Weiterentwicklung Sollmaßnahmenkatalog
Überlegungen zur Umsetzung Banken SiMaKat in der Praxis

Agenda

1. Begriffsklärung

…damit wir alle das Gleiche verstehen….

Begriff	Definition
Sollmaßnahmenkatalog	• Regulatorische Anforderung, die institutseigenen Mindestanforderungen in einem Katalog zu formulieren • Innerhalb der BBBank nennen wir unsere aktuelle Version (2.0) „BBB SoMaKat“ (als Unterscheidung zur aufsichtsrechtlichen Anforderung)
Sicherheitsmaßnahmenkatalog (SiMaKat) (Atruvia)	• Durch den zentralen IT-Dienstleister Atruvia kommunizierter Sollmaßnahmenkatalog inklusiver individueller Soll-/Ist-Abgleiche pro Service/SiKo
Bankenindividueller Sicherheitsmaßnahmenkatalog aka BaSi (Awado)	• Von Awado zur Verfügung gestellte Vorlage inkl. Leitfaden

2. Aktueller Status Quo bei der BBBank

Entwicklung in den vergangenen Jahren

2018 - 2021

- Bereits seit 2018 einfacher Sollmaßnahmenkatalog im Einsatz:
  - ➢ technische Abbildung über Hilfstexte innerhalb ForumISM
  - ➢ Ermittlung Schutzniveau durch Anwendungsmanager
  - ➢ **Probleme:**
    - ✓ manueller Aufwand
    - ✓ keine einheitliche Dokumentation
    - ✓ Auditierung aufwendig

2021 – 2023

- Weiterentwicklung in 2021 auf Basis Revisionsfeststellung:
  - ➢ Entwicklung einer IDV mit 50+ Fragen inkl. einer automatischen Schutzniveauermittlung
  - ➢ Basis bildete Erfahrungsaustausch mit anderen Banken
  - ➢ **Probleme:**
    - ✓ Unterscheidung nach Schutzobjektarten schwierig
    - ✓ Dokumentation heterogen
    - ✓ Auditierung weiterhin aufwendig

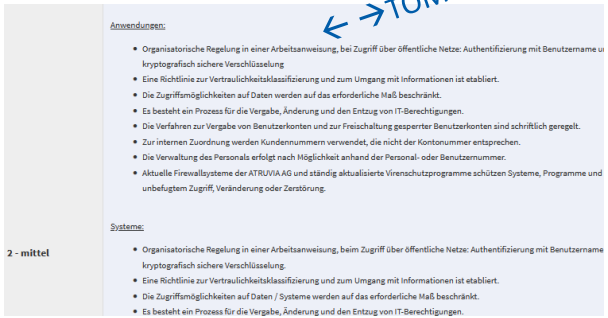
ab 2023

- BAIT, Probleme in der Praxis, Feedback Anwendungsmanager (AM):
  - → Version 3.0 notwendig
  - → Lösung?

2. Aktueller Status Quo bei der BBBank

Entwicklung in den vergangenen Jahren

Evolution unseres SoMaKat



Ergebnis	A3 C2 I2 N2
Verfügbarkeit (A)	3
Vertraulichkeit (C)	2
Integrität (I)	2
Authentizität (N)	2
Der Schutz vor Ausfällen ist über räumlich getrennte Standorte realisiert.	nein
Es wird gewährleistet, dass jeder Benutzer individuelle Passwörter benutzt. (und diese auch selbst auswählen kann)	ja

