FORUM Anwendertagung 2023

Überwachungshandlungen des ISB

Matthias Weskamp

// Abteilungsleiter Beauftragtenwesen

Bank für Kirche und Caritas eG

Die Bank von Mensch zu Mensch

Informationen zur Person

Name: Matthias Weskamp

Funktion: IS- und Notfallbeauftragter
MaRisk-Compliance-Beauftragter
Abteilungsleiter Beauftragtenwesen

Beauftragtenwesen

- Informationssicherheitsmanagement
- Notfallmanagement
- Auslagerungsmanagement
- MaRisk-Compliance

Bank für Kirche und Caritas eG

- Gründungsjahr: 1972
- Sitz: Paderborn
- Bilanzsumme: 5.344 Mio. €
- Kundengelder: 4.081 Mio. €
- Mitglieder: 1.315
- Mitarbeitende: 149

Stand: 25.01.2023

Agenda

1 // IT-Governance

2 // Informationsrisikomanagement

3 // Informationssicherheitsmanagement

4 // Identitäts- und Rechtemanagement

5 // Auslagerungen & sonstiger Fremdbezug von IT-Dienstleistungen

6 // dann wäre da noch ...

Bank für Kirche und Caritas eG

1 IT-Governance

Bank für Kirche und Caritas eG

2.5.	Zur Steuerung der für den Betrieb und die Weiterentwicklung der IT-Systeme zuständigen Bereiche durch die Geschäftsleitung sind angemessene quantitative oder qualitative Kriterien durch diese festzulegen. Die Einhaltung der Kriterien ist zu überwachen.	Bei der Festlegung der Kriterien können z. B. die Qualität der Leistungserbringung, die Verfügbarkeit, Wartbarkeit, Anpassbarkeit an neue Anforderungen, Sicherheit der IT-Systeme oder der dazugehörigen IT-Prozesse sowie deren Kosten berücksichtigt werden.

- Aufgabe des ISB?
- BKC folgt der BVR-Empfehlung aus der Arbeitshilfe zum ICT-Fragebogen
- Überwachung quartalweise im ISM-Ausschuss anhand des Realisierungsplans zur Teilstrategie IT
- Dokumentation im Protokoll zur Ausschuss-Sitzung sowie im Rahmen der Berichterstattung zur Zielerreichung der strategischen Ziele an den Vorstand

Bank für Kirche und Caritas eG

2 Informationsrisiko-management

Bank für Kirche und Caritas eG

Schutzbedarfsfeststellungen

3.5. Die Schutzbedarfsfeststellung sowie die zugehörige Dokumentation sind durch das Informationsrisikomanagement zu überprüfen.

- Aufgabe des ISB?
- in der BKC wird diese Aufgabe durch den ISB übernommen
- quartalsweise Überwachung, ob der Schutzbedarf eines Prozesses zu den verknüpften Datenklassen (Maximalprinzip) und dem Ergebnis der Business Impact Analyse (BIA) passt
- sofern möglich auch Plausibilitätsbeurteilung der BIA
- Aussage der Aufsicht: stichprobenartige Überprüfung nicht ausreichend
- Nutzung ForumISM-Auswertungen „Überprüfung Schutzbedarf Geschäftsprozesse“ und Überprüfung Schutzbedarf Datenklassen“

Bank für Kirche und Caritas eG

Auswertung Überprüfung Schutzbedarf (hier: Prozesse)

Überprüfung Schutzbedarf Geschäftsprozesse

Extras

Überprüfungs-Workflow erstellen ...

