BMC STRATEGY CONSULTANTS

Banken-IT im regulatorischen Fokus –
Informations-Sicherheitsmanagement professionalisieren und IT-Risk-Prüfungen wirksam vorbereiten

Diskussionspapier

Frankfurt, im Oktober 2019

Inhalt

1 Das neue IT-Prüfungsparadigma: breit, tief, rigoros

2 Inhaltliche Anforderungen – Herausforderungen für Banken

3 Best-Practice: proaktiv, pragmatisch, priorisiert

4 Unterstützungsansätze BMC

5 BMC Strategy Consultants Kontakt

Die bankaufsichtlichen Anforderungen an die IT (BAIT) sowie die (EZB-) IT-Risk-Prüfpraxis haben einen dramatischen Paradigmenwechsel bewirkt

Inhaltlich "rigoroses" Anforderungsparadigma

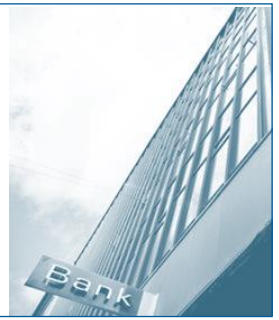
- Gesamtbild IT-Risiko über alle Prüfgebiete
- Anspruch von Vollständigkeit in „Asset-Aufnahme", Risikobewertung, Maßnahmen
- Technische Lösungen für Automatisierung ISM-Prozesse (Berechtigungsmanagement, SIEM/SOC, ...)
- Explizite Anforderungen an Ressourcen und Struktur der 2nd Line

"Rigorose" Prüfpraxis

- Große Teams mit hoher IT-Kompetenz
- Viele Stichproben, Begehungen, Datenanalysen und Prozesskontrollen
- Konkret implementierte Lösung wird bewertet (Prüfung von Verhaltenstatbeständen statt Richtlinien)
- Inhaltlicher Aufbau auf frühere Prüfungen, „Nulltoleranz“ für wiederholte Feststellungen

Trifft häufig auf schlecht vorbereitete Banken

- Geringe Einbindung und Kompetenz von Vorstand und Fachbereich
- Historisch nur niedrige Investitionen ins Thema
- Schlecht ausgestattete 1st/2nd-Line



Die Auswirkungen eines "negativen" Prüfergebnisses können dramatisch sein – Beispiele

Aufsichtsrat	▪ Vorwurf der Verletzung von Aufsichtspflichten (z.B. Prüfungsausschuss) ▪ Hinterfragung IT-Kompetenz durch die Aufsicht
Vorstand	▪ Gesamtverantwortung für Ergebnisse, Reputationsverlust ▪ Ggf. personelle Konsequenzen ▪ Hinterfragung IT-Kompetenz durch die Aufsicht
Bank insgesamt	▪ Aufgabenpakete zur "Abarbeitung" von Feststellungen mit Budgetvolumen in zwei- bis dreistelliger Millionenhöhe ▪ Zusätzlich ggf. Operational-Risk-Eigenkapital-Zuschläge im Rahmen SREP
Fachbereiche	▪ Viele neue Rollen und Aufgaben mit niedrigem Businessnutzen (DSK[1)], BISO[2)], ...) ▪ Starke operative Einbindung nötig ohne notwendiges Personal und Fähigkeiten ▪ Ggf. Verlangsamung und Erschwerung von Prozessen („Compliance-Netz“)
IT	▪ BAIT-Umsetzung schränkt ggf. Lieferfähigkeiten anderer Change-Themen (dramatisch) ein ▪ Weiterentwicklungs- und Betriebskostenanstieg durch Regulatorik

Proaktiver Handlungsbedarf in Banken

1) Daten-Schutz-Koordinatoren
2) Business Information Security Officer

Handlungsbedarf – Informationsmanagement professionalisieren, Prüfung vor- und nachbereiten

Prüfung mittelfristig vorbereiten → **IT-Risk-Prüfung** → **Ergebnisse abarbeiten**

Ziel: Informations-Sicherheitsmanagement in Bank professionalisieren

Säule 1: Effektives Vorgehen und Methode

- Gemeinschaftsaufgabe Fachbereich und IT
- Programmhafte Vorbereitung/Abarbeitung
- Risikobasiertes Vorgehen – größte Lücken mit höchstem Risiko am vordringlichsten schließen