Lösung: BBB SoMaKat 3.0

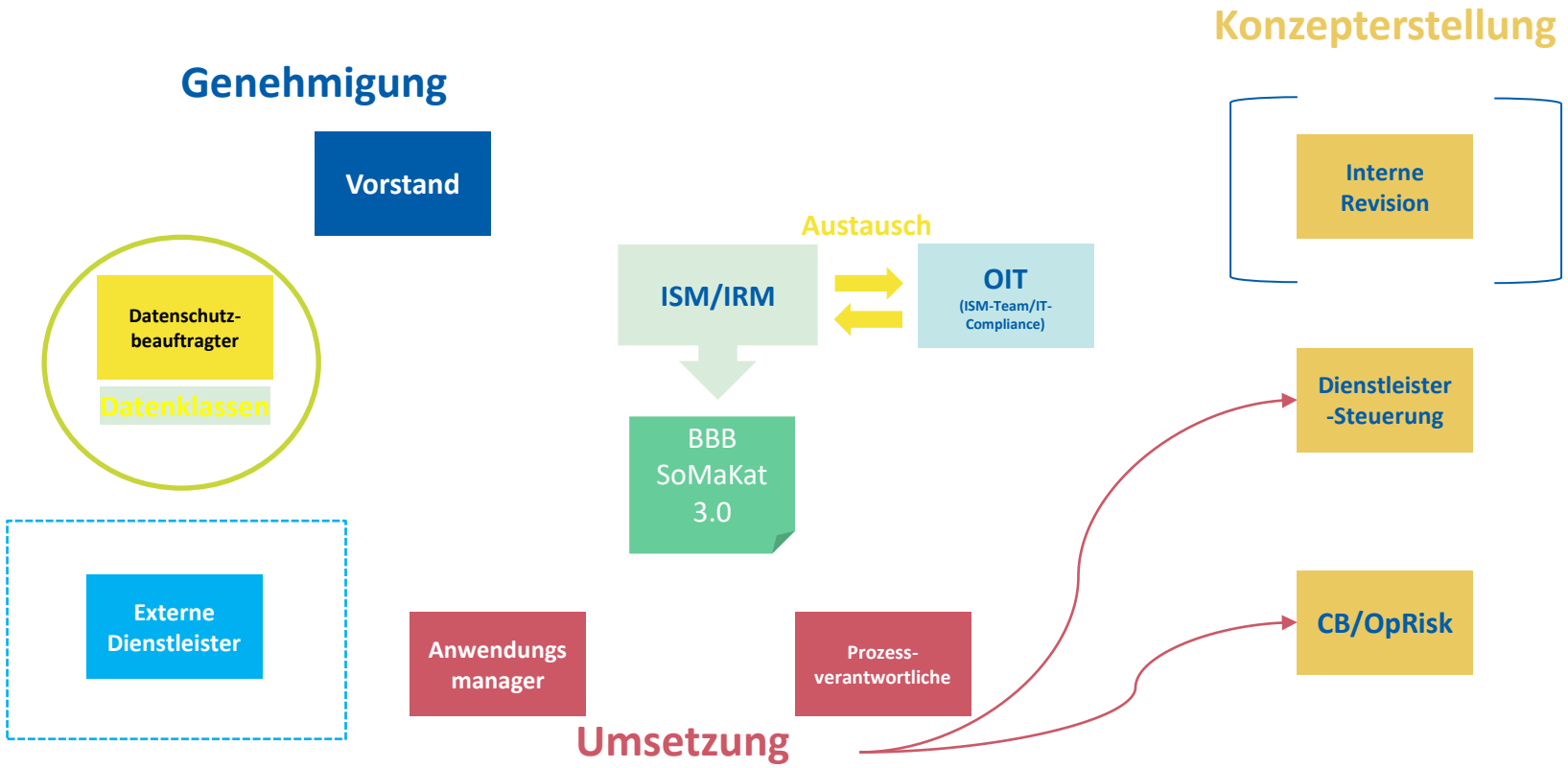
3. Standortbestimmung
Ausgangslage, Erfahrungen

- Welche guten Erfahrungen aus den bisherigen Lösungen?
  - Ausweis eines eigenen Schutzniveaus pro Schutzobjekt gut „greifbar“, aber …
  - Excel-Datei mit konkreten Maßnahmen wird als benutzerfreundlich empfunden
  - Dienstleister füllen unseren Sollmaßnahmenkatalog bisher qualifiziert aus (aber auch „nur“ 53 technische Soll-Maßnahmen)
  - Die Möglichkeit von „Vorlagen“ wird als wünschenswert angesehen
  - Innerhalb Prüfungen bislang kein negatives Feedback aber zuletzt Hinweis auf Weiterentwicklungsbedarf (bspw. Stichwort „Cluster“)

- Welches Optimierungspotenzial haben wir in den vergangen Jahren erkannt
  - … Ermittlung Schutzniveau nicht trivial (egal welcher unserer beiden SoMaKat) → am Ende in Teilen subjektiv
  - unsere technischen Soll-Maßnahmen sind nicht für alle Schutzobjekt-Arten gleichermaßen anwendbar
  - keine einfache Auswertungsmöglichkeit, welche Schutzobjekte mit einem aktuellen SoMaKat bearbeitet wurden
  - mehrere Gaps vorhanden → wie Risikoanalyse(n) aufbauen
  - Je konkreter desto besser

3. Standortbestimmung

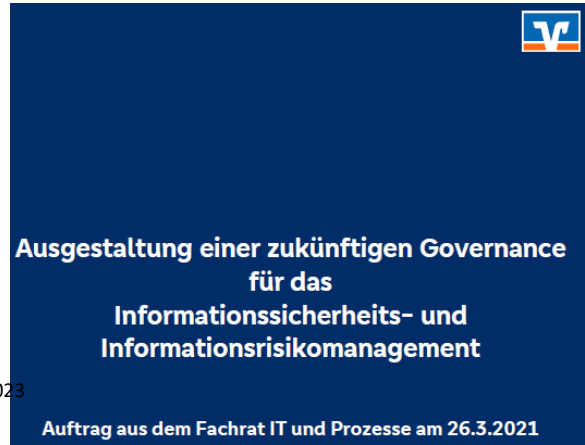
Wen müssen wir einbinden? Und wann?



