Prozesslandkarte BAIT

ISACA IT-GRC-Kongress, 28. September 2022, Mannheim

ISACA Fachgruppe IT-Compliance im Finanz- und Versicherungswesen

Jörg Lobbes, Steffen Mack, Christian Siepmann, Christian Schwartz

ISACA Germany Chapter

Vorbemerkung

"das Kleingedruckte"

Der vorgestellte Inhalt:

- ist die private Meinung der Autoren und spiegelt nicht die Einschätzung der durch die Autoren vertretenden Firmen wider
- ist unsere Interpretation der BAIT und nicht autorisiert durch die BAFIN
- hat keinen Anspruch auf Vollständigkeit
- soll eine Basis für die weitere Diskussion in der Community sein, Feedback ist erwünscht

ISACA Germany Chapter

Referenten & Autoren

Referenten & zusätzliche Autoren (an der Erstellung beteiligt, Danke)

Jörg Lobbes

IT-Compliance Officer der Eurex Clearing AG, Gruppe Deutsche Börse

Dozent der Frankfurt School of Finance and Management

Schwerpunkte BAIT, MaRisk, COBIT, ITIL, ISO27k

Steffen Mack

Manager Global Contract, Risk & Controls der Giesecke+Devrient Mobile Security GmbH

Schwerpunkt Umsetzung der regulatorischen Anforderungen (MaRisk, BAIT und KRITIS)

Christian Siepmann

Manager IT und Risikocontrolling eines Wertpapierinstituts in Stuttgart

verantwortete Zentralisierungen von IT-Systemen in Rechenzentren samt Netz-Migrationen, sowie den Aufbau von ISMS und Datenschutzprogrammen

Christian Schwartz

leitender Managing Consultant der usd AG

Leiter der ISACA-Fachgruppe IT-Compliance im Finanz- und Versicherungs-wesen

verantwortet den usd Beratungsbereich Informationssicherheit in der Finanz- und Versicherungswirtschaft

Uwe Brinkmann

IT-Prüfer, Sparkassenverband Niedersachsen
- Prüfungsstelle -

Referat IT-Revision

IT-Prüfungen (Prüfungskonzeption und -koordination, Durchführung sowie Qualitätssicherung)

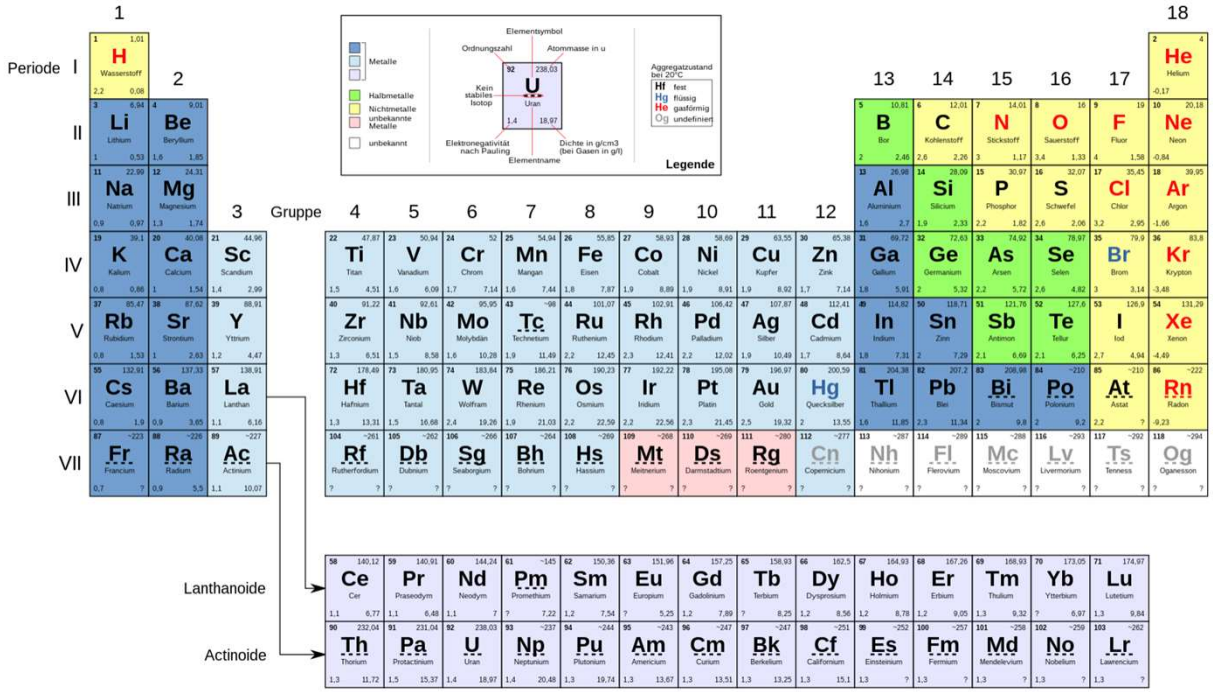
Frank Innerhofer

Geschäftsführer Innerhofer Risk Management GmbH

Schwerpunkt Informa-tionssicherheit und Risikomanagement von IT, speziell im Kontext von IT-Outsourcing