Bezeichnung	Schutzbedarf	Business Impact	Letzte Bearbeitung	Letzte Freigabe	Letzte Überprüfung
Kundenprozesse					
Privater und gewerblicher Finanzierungsbedarf					
Kreditgewährung KCE	A2:2 C3 I3 N3	nicht zeitkritisch	03.09.2021	19.08.2022	1 am 09.06.2022
Kreditgewährung Privat	A2:2 C3 I3 N3	nicht zeitkritisch	26.11.2021	30.05.2022	1 am 09.06.2022
Intensivbetreuung und Problemkreditbearbeitung	A1:1 C3 I3 N3	nicht zeitkritisch	01.06.2021	18.11.2022	1 am 09.06.2022
Behandlung von Problemkrediten	A1:1 C3 I3 N3	nicht zeitkritisch	09.06.2022	18.11.2022	1 am 09.06.2022
Risikovorsorge	A1:1 C3 I3 N3	nicht zeitkritisch	09.06.2022	18.11.2022	1 am 09.06.2022
Risikofrüherkennung	A1:1 C3 I3 N3	nicht zeitkritisch	15.11.2021	22.12.2022	1 am 09.06.2022
Risikoklassifizierung	A1:1 C3 I3 N3	nicht zeitkritisch	15.11.2021	08.07.2022	1 am 09.06.2022
Kreditvermittlung	A1:1 C3 I3 N3	nicht zeitkritisch	09.06.2022	20.12.2022	1 am 09.06.2022
Geld- und Kapitalanlage					
Einlage					
Einlagengeschäft	A1:1 C3 I3 N3	nicht zeitkritisch	06.07.2021	09.08.2022	1 am 09.06.2022
Edelmetalle/Münzen	A1:1 C3 I3 N3	nicht zeitkritisch	01.10.2021	06.10.2022	1 am 09.06.2022

Bank für Kirche und Caritas eG

risikoreduzierende Maßnahmen

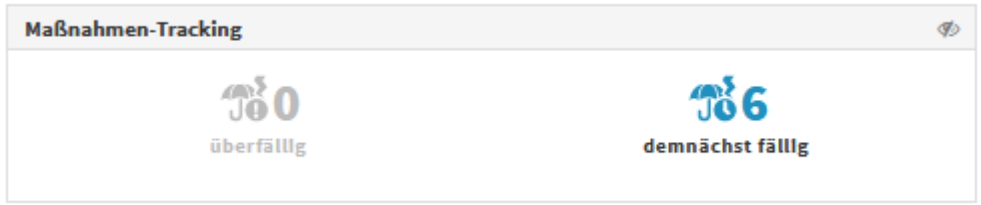
3.8.	Sonstige risikoreduzierende Maßnahmen aufgrund unvollständig umgesetzter Sollmaßnahmen sind wirksam zu koordinieren, zu dokumentieren, zu überwachen und zu steuern.

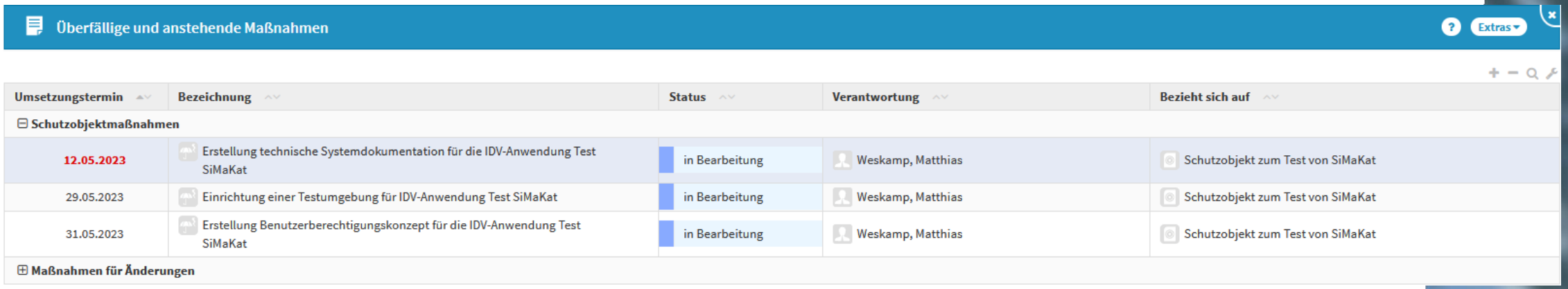
- Überwachungshandlung gewinnt mit Voranschreiten des geforderten Abgleich der Sollmaßnahmen mit den jeweils wirksam umgesetzten Maßnahmen an Bedeutung
- sofern Sollmaßnahmen (noch) nicht umgesetzt sind, werden risikoreduzierende Maßnahmen ergriffen und am Risiko in ForumISM inkl. Umsetzungstermin dokumentiert
- Überwachung mit Hilfe des Maßnahmen-Trackings in ForumISM (Risikomanagement - Rubrik Schutzobjektmaßnahmen)