4. Eine neue Hoffnung: BVR IT-Regulatorik Projekt

Ausgangssituation

- Auftrag aus dem BVR-Fachrat IT und Prozesse am 26.03.21, u.a. zur Reduktion von Komplexität, Vereinheitlichung methodisches Vorgehen, Berücksichtigung zukünftiger Herausforderungen (z.B. DORA)
- Leitfaden „Methodische Grundlagen zur IT-Regulatorik“ (LFI) vom BVR gemeinsam mit Genossenschaftsbanken, Prüfungsverbänden und weiteren Partnern in der genossenschaftlichen Finanzgruppe (GFG) herausgegeben
- Ablösung „SOIT Teil 1 – allgemeiner Teil“ und BAIT-Interpretation der GFG mit Veröffentlichung des LFI
- Projektmitwirkung der BBBank hinsichtlich Erarbeitung dieser methodischen Hilfestellung für Geno-Banken sowie zur Erreichung der Regulatorikkonformität
- BBBank hat **grosse Hoffnung** auf inhaltliche Zusammenarbeit gesetzt, u.a. auch was konkrete Anforderungen / Umgang an den Sollmaßnahmenkatalog betrifft
- **Wurde diese erfüllt…?**



4. Eine neue Hoffnung: BVR IT-Regulatorik Projekt

Rahmendaten zum LFI resp. zum SoMaKat

- 31.03.23: Veröffentlichung LFI „Methodische Grundlagen zur IT-Regulatorik“ – Umsetzung der MaRisk / BAIT im Zusammenspiel mit gängigen Standards

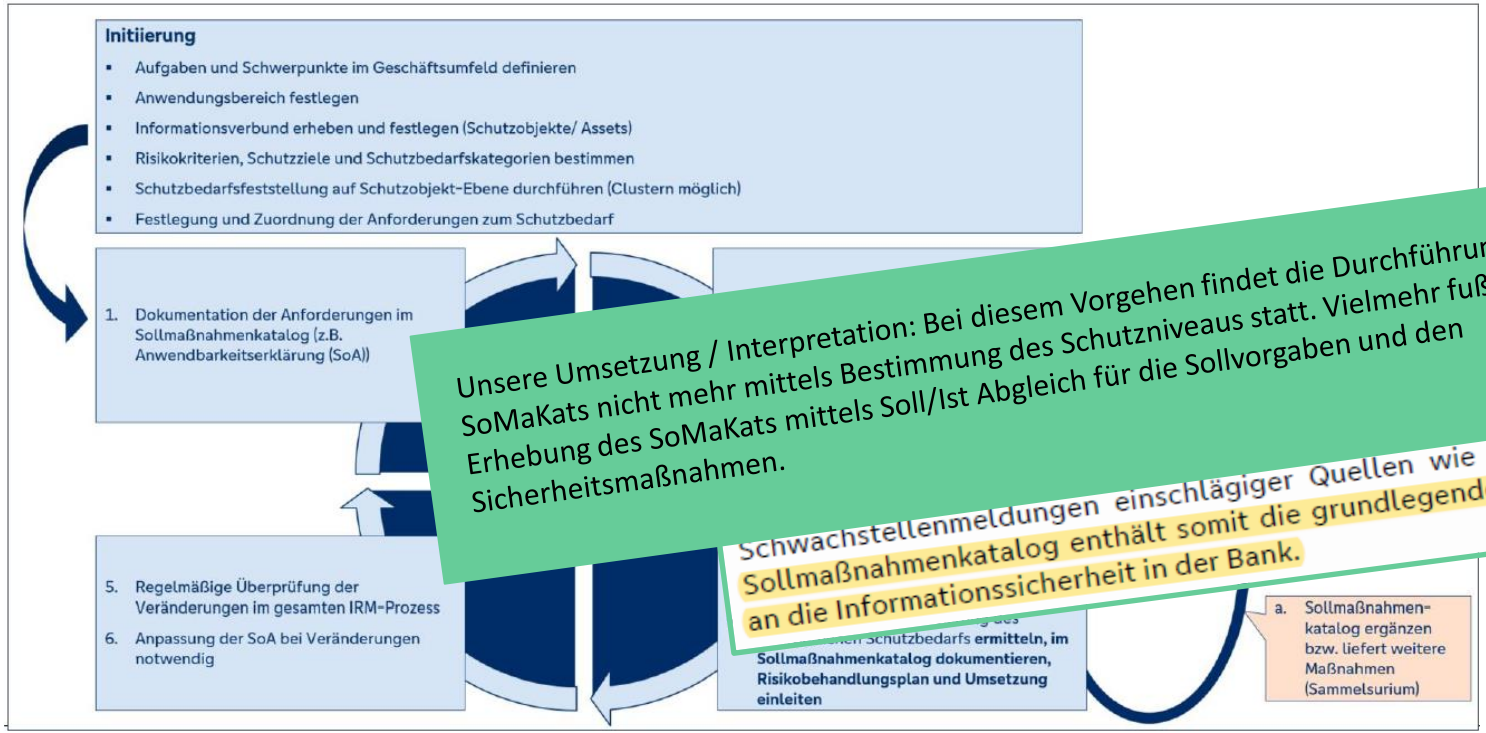
> werden. Die MaRisk und die BAIT sind prinzipienorientiert ausgestaltet. Konkrete Vorgaben wie bestimmte Prozesse auszugestalten sind oder wie z.B. eine Methodik zur Ermittlung des Schutzbedarfes der einzelnen Bestandteile des Informationsverbunds oder zur Erstellung eines Sollmaßnahmenkatalogs, geben die regulatorischen Anforderungen nicht vor, so dass eine individuelle Interpretation und Anlehnung an die Rahmenbedingungen der Bank möglich ist.