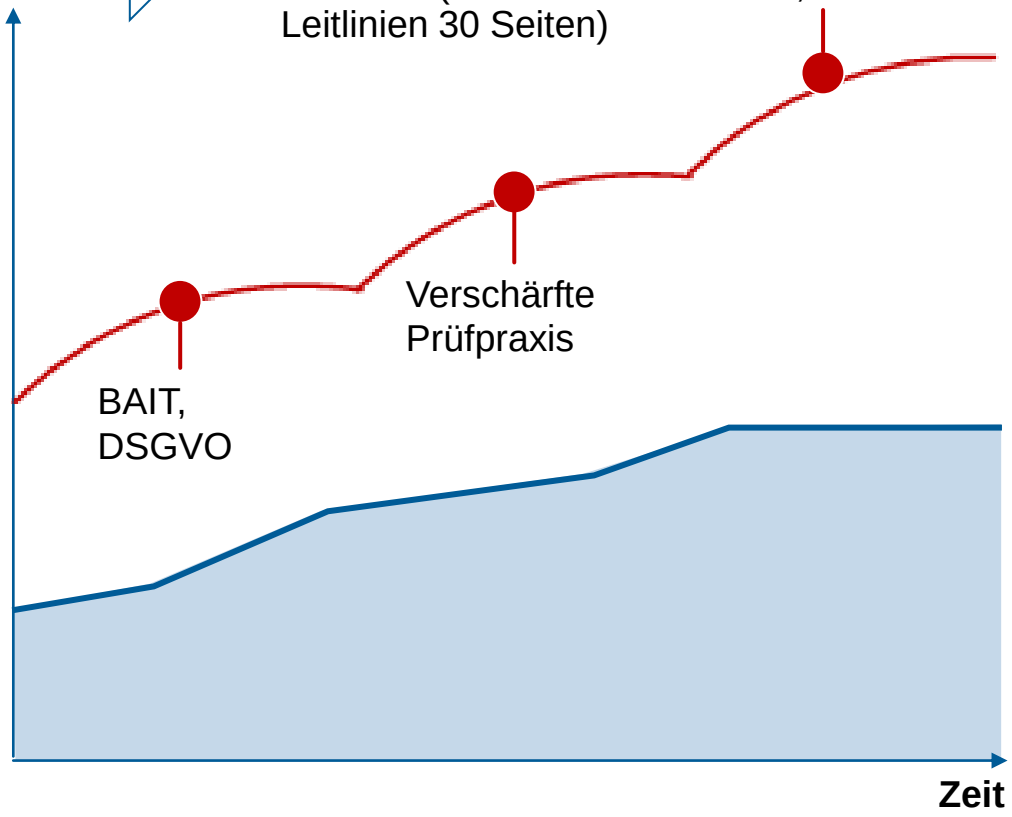
Säule 2: Tragfähige inhaltliche Lösungen schaffen

- Sinnvolle technische, prozessuale, organisatorische und policy-basierte Lösungen schaffen
- Übergreifende Integration der Einzellösungen z. B. in Tool- und Prozessarchitektur