ISACA Germany Chapter

Das Ziel



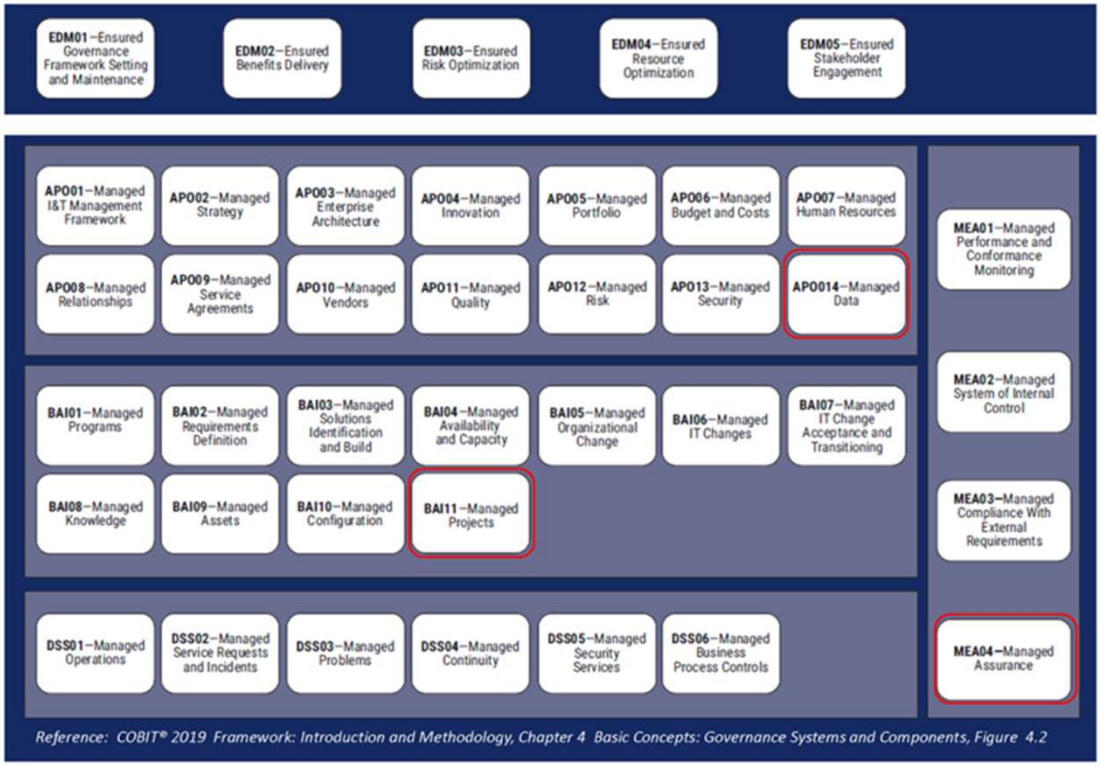
Ein Bild sagt mehr als 100 Worte.

Eine übersichtliche Darstellung aller Prozesse der BAIT.

Quelle: https://commons.wikimedia.org/wiki/File:Periodensystem_newdraft.svg

ISACA Germany Chapter

Das Ziel



Vergleichbar auch mit relevanten Prozessmodellen, wie ITIL und COBIT

Quelle: Information Systems Audit and Control Association (ISACA), Control Objectives for Information and Related Technology (COBIT 2019)

ISACA Germany Chapter

Das Ziel

BaFin Bundesanstalt für Finanzdienstleistungsaufsicht

AT 4.3 Internes Kontrollsystem

1. In jedem Institut sind entsprechend Art, Umfang, Komplexität und Risikogehalt der Geschäftsaktivitäten

   a. Regelungen zur Aufbau- und Ablauforganisation zu treffen,
   b. Risikosteuerungs- und -controllingprozesse einzurichten und
   c. eine Risikocontrolling-Funktion und eine Compliance-Funktion zu implementieren.

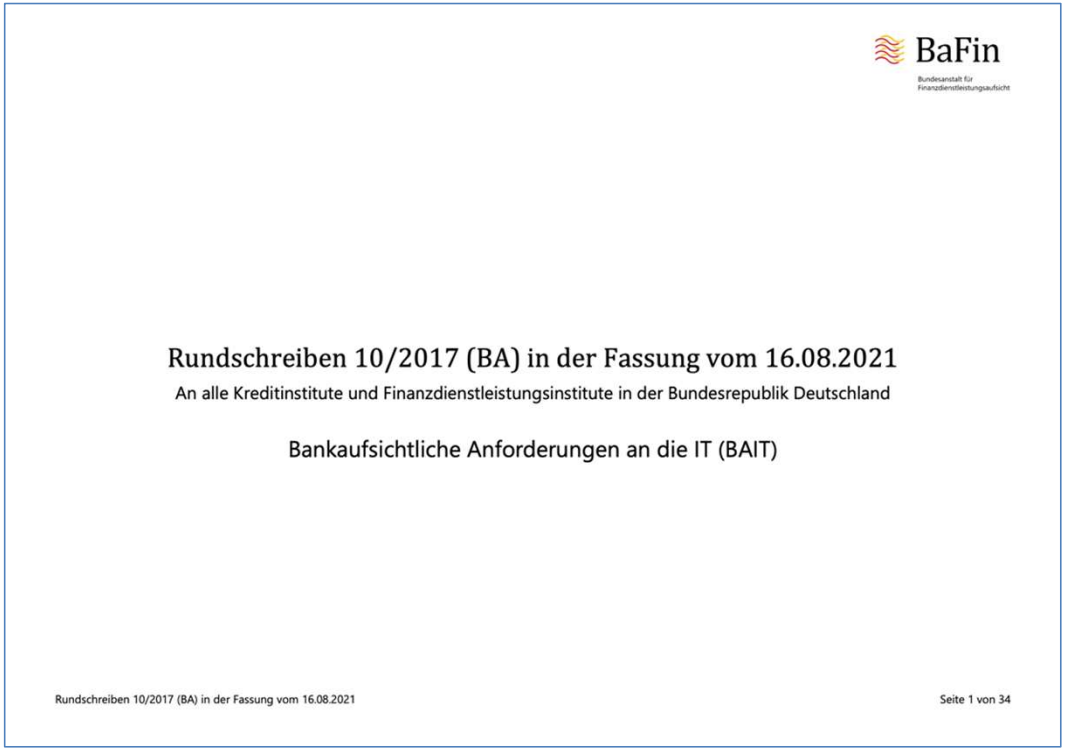
Prozesslandkarte BAIT anwendbar als:

- Best Practice Vorlage für die notwendige IT-Prozesslandschaft
- zur Umsetzung von KWG §25a MaRisk AT5
- Vorlage für IKS in den Instituten

Quelle: MaRisk BAFIN www.bafin.de

ISACA Germany Chapter

BAIT



BaFin
Bundesanstalt für Finanzdienstleistungsaufsicht

Rundschreiben 10/2017 (BA) in der Fassung vom 16.08.2021

An alle Kreditinstitute und Finanzdienstleistungsinstitute in der Bundesrepublik Deutschland

Bankaufsichtliche Anforderungen an die IT (BAIT)

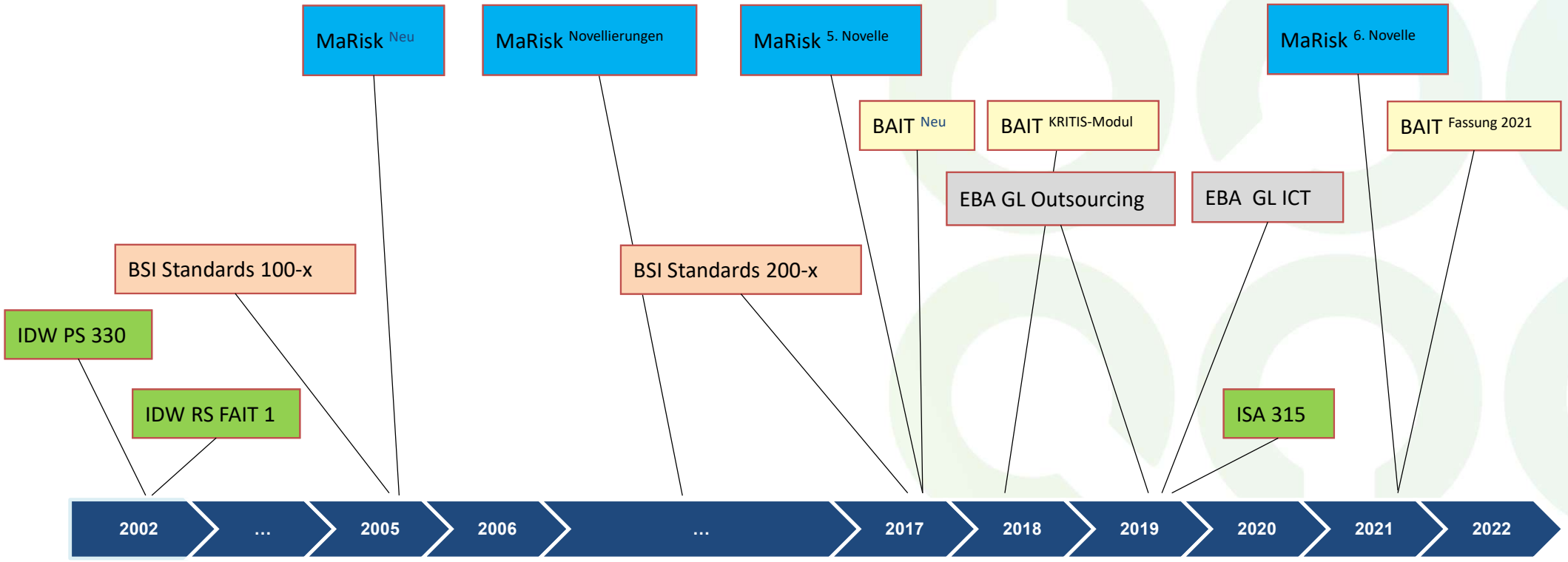
Rundschreiben 10/2017 (BA) in der Fassung vom 16.08.2021 Seite 1 von 34

Quelle: BAIT BAFIN www.bafin.de

ISACA Germany Chapter

BAIT

Zeitliche Entwicklung aufsichtsrechtlicher IT-Anforderungen und Prüfungsstandards