- Vorgaben an das „**was**“, nicht an das „wie“ (≠ konkreter Bestandteil BAIT oder ISO 27001), Konsequenz: → **Banken sind bzgl. Methodik zur Ausgestaltung des SoMaKats frei**

> Die Banken können hierzu bei der Ausgestaltung und zur Orientierung auf die **Referenzmaßnahmen aus dem Anhang A der ISO/IEC 27001:2017** sowie ergänzend der ISO/IEC 27002:2017 zurückgreifen. In diesem Zusammenhang ist hervorzuheben, dass die ISO 27002:2017 ausschließlich einen Katalog an **Maßnahmenempfehlungen** zur Verfügung stellt, um die aus Anhang A der 27001:2017 dargestellten Anforderungen/ Maßnahmenziele zu erreichen. Eine Verpflichtung zur vollständigen

4. Eine neue Hoffnung: BVR IT-Regulatorik Projekt

Rahmendaten zum LFI resp. zum SoMaKat



Unsere Umsetzung / Interpretation: Bei diesem Vorgehen findet die Durchführung des SoMaKats nicht mehr mittels Bestimmung des Schutzniveaus statt. Vielmehr fußt die Erhebung des SoMaKats mittels Soll/Ist Abgleich für die Sollvorgaben und den Sicherheitsmaßnahmen.

Schwachstellenmeldungen einschlägiger Quellen wie z.B. des BSI. Der Sollmaßnahmenkatalog enthält somit die grundlegenden Anforderungen an die Informationssicherheit in der Bank.

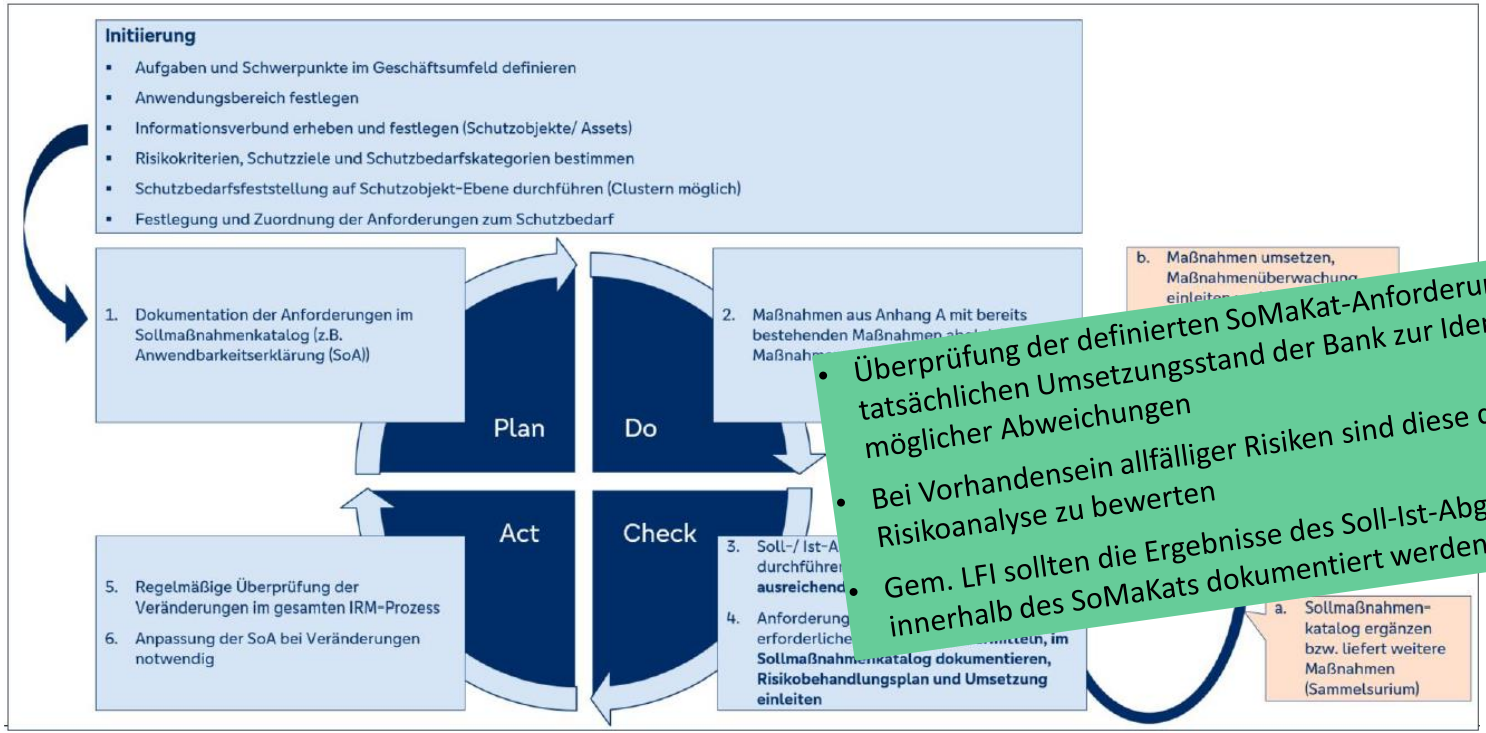
- Basierend auf Ergebnissen der Schutzbedarfsermittlung erfolgt…
- … die Festlegung der definierten Anforderungen (anhand des SoMaKats), z.B. mittels Rückgriff auf die Controls aus der SoA