Bank für Kirche und Caritas eG

risikoreduzierende Maßnahmen

- Dokumentation in ForumISM unter den Überwachungsaktivitäten
- Aufnahme in die ISB-Berichterstattung (regelmäßig bzw. ggf. auch anlassbezogen)





Umsetzungstermin	Bezeichnung	Status	Verantwortung	Bezieht sich auf
Schutzobjektmaßnahmen				
12.05.2023	Erstellung technische Systemdokumentation für die IDV-Anwendung Test SiMaKat	in Bearbeitung	Weskamp, Matthias	Schutzobjekt zum Test von SiMaKat
29.05.2023	Einrichtung einer Testumgebung für IDV-Anwendung Test SiMaKat	in Bearbeitung	Weskamp, Matthias	Schutzobjekt zum Test von SiMaKat
31.05.2023	Erstellung Benutzerberechtigungskonzept für die IDV-Anwendung Test SiMaKat	in Bearbeitung	Weskamp, Matthias	Schutzobjekt zum Test von SiMaKat
Maßnahmen für Änderungen				

Bank für Kirche und Caritas eG

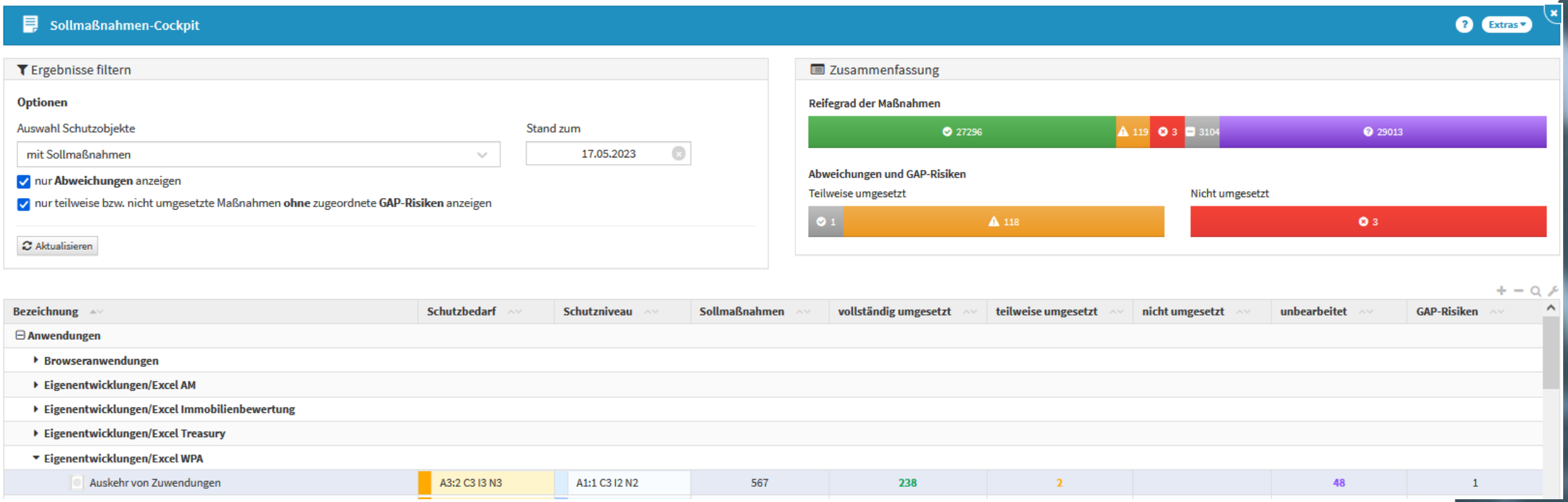
Risikoanalyse

3.9. Das Informationsrisikomanagement hat die Risikoanalyse zu koordinieren und zu überwachen sowie deren Ergebnisse in den Prozess des Managements der operationellen Risiken zu überführen. Die Behandlung der Risiken ist kompetenzgerecht zu genehmigen.

