald Bank eG
Volks- und Raiffeisenbank

Zeitlicher Ablauf

Westerwald Bank eG
Volks- und Raiffeisenbank

Wesentliche Meilensteine

- Definition des Informationsverbundes
  - Bereits erledigt
  - In ForumISM dokumentiert
- Clusteranpassung
  - Überprüfung auf Relevanz der einzelnen Cluster

- Soll-Soll-Abgleich mit Dienstleistern
  - Anfrage von Nachweisen zu
    - ISO/IEC 270XX
    - IT-Grundschutzkataloge des Bundesamts für Sicherheit in der Informationstechnik
    - Softwarebescheinigung nach IDW PS XXX
  - Falls keine der Nachweise erfolgen kann, ist eine individuelle Anfrage geplant

Wesentliche Meilensteine

- Bearbeitung Cluster 00 Organisation
  - Zentrale Beantwortung in ForumNSR
  - Viele Fragen können mit Verweis auf die schriftlich fixierte Ordnung (Arbeitsanweisungen) beantwortet werden

- Clusterzuordnung der einzelnen Schutzobjekte in ForumISM
  - Beantwortung der Servicespezifischen Maßnahmen am Schutzobjekt
  - Entgegen der Empfehlung ergibt unseres Erachtens eine zentrale Betrachtung der servicespezifischen Maßnahmen vorab Sinn
  - Bspw. „A.8.1.1-3 Inventarisierung der Werte – Informationsarten“
    - Antwort: „Dokumentation erfolgt am Schutzobjekt in ForumISM“
    - Maßnahme kann einmal zentral in ForumNSR beantwortet werden

Wesentliche Meilensteine

- Bearbeitung der Cluster 01-13 zentral in ForumNSR
  - Überprüfung ob Fragen zentral beantwortet werden können
    - Wenn ja:
      - Reifegrad vollständig umgesetzt
      - Bearbeitungsstand (ist): einheitliche Stellungnahme erfasst
    - Wenn nein:
      - Reifegrad teilweise umgesetzt
      - Bearbeitungsstand (ist): Bearbeitungshinweis bspw. „zu prüfen“

Wesentliche Meilensteine

- Erneute Betrachtung am Schutzobjekt in ForumISM
  - Gemeinsam mit Fachbereich und IT …
    - … überprüfen ob umgesetzte Maßnahmen übernommen werden können
    - … Teilweise umgesetzte Maßnahmen behandeln

- Bestätigung der Korrektheit und Vollständigkeit der umgesetzten Maßnahmen am Schutzobjekt
  - Erfolgt mittels Workflow durch den Fachbereich in ForumISM

Herausforderungen

Westerwald Bank eG
Volks- und Raiffeisenbank

Herausforderungen bei der Umsetzung des BASI

- Viele Fragen können vom Fachbereich nicht beantwortet werden, da technisches Know-how fehlt
  - Bspw. 11 Browseranwendung, A.12.4.1-1 Ereignisprotokollierung: *„Ereignisprotokolle, die Benutzertätigkeiten, Ausnahmen, Störungen und Informationssicherheitsvorfälle aufzeichnen, werden erzeugt, aufbewahrt und regelmäßig überprüft.“*
  - ➢ Einbindung IT und ggf. Nachfrage beim Dienstleister erforderlich

- Nadelöhr Bereich Informationssicherheit
  - Die Erfahrung hat gezeigt, dass der Bereich Informationssicherheit den Fachbereich bei der Umsetzung unterstützen muss
  - ➢ Langsames Voranschreiten, da die Aufgaben nicht parallel erledigt werden können

- Zentrale Bearbeitung vorab in ForumNSR sehr zeitintensiv (ca. 80 PT)

Ausblick auf DORA / BaSo

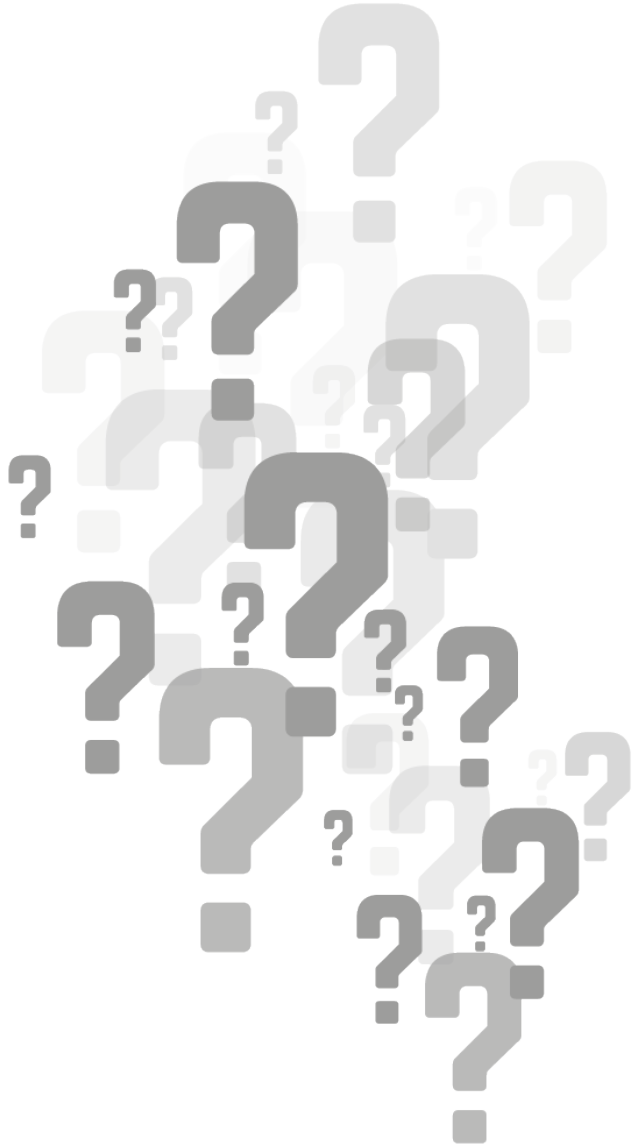
Westerwald Bank eG
Volks- und Raiffeisenbank

Ausblick DORA / BaSo

- Digital Operational Resilience Act
  - *„finanzsektorweite Regulierung für die Themen Cybersicherheit, IKT-Risiken und digitale operationale Resilienz“*
  - Durch die Europäische Union geschaffen
  - Tritt zum 17.01.2025 in Kraft

- Aus BASI wird BaSo
  - Wird durch ZAM eG zur Verfügung gestellt, regelmäßig überprüft und aktualisiert
  - Beinhaltet DORA-Anforderungen
  - Desweiteren heißt es seitens der ZAM eG: „(Dienstleister-) Informationen werden von der ZAM eG vorsortiert, veredelt, bewertet und in definierten Zeitabständen als Musterdaten direkt in die Systemwelt der Institute als Vorschlag eingespielt“

Ihre Fragen?



Westerwald Bank eG
Volks- und Raiffeisenbank

Westerwald Bank eG
Volks- und Raiffeisenbank