…ch Empfehlung:

Quelle: LFI: Herleitung der Anforderungen zum Schutzbedarf gemäß BAIT in Anlehnung an ISO/IEC 27001:2017

4. Eine neue Hoffnung: BVR IT-Regulatorik Projekt

Rahmendaten zum LFI resp. zum SoMaKat



- Überprüfung der definierten SoMaKat-Anforderungen auf tatsächlichen Umsetzungsstand der Bank zur Identifikation möglicher Abweichungen
- Bei Vorhandensein allfälliger Risiken sind diese dann mit einer Risikoanalyse zu bewerten
- Gem. LFI sollten die Ergebnisse des Soll-Ist-Abgleichs innerhalb des SoMaKats dokumentiert werden

Quelle: LFI: Herleitung der Anforderungen zum Schutzbedarf gemäß BAIT in Anlehnung an ISO/IEC 27001:2017

4. Eine neue Hoffnung: BVR IT-Regulatorik Projekt

… Erkenntnisse… und wurden unsere Erwartungen erfüllt?

- Für die in der Erstveröffentlichung des LFI im März 2023 **noch nicht umgesetzten** aber **perspektivisch zu berücksichtigenden Inputs** wurde ein Dokument erstellt („Verbesserungsvorschlägen zum Leitfaden für die Nachfolgeorganisation“)
- In diesem Dokument sind auch konkrete Punkte bzgl. Anforderungen an den **SoMaKat** enthalten, sowohl von der BBBank als auch von anderen Mitwirkenden
- Wie die Herleitung bereits aufgezeigt hat, wird den Banken – zumindest aktuell – **keine umfängliche Unterstützung** bzgl. des „**wie**“ zur Verfügung gestellt. Inwieweit sich das perspektivisch – z.B. mit einem LFI v2.0 vertieft, ist abzuwarten
- Zwischenzeitlich entwickeln wir uns derweil weiter in der praktischen Umsetzung eines individualisierten - sich ggf. doch gar nicht mal so von anderen Banken im Vorgehen unterscheidenden Ansatz - an eine **effiziente und effektive Umsetzung des SoMaKats**

5. Anforderungen BBBank an neue Lösung

Unsere optimale Rezeptur für einen gelungenen SoMaKat

MUSS

- Eindeutige Maßnahmen
- Unterscheidung nach Clustern
- Einfache Anwendbarkeit
- Vorlagen-Charakter
- Auditierbarkeit (mind. Auswertung aktueller SoMaKat)
- ISO27001-Charakter

KANN

- Umsetzung innerhalb ForumISM
- Wenig Aufwand (bei allen Beteiligten)
- Erweiterte Auditierbarkeit
- Arbeiten mit Standard-/Vorlagen-Risiken

Sonstige Gedanken

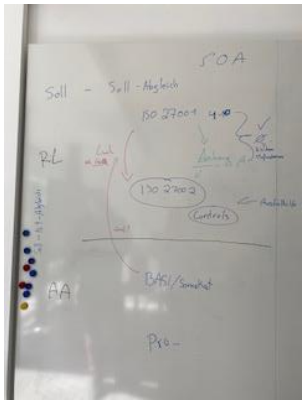
- Akzeptanz der Stakeholder antizipieren
- Kompatibilität mit Entwicklungen im Verbund
- Schnellschuss vs. „zu spät“