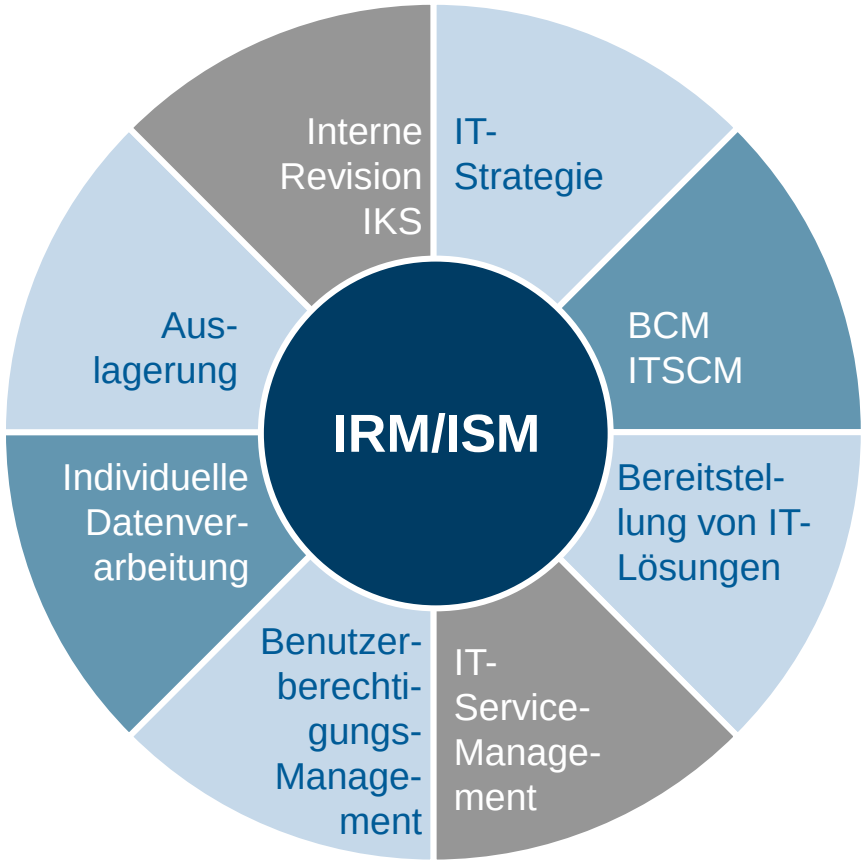
Die inhaltlichen Anforderungen steigen weiter an – aufgrund längerer Investitions- und Umsetzungszyklen hinken Banken oft hinterher

Beispiele neue Verschärfungen:

- Konkretisierung AT 7.3 MaRisk (Notfallmanagement) in 10. BAIT-Kapitel
- EBA-Leitlinien für Auslagerungssachverhalte[1] (MaRisk AT6 3 Seiten, EBA-Leitlinien 30 Seiten)



Themenfelder ISM etc.



1) Incl. Cloud-Regelungen

Auf übergreifender Ebene zeigt sich ein stringentes Prüfschema, dass praktisch wirksame, konsistente und verzahnte ISM-Zielbilder verlangt

Übergreifende Anforderungsdimensionen

Vollständigkeit der Assets/ Grundgesamtheit	Vollständigkeit und Validität Bewertungs-kriterien	Rigorose Bewertung der Risiken	Aktuelle, nachvollziehbare Dokumentation	Wirksame Maßnahmen	Maßnahmen-Ergebnis-Reporting
▪ Alle IT-Assets (inkl. BMA, IDV, Infra-struktur) ▪ Auslagerungstatbe-stände, Berechtigungen ▪ Abhängigkeiten	▪ Risiken ▪ Schutzbedarfe ▪ BIA ▪ …	▪ „Enge“ Auslegung ▪ Materielle „Nachvoll-ziehbarkeit“ ▪ Integration aktueller Monita	▪ Keine veraltete Paperware ▪ Inhaltliche Nach-vollziehbarkeit ▪ Zugriffsmöglichkeit	▪ Nachweisbar wirksam ▪ Überprüfung Wirksamkeit durch Kontrollprozesse	▪ Planung realistisch und mit Budget und verfügbarer Kapazität unterlegt ▪ Volle Transparenz

Operating Model "Informations-/IT Risk Management (BAIT)“"

- Klarheit der Rollen und Verantwortlichkeiten
- Ressourcenausstattung

Stimmiges konsistentes Lösungszielbild ...