Quelle: eigene Darstellung

ISACA Germany Chapter

BAIT

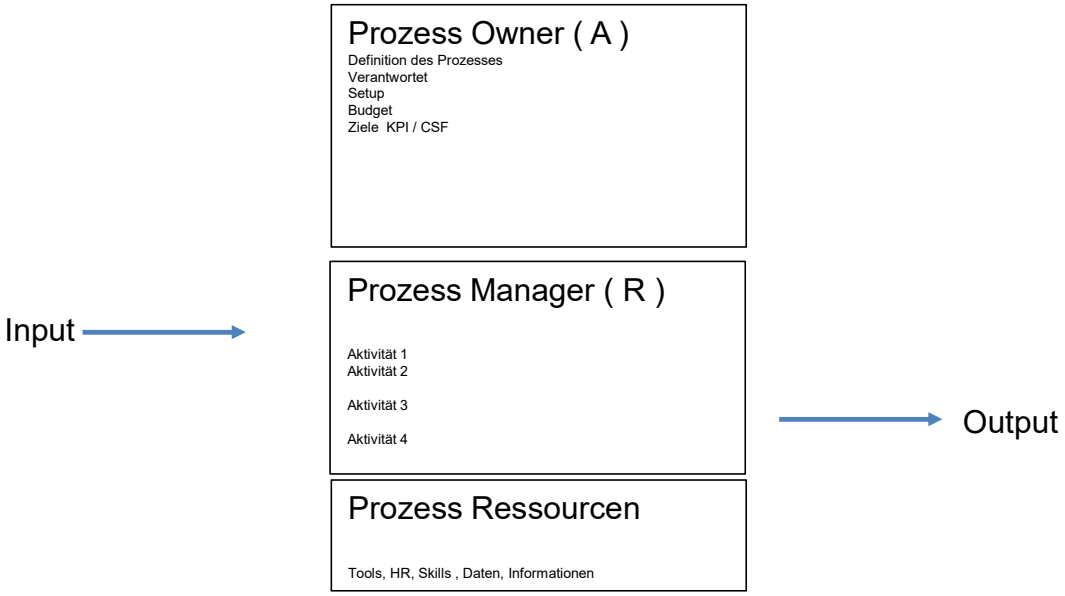
Inhalt

Quelle: BAIT BAFIN www.bafin.de

ISACA Germany Chapter

Was ist ein Prozess?

Generisches Prozessmodell Prozessmodell nach ITIL



R & A entsprechend der RACI – Matrix

R - responsible
A - accountable

Quelle: eigene Darstellung

ISACA Germany Chapter

Was ist ein Prozess?

Prozesse im Sinne des IKS

Ein Prozess ist eine zeitliche und logische Verkettung von Einzelaktivitäten mit vorgegebenem In- und Output sowie definierten Mess- und Steuerungsgrößen.

Prozesse werden in Prozessbeschreibungen beschrieben und durch Verfahrens- und Arbeitsanweisungen ergänzt.

Unterteilung in:

primäre Prozesse (Kernprozesse)

sekundäre Prozesse (unterstützend)

Performance Management
KPI

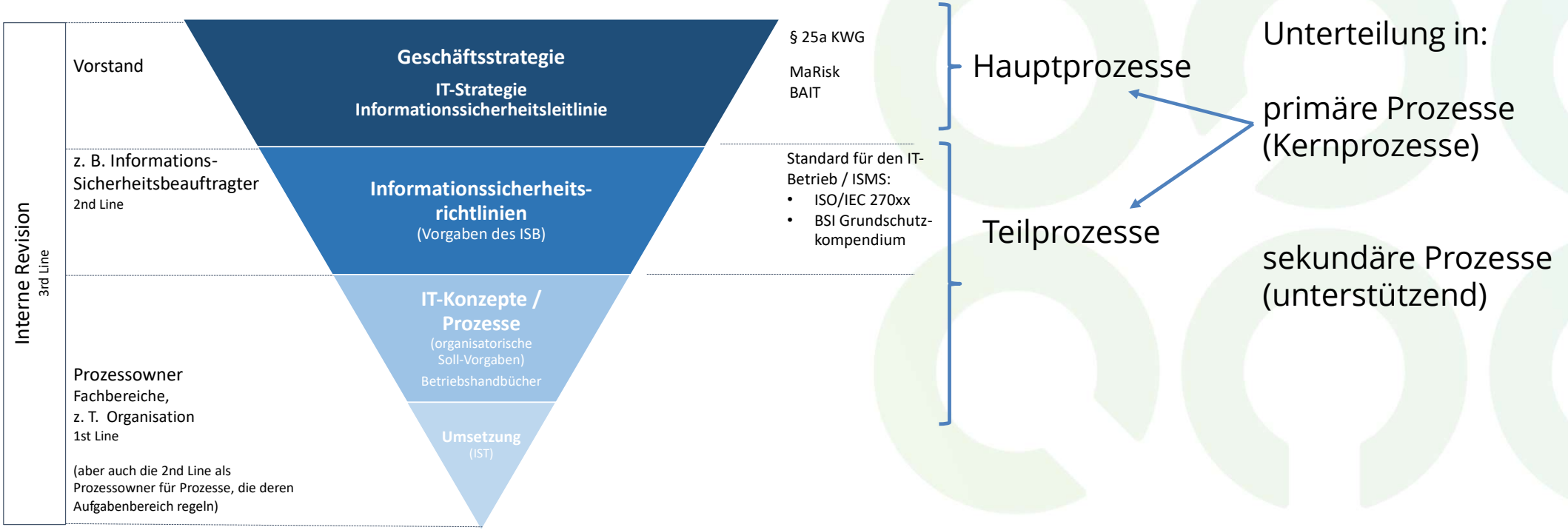
Risikomanagement
KRI

Quelle: Oliver Bungartz, Handbuch Interner Kontrollsysteme (IKS), Erich Schmidt Verlag

ISACA Germany Chapter

Was ist ein Prozess?