- Überwachung monatlich anhand der Übersicht „Sollmaßnahmencockpit“ und der Auswertung „Überprüfung Risikoanalyse“
  - wurde zu jeder nicht umgesetzten Sollmaßnahme ein Risiko erfasst?
  - Überwachung auf Plausibilität
  - Begründungen vorhanden?
- Dokumentation mit Verweis auf Workflow in ForumISM unter „Überwachungsaktivitäten“

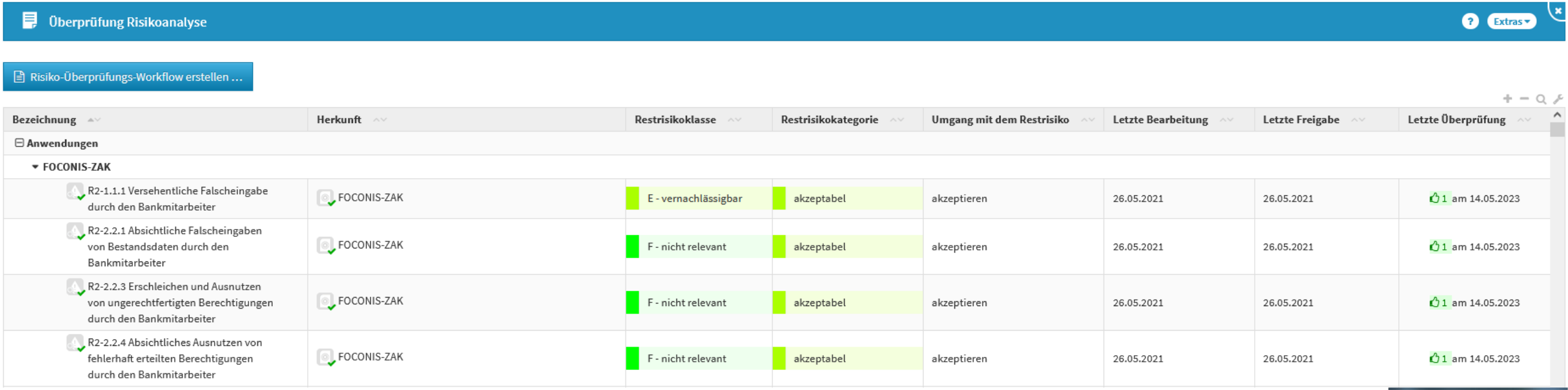
Bank für Kirche und Caritas eG

Auswertung Sollmaßnahmen-Cockpit



Bank für Kirche und Caritas eG

Risikoanalyse



Bezeichnung	Herkunft	Restrisikoklasse	Restrisikokategorie	Umgang mit dem Restrisiko	Letzte Bearbeitung	Letzte Freigabe	Letzte Überprüfung
Anwendungen							
FOCONIS-ZAK							
R2-1.1.1 Versehentliche Falscheingabe durch den Bankmitarbeiter	FOCONIS-ZAK	E - vernachlässigbar	akzeptabel	akzeptieren	26.05.2021	26.05.2021	1 am 14.05.2023
R2-2.2.1 Absichtliche Falscheingaben von Bestandsdaten durch den Bankmitarbeiter	FOCONIS-ZAK	F - nicht relevant	akzeptabel	akzeptieren	26.05.2021	26.05.2021	1 am 14.05.2023
R2-2.2.3 Erschleichen und Ausnutzen von ungerechtfertigten Berechtigungen durch den Bankmitarbeiter	FOCONIS-ZAK	F - nicht relevant	akzeptabel	akzeptieren	26.05.2021	26.05.2021	1 am 14.05.2023
R2-2.2.4 Absichtliches Ausnutzen von fehlerhaft erteilten Berechtigungen durch den Bankmitarbeiter	FOCONIS-ZAK	F - nicht relevant	akzeptabel	akzeptieren	26.05.2021	26.05.2021	1 am 14.05.2023