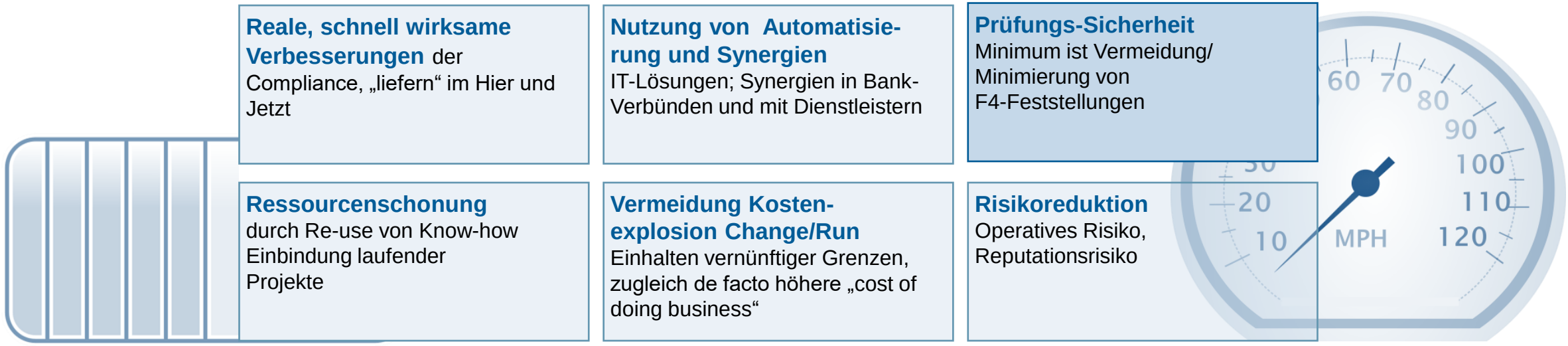
... über Prüfbereiche hinweg

Banken müssen auf diese Herausforderung vorbereitet sein – dabei sind heterogene Erwartungen (auch des Bank-Top-Managements) zu erfüllen

Erwartungen und Anforderungen an Lösungsansatz

Operativ — ***Strategisch***

Nachvollziehbarkeit und Verständlichkeit heterogener „technischer“ sowie „kleinteiliger“ Inhalte und Fortschritte	**Risikoadjustierte Themenpriorisierung** Effektives, „priorisiertes“ Vorgehen mit Fokus auf große Lücken (= Risiko gravierender Feststellungen)	**Skalierbare, nachhaltige** und effiziente betriebliche Lösungen; wenn möglich „Zusatznutzen“
Reale, schnell wirksame Verbesserungen der Compliance, „liefern“ im Hier und Jetzt	**Nutzung von Automatisierung und Synergien** IT-Lösungen; Synergien in Bank-Verbünden und mit Dienstleistern	**Prüfungs-Sicherheit** Minimum ist Vermeidung/ Minimierung von F4-Feststellungen
Ressourcenschonung durch Re-use von Know-how Einbindung laufender Projekte	**Vermeidung Kostenexplosion Change/Run** Einhalten vernünftiger Grenzen, zugleich de facto höhere „cost of doing business“	**Risikoreduktion** Operatives Risiko, Reputationsrisiko

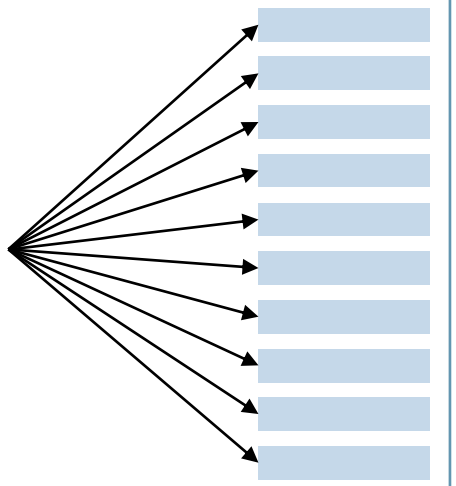
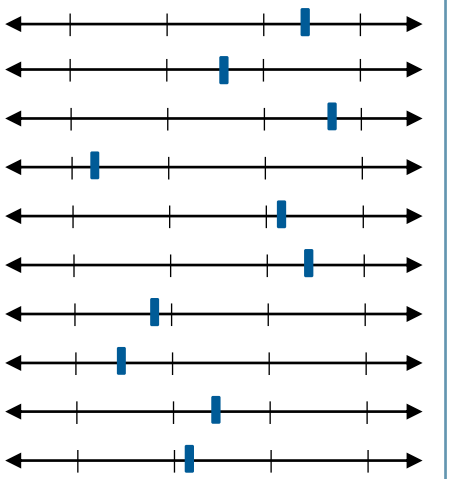