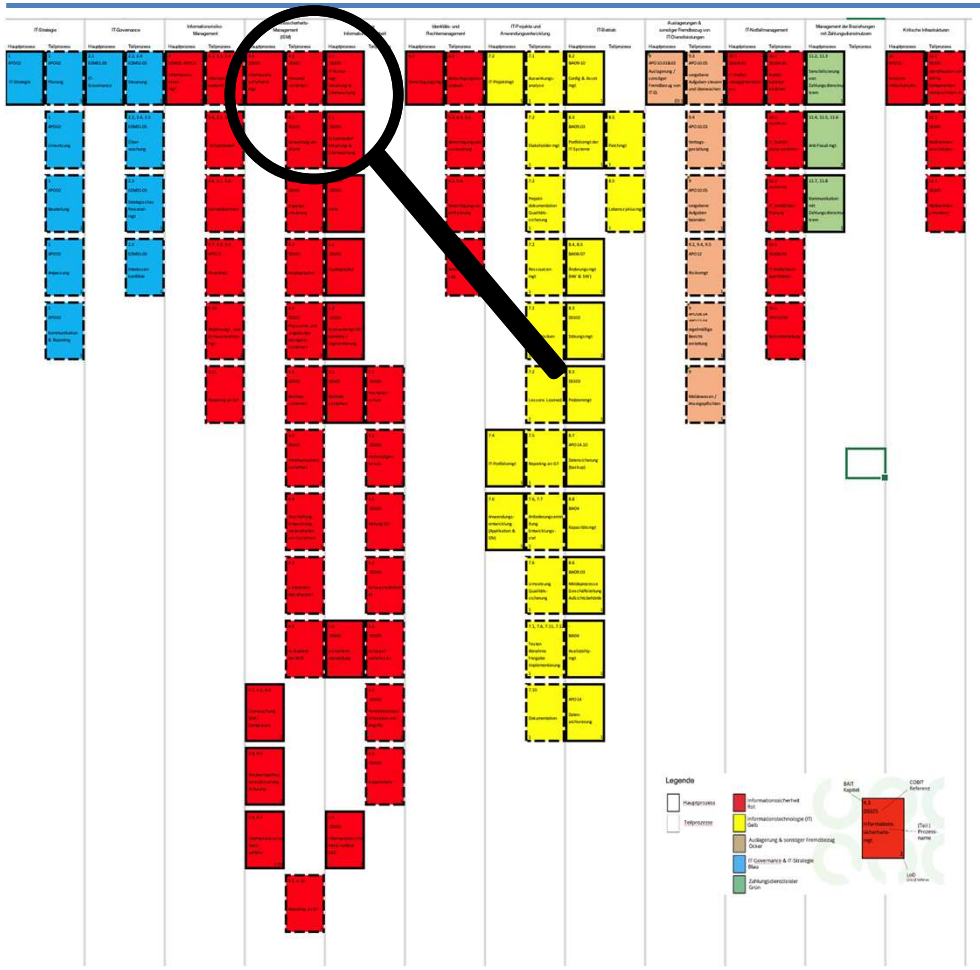
Prozesse und deren Zuordnung (am Beispiel ISM)