- Fokus auf neu erfasste und geänderte Risikoanalysen

Bank für Kirche und Caritas eG

3 Informationssicherheits-management

Bank für Kirche und Caritas eG

Aufgaben des ISB

4.4.	Die Geschäftsleitung hat die Funktion des Informationssicherheitsbeauftragten einzurichten. Diese Funktion umfasst die Verantwortung für die Wahrnehmung aller Belange der Informationssicherheit innerhalb des Instituts und gegenüber Dritten. Sie stellt sicher, dass die in der IT-Strategie, der Informationssicherheitsleitlinie und den Informationssicherheitsrichtlinien des Instituts festgelegten Ziele und Maßnahmen hinsichtlich der Informationssicherheit sowohl intern als auch gegenüber Dritten transparent gemacht und deren Einhaltung regelmäßig sowie anlassbezogen überprüft und überwacht werden.	Die Funktion des Informationssicherheitsbeauftragten umfasst insbesondere die nachfolgenden Aufgaben: ▪ die Geschäftsleitung beim Festlegen und Anpassen der Informationssicherheitsleitlinie zu unterstützen und in allen Fragen der Informationssicherheit zu beraten; dies umfasst auch Hilfestellungen bei der Lösung von Zielkonflikten (z. B. Wirtschaftlichkeit kontra Informationssicherheit) ▪ Erstellung von Informationssicherheitsrichtlinien und ggf. weiteren einschlägigen Regelungen sowie die Kontrolle ihrer Einhaltung ▪ den Informationssicherheitsprozess im Institut zu steuern und zu koordinieren sowie diesen gegenüber IT-Dienstleistern zu überwachen und bei allen damit zusammenhängenden Aufgaben mitzuwirken ▪ die Beteiligung bei der Erstellung und Fortschreibung des Notfallkonzepts bzgl. der Informationssicherheitsbelange ▪ die Realisierung von Informationssicherheitsmaßnahmen zu initiieren und zu überwachen ▪ Überwachung und Hinwirkung auf Einhaltung der Informationssicherheit bei Projekten und Beschaffungen ▪ als Ansprechpartner für Fragen der Informationssicherheit innerhalb des Instituts und für Dritte bereitzustehen ▪ Informationssicherheitsvorfälle zu untersuchen und an die Geschäftsleitung zu berichten ▪ Sensibilisierungs- und Schulungsmaßnahmen zur Informationssicherheit zu initiieren und zu koordinieren. Der Informationssicherheitsbeauftragte kann durch ein Informationssicherheitsmanagement-Team unterstützt werden.

Bank für Kirche und Caritas eG

Informationssicherheitsrichtlinien

- bislang Konzentration auf die Überwachung der Einhaltung von Arbeitsanweisungen
    - bspw. Bildschirmsperre
    - Chip-Aus- bzw. Rückgabe
    - Vereinbarung Bankgeheimnis & Datenschutz mit neuen Mitarbeitern
    - Überlassungsvereinbarung mobile Endgeräte
    - Kompetenzvergabeprozess

- mit Erstellung einer Vielzahl von themenspezifischen Sicherheitsrichtlinien nun zunächst Konzentration darauf, ob sich deren Vorgaben in den entsprechenden Arbeitsanweisungen wiederfinden (GAP-Analyse)

- Dokumentation unter den Überwachungsaktivitäten in ForumISM

930.4461.004-Sicherheitsrichtlinie Netzwerk
930.4461.005-Sicherheitsrichtlinie Kryptografie
930.4461.006-Sicherheitsrichtlinie physische Sicherheit
930.4461.007-Sicherheitsrichtlinie Passwort
930.4461.008-Klassifizierung und Handhabung von Informationen
930.4461.008-Sicherheitsrichtlinie Personal
930.4461.009 Sicherheitsrichtlinie Identitäts- und Rechtemanagement
930.4461.010 Sicherheitsrichtlinie Assetmanagement
930.4461.011 Sicherheitsrichtlinie Patchmanagement
930.4461.012-Entsorgung Informationsträger
930.4461.013-Sicherheitsrichtlinie Protokollierung
930.4461.014-Sicherheitsrichtlinie Entwicklung
930.4461.015-Sicherheitsrichtlinie Auslagerungsmanagement
930.4461.016-Sicherheitsrichtlinie Notfallmanagement
930.4461.017-Sicherheitsrichtlinie Fernwartung
930.4461.018-Allgemeine Sicherheitsrichtlinie
930.4461.019-Sicherheitsrichtlinie mobile Endgeräte
930.4461.020-Sicherheitsrichtlinie Arbeitsplatz