Am Markt hat sich die präventive, risiko-orientierte und programmatische Herangehensweise zur Schaffung von Regulatory Readiness bewährt

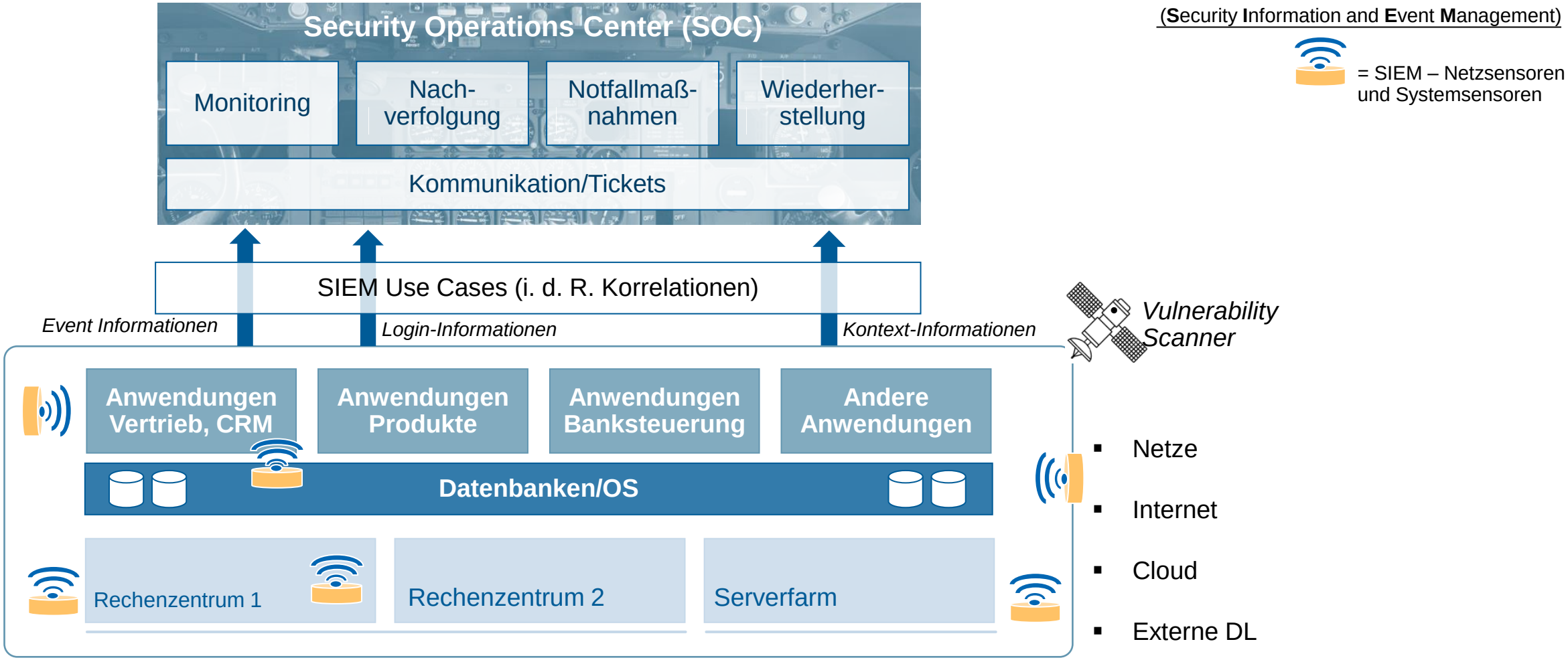
„Good Practice“ zur Erzeugung von Regulatory Readiness		In der Regel nicht zu empfehlende Vorgehensweisen
✓ Regulatorisches Readiness Informationsmanagement **Programm** (ca. 1-3 Jahre)	⟷	Vielzahl unterschiedlich gesteuerter Einzelinitiativen
✓ **Gemeinsame Fachbereichs-, IT- und Compliance-Verantwortung**	⟷	IT soll das Problem alleine lösen
✓ **Risikoorientiertes Vorgehen**, Priorisierung von „Gaps“	⟷	„Gießkannenprinzip“
✓ Transparent vorlegbare **Roadmap** mit klar messbaren Ergebnissen pro Quartal	⟷	„Alles gleichzeitig starten“
✓ Steuerung durch Bereichsebene unter **Vorstands-einbindung**	⟷	Dezentrale Steuerung oder „Top-down only“

