DEUTSCHE BUNDESBANK
EUROSYSTEM

Veranstaltung „IT-Aufsicht bei Banken“

LSI-ICT-SREP - erste Erkenntnisse der Aufsicht

Andreas Vogel, Deutsche Bundesbank, Zentralbereich Banken und Finanzaufsicht

Agenda

1. **Hintergrund zum ICT SREP**

2. **Erste Erkenntnisse der Aufsicht**
   – Risikolevel
   – Risikokontrollen

3. **Status quo und Ausblick**

Aufsichtlicher Überprüfungs- und Bewertungsprozess zu IT-Risiken
Erste umfassende Analyse der IT-Risiken im deutschen Bankensektor

2018

- Inkrafttreten der EBA „Leitlinien für die IKT-Risikobewertung im Rahmen des aufsichtlichen Überprüfungs- und Bewertungsprozesses (SREP)“
  - Umfassende aufsichtliche Bewertung der Risikolevel und -kontrollen
  - Notwendigkeit zur strukturierten Datenerhebung bei Instituten bzw. deren IT-Dienstleistern

2019

- Erster Testlauf bei HP-LSIs sowie weiteren ausgewählten Instituten
- Überarbeitung der SSM Methodik auf Basis der gemachten Erfahrungen

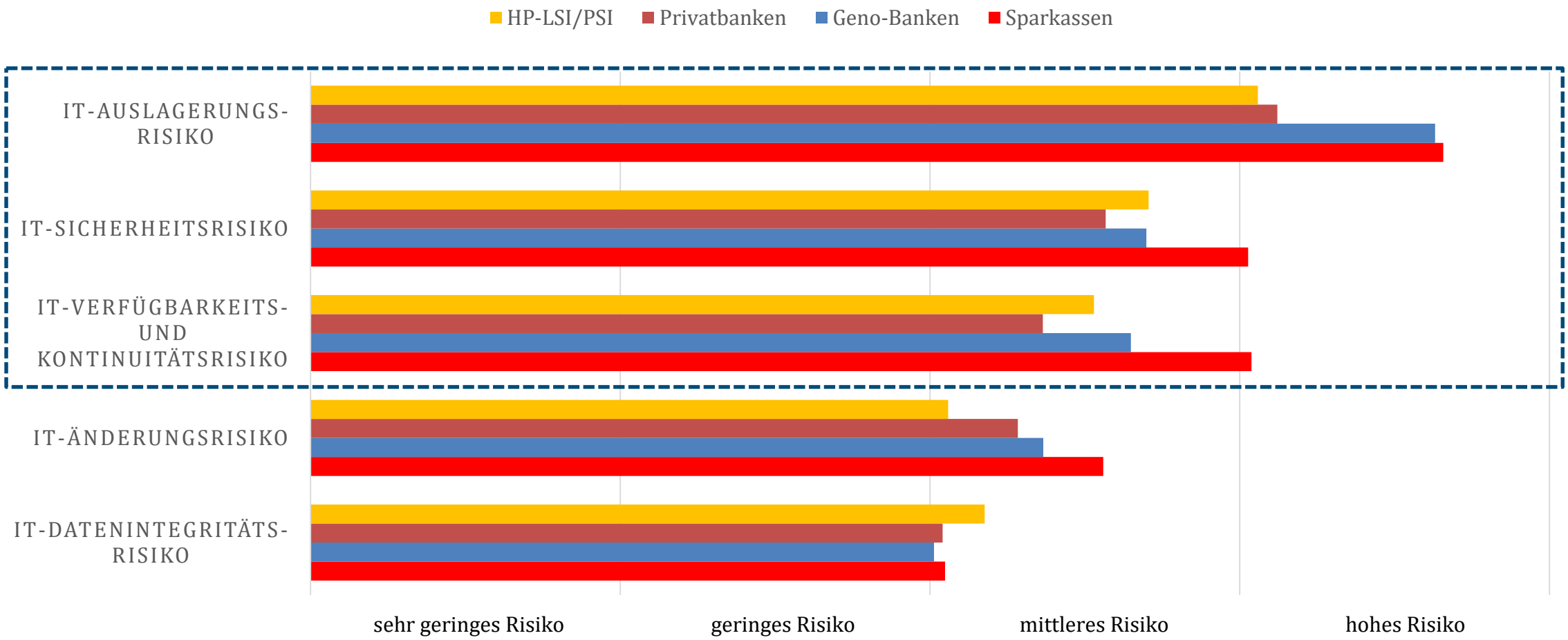
2020

- Erstmalige Durchführung im Echtbetrieb geplant
- Aufgrund von COVID-19 Pandemie um ein Jahr verschoben

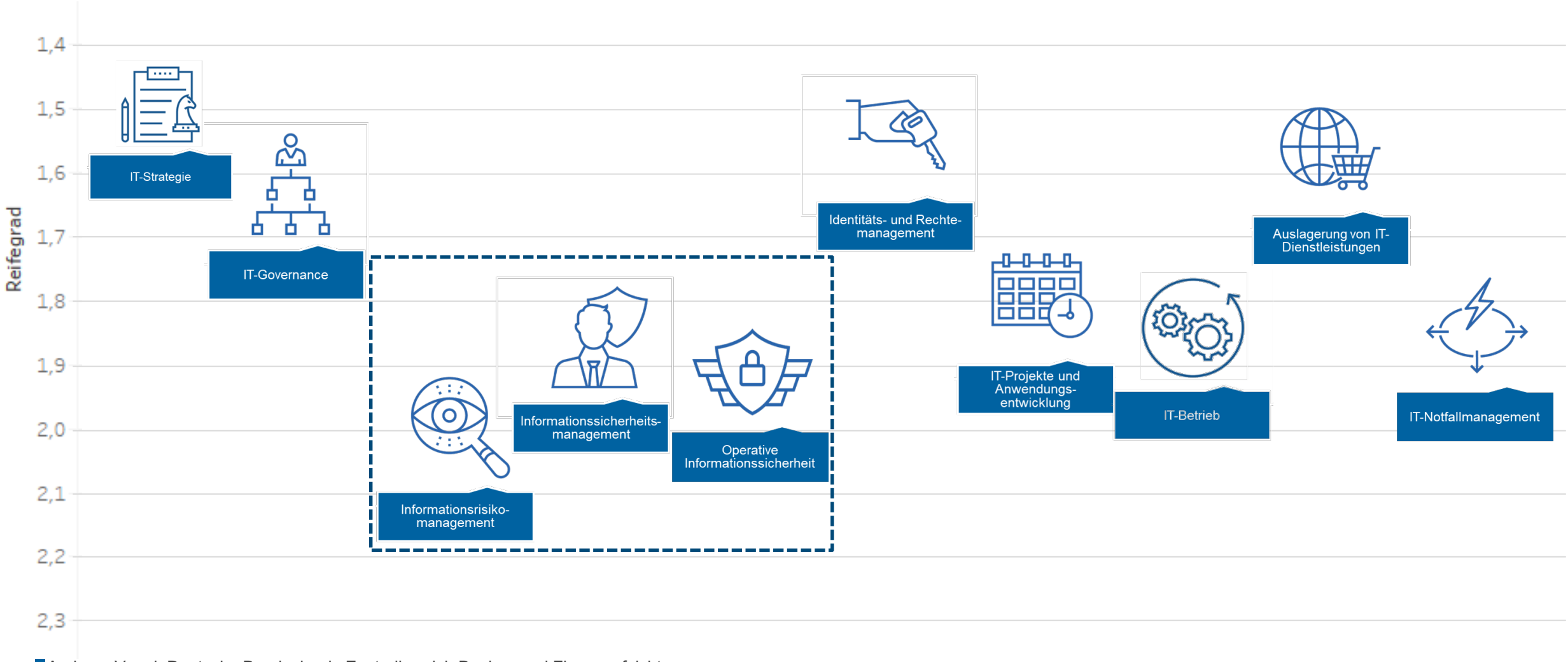
2021/22

- Versendung der Fragebögen an alle Kreditinstitute in nationaler Aufsicht, die den „Full“ SREP durchlaufen