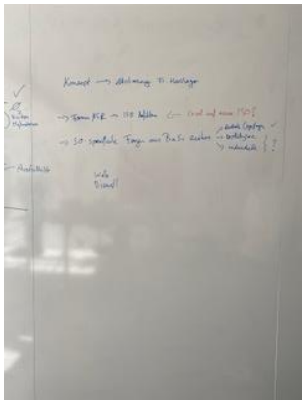
6. Lösungsfindung BBBank

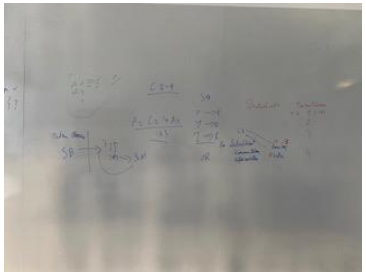
Die Nadel im Heuhaufen?

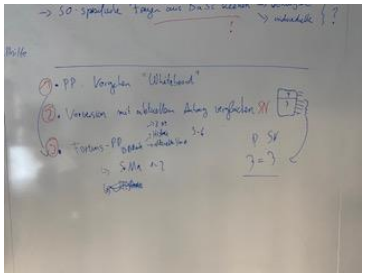
6. Lösungsfindung BBBank

Am Anfang herrschte Chaos…









Teamwork

Unsere 3 Ws zur Lösungsfindung:

- Workshops
- Whiteboards
- **Wir** schaffen das

6. Lösungsfindung BBBank

Banken SiMaKat – das wäre doch was?!

Kompatibilität Verfahren ZAM?

Pro
- Cluster
- vorgegebene Maßnahme
- Vorbelegung in ForumNSR möglich
- Auswertung möglich

Contra
- hoher initialer Aufwand
- Servicespezifisch?

BaSi (ForumNSR)

BBB SoMaKat auf Basis BaSi (eigenes Sollmaßnahmen-profil)

Pro
- Siehe links

Contra
- **Sehr** hoher initialer Aufwand
- Hoher Pflegeaufwand

Erkenntnisse in den Workshops

Pro
- Schneller Wechsel möglich
- Bekanntes Verfahren
- Leicht im Austausch mit DL

Contra
- Keine Auswertung!
- Nicht auf Anwendungsart

BBB SoMaKat Update (Excel)

BBB SoMaKat Update (Sollmaßnahmen-profil)

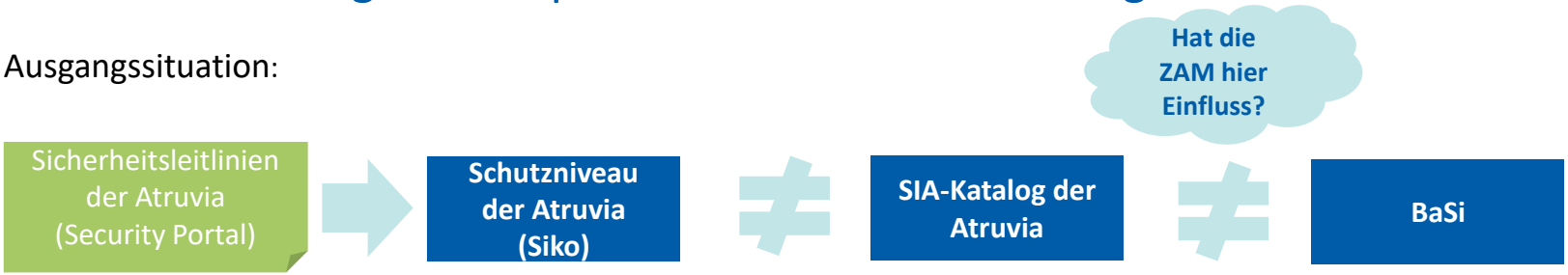
Pro
- Schneller Wechsel
- Auswertung möglich
- Auf Bekanntem aufgesetzt

Contra
- Hohe Eigenleistung notwendig
- Cluster?
- Unterschied zu „oben“

7. Praktische Umsetzung in BBBank

Unser Umsetzung am Beispiel von Atruvia-Anwendungen

Ausgangssituation:

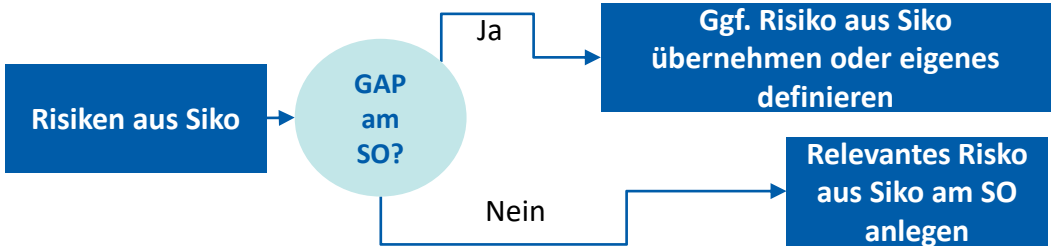


Umsetzung:

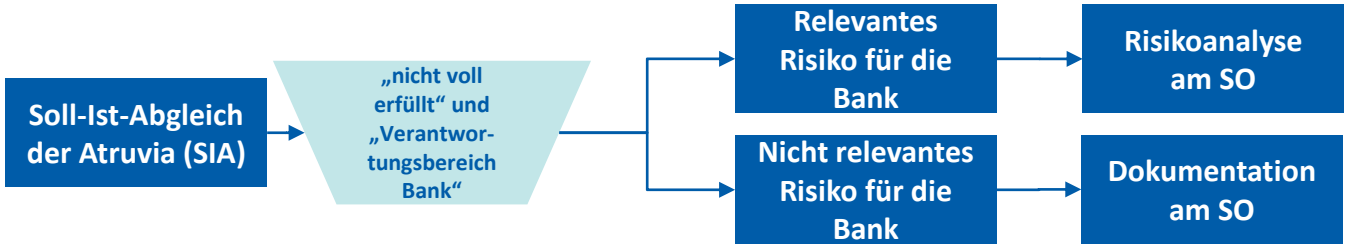
7. Praktische Umsetzung in BBBank

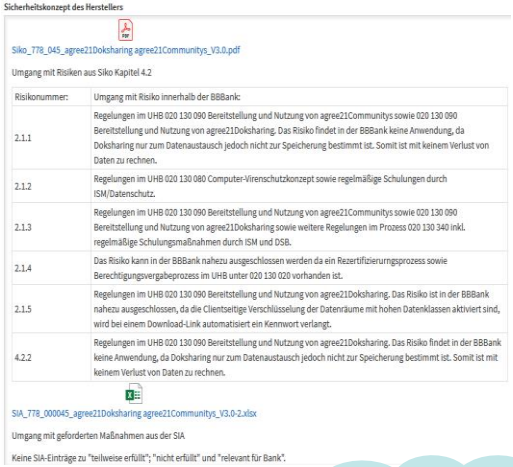
Unser Umsetzung am Beispiel von Atruvia-Anwendungen

Umsetzung der GAPs / Risiken aus den Atruvia Sikos:



Umsetzung der offenen Maßnahmen aus dem SIA:




Sicherheitskonzept des Herstellers

Siko_778_045_agree21Doksharing agree21Communitys_V3.0.pdf

Umgang mit Risiken aus Siko Kapitel 4.2

Risikonummer:	Umgang mit Risiko innerhalb der BBBank:
2.1.1	Regelungen im UHB 020 130 090 Bereitstellung und Nutzung von agree21Communitys sowie 020 130 090 Bereitstellung und Nutzung von agree21Doksharing. Das Risiko findet in der BBBank keine Anwendung, da Doksharing nur zum Datenaustausch jedoch nicht zur Speicherung bestimmt ist. Somit ist mit keinem Verlust von Daten zu rechnen.
2.1.2	Regelungen im UHB 020 130 080 Computer-Virenschutzkonzept sowie regelmäßige Schulungen durch ISM/Datenschutz.
2.1.3	Regelungen im UHB 020 130 090 Bereitstellung und Nutzung von agree21Communitys sowie 020 130 090 Bereitstellung und Nutzung von agree21Doksharing sowie weitere Regelungen im Prozess 020 130 340 inkl. regelmäßige Schulungsmaßnahmen durch ISM und DSB.
2.1.4	Das Risiko kann in der BBBank nahezu ausgeschlossen werden da ein Rezertifizierungsprozess sowie Berechtigungsvergabeprozess im UHB unter 020 130 020 vorhanden ist.
2.1.5	Regelungen im UHB 020 130 090 Bereitstellung und Nutzung von agree21Doksharing. Das Risiko ist in der BBBank nahezu ausgeschlossen, da die Clientseitige Verschlüsselung der Datenräume mit hohen Datenklassen aktiviert sind, wird bei einem Download-Link automatisiert ein Kennwort verlangt.
4.2.2	Regelungen im UHB 020 130 090 Bereitstellung und Nutzung von agree21Doksharing. Das Risiko findet in der BBBank keine Anwendung, da Doksharing nur zum Datenaustausch jedoch nicht zur Speicherung bestimmt ist. Somit ist mit keinem Verlust von Daten zu rechnen.