Bank für Kirche und Caritas eG

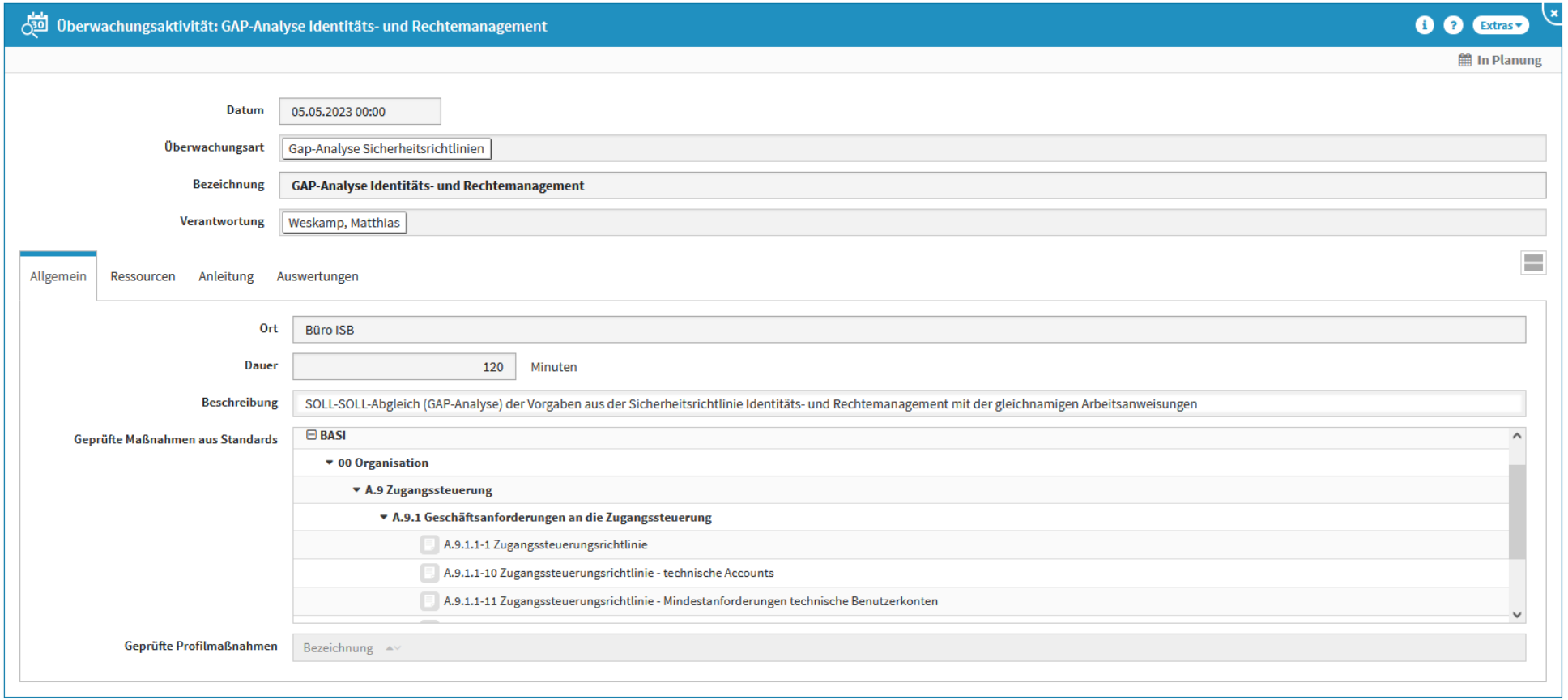
Exkurs: Auditierung

4.8.	Das Institut hat eine Richtlinie über das Testen und Überprüfen der Maßnahmen zum Schutz der Informationssicherheit einzuführen und diese regelmäßig und anlassbezogen zu überprüfen und bei Bedarf anzupassen.	Die Richtlinie berücksichtigt u. a.: ▪ die allgemeine Bedrohungslage ▪ die individuelle Risikosituation des Instituts ▪ Kategorien von Test- und Überprüfungsobjekten (z. B. das Institut, IT-Systeme, Komponenten) ▪ Art, Umfang und Frequenz von Tests und Überprüfungen ▪ Zuständigkeiten und Regelungen zur Vermeidung von Interessenkonflikten.