Dabei wird die Sicht auf "Risikofelder" in eine Projektlogik mit klaren Verantwortlichkeiten übergeleitet

BEISPIEL

Quellen	Anforderungen	Relevante Anforderungen	Projekt-zuordnung	Ziellerreichungs-definition („Sprunghöhe“)
Health-checks in einzelnen Disziplinen MaRisk/BAIT Self-Assessment EZB IT-Questionaire Gruppenrichtlinie ISM Konzernrichtlinie Notfall WP-Jahres-abschlussprüfung Revisionsmonita Andere, z.B., DSGVO, EBA RL Outsourcing	▪ Findings ▪ Monita ▪ Anforderungen	▪ Bereinigung Redundanzen ▪ Priorisierung nach – Wichtigkeit – Dringlichkeit ▪ Soll-Ist Gap Abgleich ▪ Zuordnung Risikofelder		

Technische Lösungen sind Grundvoraussetzungen für einen effizienten und wirksamen Sicherheitsbetrieb – Beispiel (SIEM)



BMC Strategy Consultants unterstützt Banken in der Professionalisierung des Informationsmanagements

BMC-Strategy-Consultants-Ansatz

IT-Risk-Prüfung

Vorgelagerte Professionalisierung Informationsmanagement

Nachgelagerte Professionalisierung Informationsmanagement

A	B	C	D
IT-Risk-Prüfungserfahrung	**Managementansatz**	**Technisches und prozessuales Lösungs-Know-how**	**Tools**

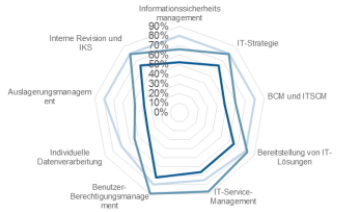
Ergebnisse für unsere Klienten

- ✓ Erhöhung Prüfungssicherheit
- ✓ Wirtschaftlich sinnvolles Vorgehen
- ✓ Nachhaltige technisch-prozessuale Lösungen
- ✓ Einbeziehung der Bank in Veränderungsprozess

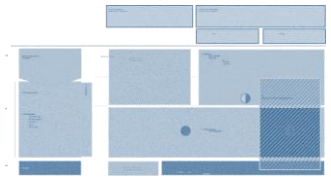
Unsere Unterstützungsansätze

I. Prüfungsvorbereitende Optimierung ("Regulatory Readiness")

Ia Regulatory Readiness Lückenanalyse



Ib Design Scope und Setup Regulatory Readiness Programm

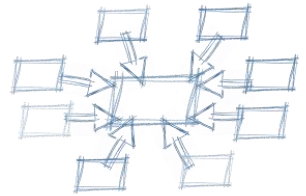


Ic Ext. Programmsteuerung Umsetzung Vorbereitende Maßnahmen und Fortschrittscontrolling

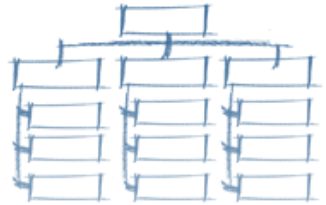
IT-Risk-Prüfung

II. Nachgelagertes Abarbeiten

IIa Design Zielbildoptionen



IIb Aufsetzen und Budgetierung Umsetzungsprojekt



IIc Ext. Programmsteuerung Umsetzung Maß-nahmen und Fortschrittscontrolling

BMC Strategy Consultants: Kontakt

Deutschland:
BMC Strategy Consultants GmbH

Taunus Turm, Taunustor 1
DE-60310 Frankfurt am Main
+ 49 69 50 50 60 4-586

Roland.Bubik@bmc-strategy.com
+49 170 554 1013

Thomas.Pasche@bmc-strategy.com
+49 175 290 5018

Schwesterfirma in Österreich:
BMC Professionals GmbH

Tuerkenschanzplatz 7/4
AT-1180 Wien
+ 43 6604 968608

Roland.Kropf@bmc-professionals.com