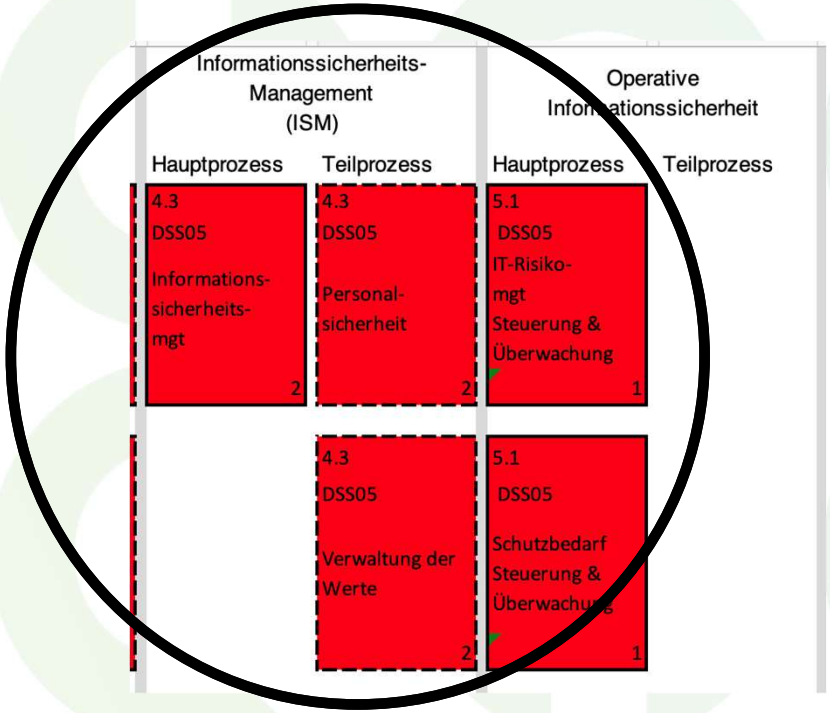


Quelle: eigene Darstellung

ISACA Germany Chapter

Das Ergebnis: die Prozesslandkarte BAIT





Quelle: eigene Darstellung nach unserer Interpretation der BAIT

ISACA Germany Chapter

Das Ergebnis: die Prozesslandkarte BAIT

Legende

Hauptprozess

Teilprozesse

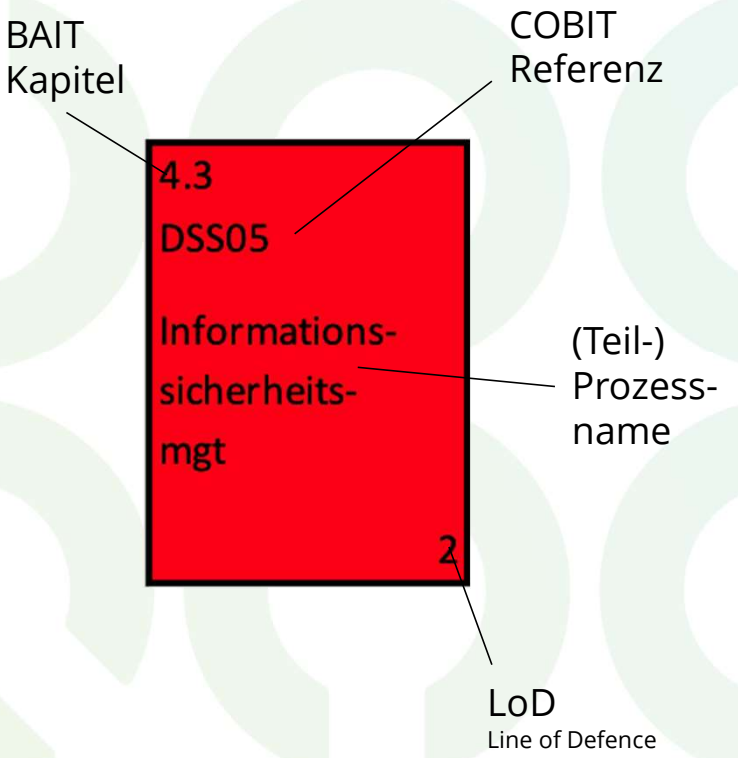
Informationssicherheit
Rot

Informationstechnologie (IT)
Gelb

Auslagerung & sonstiger Fremdbezug
Ocker

IT-Governance & IT-Strategie
Blau

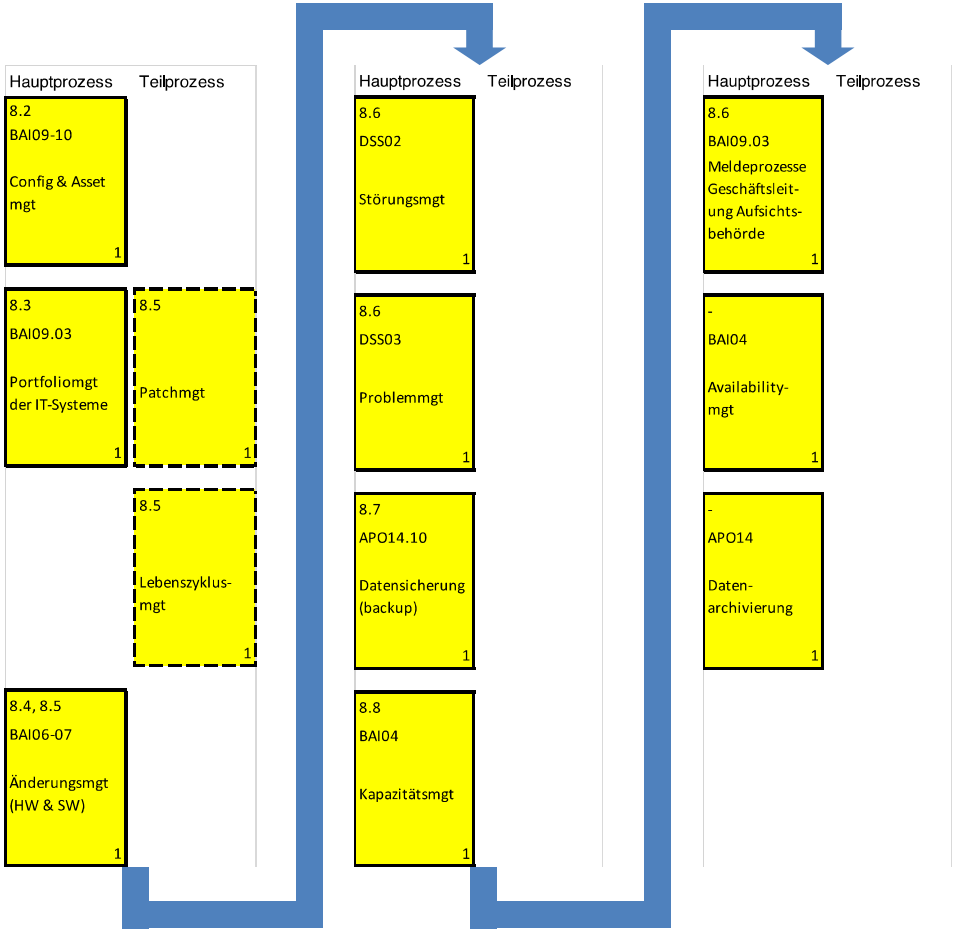
Zahlungsdienstleister
Grün



Quelle: eigene Darstellung nach unserer Interpretation der BAIT

ISACA Germany Chapter

Prozesse im Kapitel IT-Betrieb



Thematische Gruppierung

- Konfigurations-, Asset- und Portfoliomanagement
- Changemanagement
- Störungs- und Problemmanagement
- Backup (und Archivierung)
- Kapazitäts- (und Availabilitymanagement)