- Aufgabe des ISB?
- hier noch in der Abstimmungsphase
- derzeit Überlegungen, zunächst die Berücksichtigung der Soll-Vorgaben aus den Sicherheitsrichtlinien in den themenspezifischen Arbeitsanweisungen zu auditieren (SOLL-SOLL-Abgleich)

Bank für Kirche und Caritas eG

Exkurs: Auditierung



- Verknüpfung der auditierten Sollmaßnahmen mit der Überwachungs-handlung

Bank für Kirche und Caritas eG

4

Identitäts- und Rechtemanagement

Bank für Kirche und Caritas eG

Privilegierte Nutzer

6.7. Das Institut hat nach Maßgabe des Schutzbedarfs und der Soll-Anforderungen Prozesse zur Protokollierung und Überwachung einzurichten, die überprüfbar machen, dass die Berechtigungen nur wie vorgesehen eingesetzt werden. Aufgrund der damit verbundenen weitreichenden Eingriffsmöglichkeiten hat das Institut insbesondere für die Aktivitäten mit privilegierten (besonders kritischen) Benutzer- und Zutrittsrechten angemessene Prozesse zur Protokollierung und Überwachung einzurichten.

Die übergeordnete Verantwortung für die Prozesse zur Protokollierung und Überwachung von Berechtigungen wird einer Stelle zugeordnet, die unabhängig vom berechtigten Benutzer oder dessen Organisationseinheit ist. Zu privilegierten Zutrittsrechten zählen in der Regel die Rechte zum Zutritt zu Rechenzentren, Technikräumen sowie sonstigen sensiblen Bereichen.

- Überwachung privilegierter Nutzer in den Anwendungen VR-Control, FSA, etc.
- Turnus derzeit monatlich
- eine Lösung ggf. mit agree21OpSec möglich (AD-Events)

Bank für Kirche und Caritas eG

5

Auslagerungen und sonstiger Fremdbezug von IT-Dienstleistungen

Bank für Kirche und Caritas eG

Überwachung Informationssicherheitsprozess

9.3.	Der sonstige Fremdbezug von IT-Dienstleistungen ist im Einklang mit den Strategien unter Berücksichtigung der Risikobewertung des Instituts zu steuern. Die Erbringung der vom Dienstleister geschuldeten Leistung ist entsprechend der Risikobewertung zu überwachen.	Hierfür wird eine vollständige, strukturierte Vertragsübersicht vorgehalten. Die Steuerung kann auf der Basis dieser Vertragsübersicht durch Bündelung von Verträgen des sonstigen Fremdbezugs von IT-Dienstleistungen (Vertragsportfolio) erfolgen. Bestehende Steuerungsmechanismen können hierzu genutzt werden.

- Aufgabe des ISB?
- BAIT 4.4 – Aufgabe des ISB, den Informationssicherheitsprozess im Institut und gegenüber Dienstleistern zu steuern
- sofern relevant (Auslagerung oder sonstiger IT-Fremdbezug), Überwachung, ob Vertrag entsprechende Vereinbarungen, bspw.
    - Überlassung von Prüfungsberichten mit Bezug zu IS
    - Verpflichtung zu Meldung von IS-Vorfällen

  enthält

Bank für Kirche und Caritas eG

Risikobewertung

9.4. Die aus der Risikobewertung zum sonstigen Fremdbezug von IT-Dienstleistungen abgeleiteten Maßnahmen sind angemessen in der Vertragsgestaltung zu berücksichtigen. Die Ergebnisse der Risikobewertung sind in angemessener Art und Weise im Managementprozess des operationellen Risikos, vor allem im Bereich der Gesamtrisikobewertung des operationellen Risikos, zu berücksichtigen.

Dies beinhaltet beispielsweise Vereinbarungen zum Informationsrisikomanagement, zum Informationssicherheitsmanagement, zum Notfallmanagement und zum IT-Betrieb, die im Regelfall den Zielvorgaben des Instituts entsprechen.

Bei Relevanz wird auch die Möglichkeit eines Ausfalls eines IT-Dienstleisters berücksichtigt und eine diesbezügliche Exit- bzw. Alternativ-Strategie entwickelt und dokumentiert.

Als erforderlich erkannte Maßnahmen sind auch im Fall der Einbindung von Subunternehmen des IT-Dienstleisters zu berücksichtigen.