Alle befragten Institute sehen IT-Risiken auf mindestens mittlerem Niveau
Größte IT-Risiken werden bei Auslagerungen, Sicherheit und Verfügbarkeit gesehen



Institute sehen eigene Reifegrade auf hohem absolutem Niveau
Informationsrisiko- und Informationssicherheitsprozesse vergleichsweise ausbaufähig



Informationssicherheitsmanagement definiert und überwacht Schutzmaßnahmen
Jedes Institut benötigt einen unabhängigen Informationssicherheitsbeauftragten (ISB)

Anforderung der BAIT 4.5.f: *„Die Funktion des Informationssicherheits-beauftragten ist organisatorisch und prozessual unabhängig auszugestalten, um mögliche Interessenskonflikte zu vermeiden.“ „Jedes Institut hat die Funktion des Informationssicherheitsbeauftragten grundsätzlich im eigenen Haus vorzuhalten.“*

Zielsetzung: Unabhängige Überprüfung und Steuerung der Informationssicherheit

Häufige Probleme:
- ISB-Funktion ist in der zu überwachenden IT-Organisation angesiedelt
- Überwachungsaufgaben der ISB-Funktion (2. Verteidigungslinie) werden durch die IT-Organisation (1. Verteidigungslinie) vorgenommen
- ISB-Funktion hat unzureichende Ressourcen / fehlender Vertreter für ISB

Informationsrisikomanagement entscheidend für nachhaltige Kontrolle des IT-Risikos
Regelmäßiger Soll-Ist-Abgleich notwendig für die Identifizierung von Schwachstellen

Anforderung der BAIT 3.7.: *„Das Institut hat auf Basis der festgelegten Risikokriterien einen Vergleich der Sollmaßnahmen mit den jeweils wirksam umgesetzten Maßnahmen (dem Ist-Zustand) durchzuführen.“*

Zielsetzung: Zeitnahe Identifizierung und Behandlung von Informationsrisiken

Häufige Probleme:

- kein regelmäßiger bzw. unangemessen langer Zeitraum für Abgleich der implementierten Maßnahmen mit den Sollmaßnahmen
- zu unspezifische Vorgaben im Sollmaßnahmenkatalog um Abgleich durchzuführen
- unzureichende Kommunikation der Ergebnisse

Operative Informationssicherheit setzt Vorgaben des ISM um Security Information and Event Management (SIEM) alarmiert bei Angriffen