Nicht in der BAIT behandelte (aber relevante) Themen

- Datenarchivierung
- Availabilitymanagement

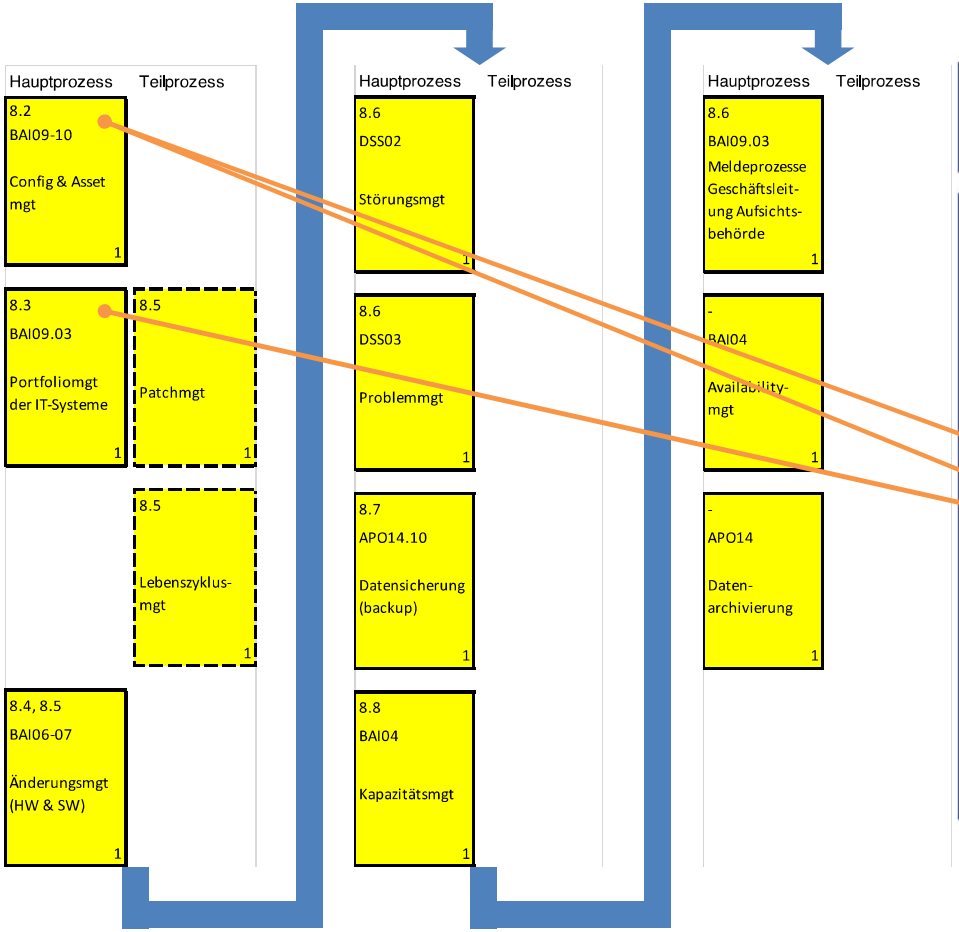
Teilprozesse

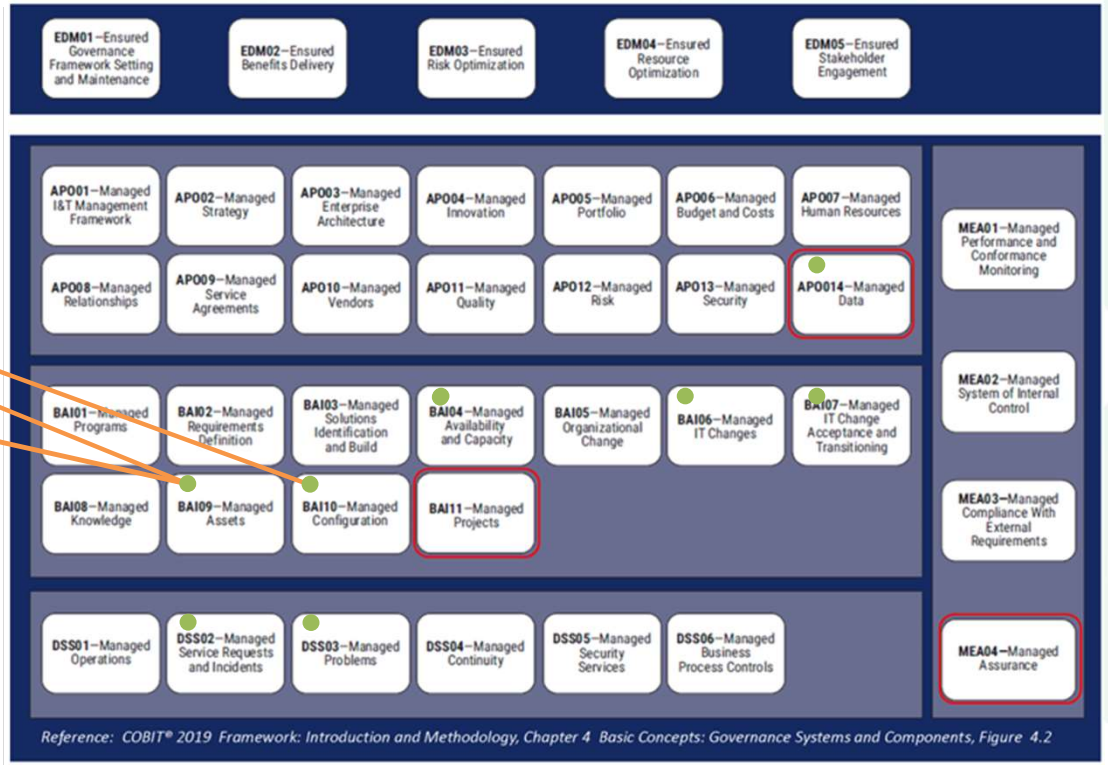
- Patchmanagement
- Lebenszyklusmanagement