- ISB ist in die Risikobewertung einzubinden (BAIT 9.2)
- Stichwort „Vereinbarungen, die den Zielvorgaben des Instituts entsprechen“
- in Zukunft Vereinbarung SoMaKat mit Dienstleistern
    - abgespeckter Sollmaßnahmenkatalog für Dienstleister?
    - Hilfestellung aus dem Verbund?
    - Vorgehensweise bei bestehenden Auslagerungen/IT-Fremdbezügen?

Bank für Kirche und Caritas eG

6

dann wäre da noch ...

Bank für Kirche und Caritas eG

IT-Projekte und Anwendungsentwicklung

7.3.	IT-Projekte sind angemessen unter Berücksichtigung ihrer Ziele und Risiken im Hinblick auf die Dauer, Ressourcen und Qualität zu steuern. Hierfür sind Vorgehensmodelle festzulegen, deren Einhaltung zu überwachen ist.	Beispielsweise kann die Entscheidung über den Übergang zwischen den Projektphasen bzw. Projektabschnitten von eindeutigen Qualitätskriterien des jeweiligen Vorgehensmodells abhängen.
7.4.	Das Portfolio der IT-Projekte ist angemessen zu überwachen und zu steuern. Dabei ist zu berücksichtigen, dass auch aus Abhängigkeiten verschiedener Projekte voneinander Risiken resultieren können.	Die Portfoliosicht ermöglicht einen Überblick über die IT-Projekte mit den entsprechenden Projektdaten, Ressourcen, Risiken und Abhängigkeiten.
7.12.	Nach Produktivsetzung der Anwendung sind mögliche Abweichungen vom Regelbetrieb zu überwachen, deren Ursachen zu untersuchen und ggf. Maßnahmen zur Nachbesserung zu veranlassen.	Hinweise auf erhebliche Mängel können z. B. Häufungen von Abweichungen vom Regelbetrieb sein.

- eher Aufgabe Projektmanagement bzw. Infrastruktur-IT
- Einbindung des ISB bei relevanten Projekten und der Beschaffung von IT-Systemen (Aktualität Informations-verbund, Sikos, SOLL-IST-Abgleich SoMaKat, ...)

Bank für Kirche und Caritas eG

IT-Betrieb

8.6. Die Meldungen über ungeplante Abweichungen vom Regelbetrieb (Störungen) und deren Ursachen sind in geeigneter Weise zu erfassen, zu bewerten, insbesondere hinsichtlich möglicherweise resultierender Risiken zu priorisieren und entsprechend festgelegter Kriterien zu eskalieren. Hierzu sind Standardvorgehensweisen z. B. für Maßnahmen und Kommunikation sowie Zuständigkeiten (z. B. für Schadcode auf Endgeräten, Fehlfunktionen) zu definieren. Bearbeitung, Ursachenanalyse und Lösungsfindung inkl. Nachverfolgung sind zu dokumentieren. Ein geordneter Prozess zur Analyse möglicher Korrelationen von Störungen und deren Ursachen muss vorhanden sein. Der Bearbeitungsstand offener Meldungen über Störungen, wie auch die Angemessenheit der Bewertung und Priorisierung, ist zu überwachen und zu steuern. Das Institut hat geeignete Kriterien für die Information der Beteiligten (z. B. Geschäftsleitung, zuständige Aufsichtsbehörde) über Störungen festzulegen.

Die Identifikation der Risiken kann beispielsweise anhand des Aufzeigens der Verletzung der Schutzziele erfolgen.

Die Ursachenanalyse erfolgt auch dann, wenn mehrere IT-Systeme zur Störungs- und Ursachenerfassung sowie –bearbeitung eingesetzt werden.

Hier können standardisierte Incident– und Problemmanagement-Lösungen eingesetzt werden.

- Begrifflichkeiten Kontrolle, Überwachung und Überprüfung werden synonym verwendet
- Überwachung des IT-Betriebes ist in der BKC Aufgabe der Infrastruktur-IT

// Vielen Dank für Ihre Aufmerksamkeit!

Matthias Weskamp
// Abteilungsleiter Beauftragtenwesen

05251 121-1191
matthias.weskamp@bkc-paderborn.de
www.bkc-paderborn.de