Operative Informationssicherheit

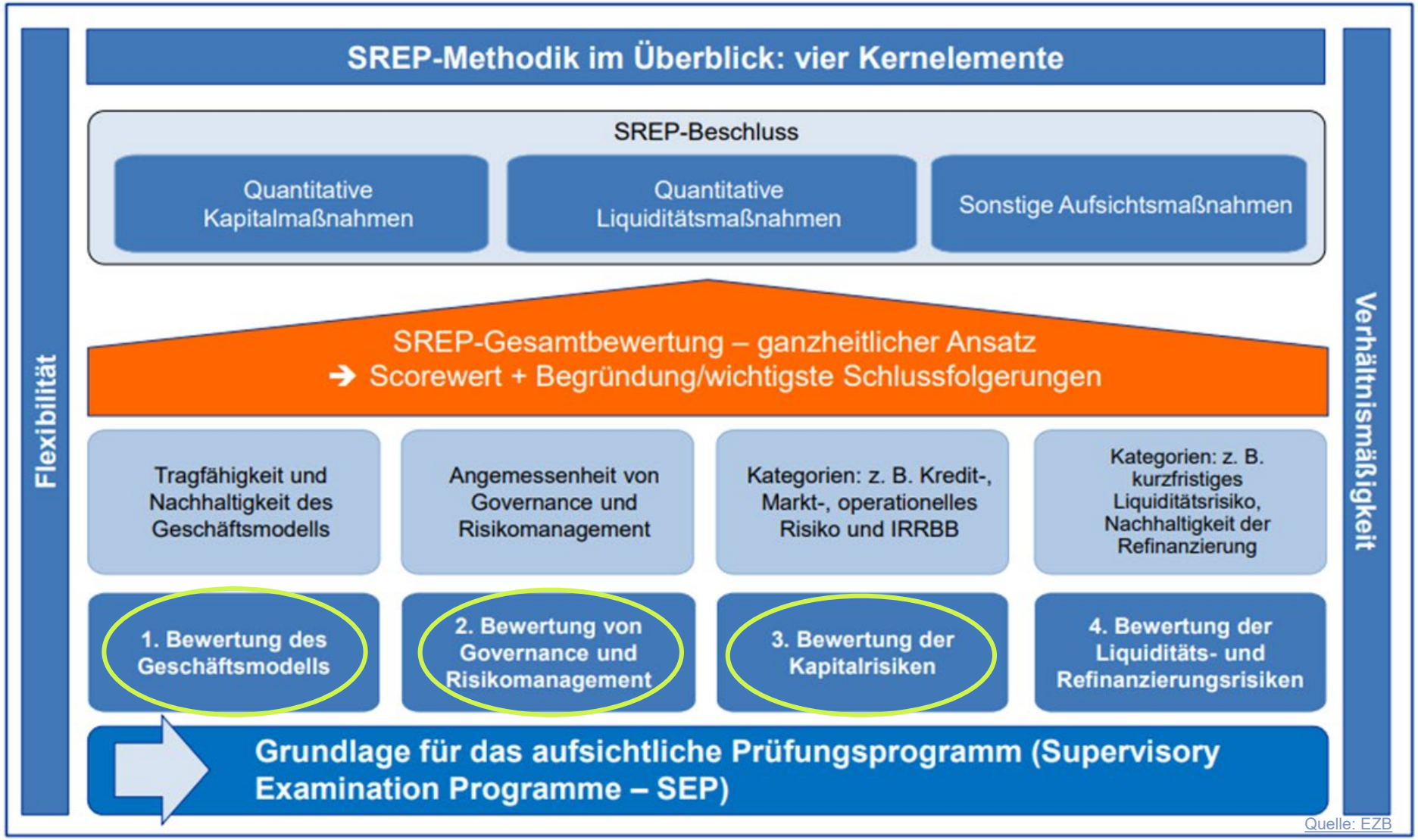
Anforderung der BAIT 5.3.ff: *„Gefährdungen des Informationsverbundes sind möglichst frühzeitig zu identifizieren. Potentiell sicherheitsrelevante Informationen sind angemessen zeitnah, regelbasiert und zentral auszuwerten. [..]“; „Sicherheitsrelevante Ereignisse sind zeitnah zu analysieren, und auf daraus resultierende Informationssicherheitsvorfälle ist […] angemessen zu reagieren.“*

Zielsetzung: Frühzeitige Entdeckung und Behandlung von Angriffen

Häufige Probleme:

- relevante IT-Systeme werden nicht analysiert / fehlende Anbindung
- unzureichende Überwachung der Alarme
- unzureichende Reaktionsfähigkeit auf IS-Vorfälle

IT-Risiken wirken sich vielfältig auf das Risikoprofil der Institute aus
Aufsicht ergreift sowohl Kapital- als auch sonstige Maßnahmen



Quelle: EZB

Status quo und Ausblick
ICT SREP wird auf Basis der Erkenntnisse und im Dialog mit Industrie weiterentwickelt