SIA_778_000045_agree21Doksharing agree21Communitys_V3.0-2.xlsx

Umgang mit geforderten Maßnahmen aus der SIA

Keine SIA-Einträge zu "teilweise erfüllt"; "nicht erfüllt" und "relevant für Bank".

Egal wie.. Der Umgang mit dem Risiko ist zu dokumentieren

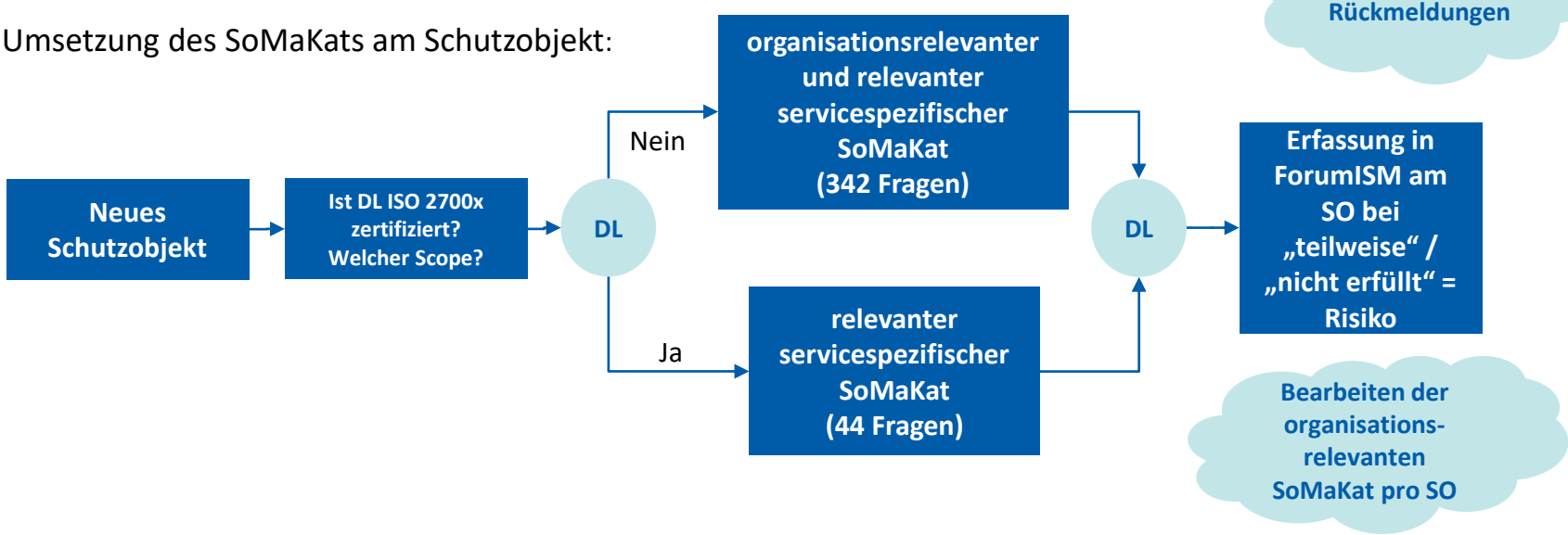
7. Praktische Umsetzung in BBBank

Unser Umsetzung am Beispiel von Browser-Anwendungen

Umsetzung des Schutzniveaus:

Import / Export Funktion der DL Rückmeldungen

Umsetzung des SoMaKats am Schutzobjekt:



8. ZeitPLANUNG

Aufgabenpakete, Timeline

2022 — Zeitplan >= 18 Monate — 2024

ToDos:	Entwicklung Konzept	Konzept challengen	Genehmigung Vorstand	Kommunikation/Schulung	Umsetzung
	ISM/OIT	Controlling Op/Risk Revision Pilotgruppe PV/AM	ISM	ISM	AM: im Rahmen der nächsten Wiedervorlage

Befüllung Forum (durch ISM/OIT)

Aufwände:				
• Workshops • Eigenstudium • Probeweise Erfassungen	• Review durch beteiligte Stellen • Diskussion • Mehrere Durchläufe einplanen	• Genehmigung des Konzepts	• Schulungsvideos • Unterlagen • Digitale Sprechstunden	• Erfassung in ForumISM • Kontaktaufnahme DL

9. Lessons learned

- Ideen sammeln ist wichtig, aber irgendwann muss man auch „losgehen“
- Wir haben noch einiges von uns, aber eine gut überlegte Basis ist ein wichtiges Fundament

BBB SoMaKat aktuell

BBB SoMaKat 3.0

- Bankinterner Austausch ist sehr wertvoll, gleichzeitig aber immer das individuelle Verständnis gegenprüfen
- Kein einmaliges Projekt, sondern andauernde Aufgabe
- Wir sind nicht alleine mit der Fragestellung → profitieren vom Schwarmwissen

Vielen Dank
für Ihre Aufmerksamkeit