Quelle: eigene Darstellung nach unserer Interpretation der BAIT

ISACA Germany Chapter

Prozesse im Kapitel IT-Betrieb im Bezug zu COBIT



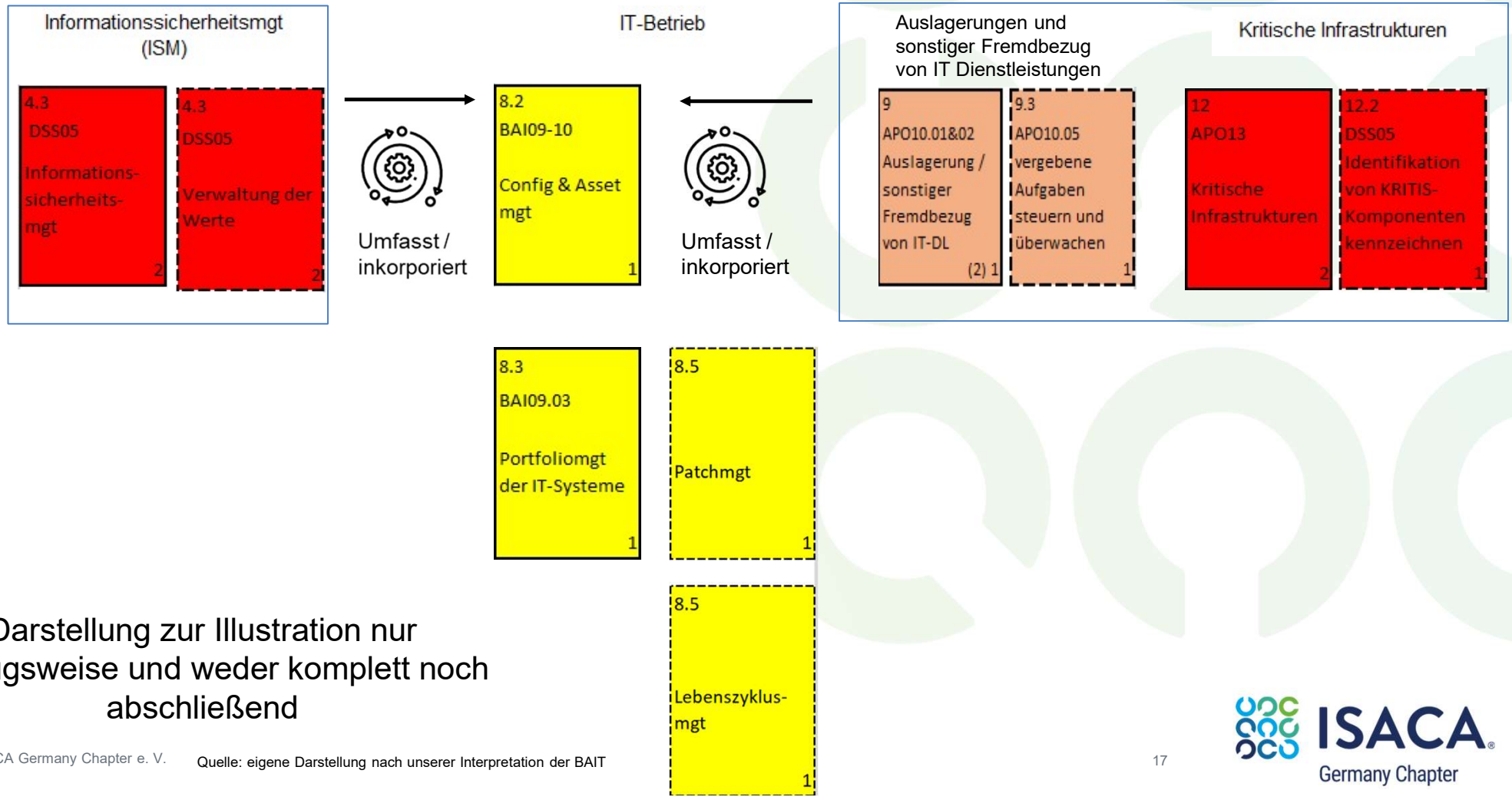


Quelle: eigene Darstellung nach unserer Interpretation der BAIT

Quelle: Information Systems Audit and Control Association (ISACA)
Control Objectives for Information and Related Technology (COBIT 2019)

ISACA Germany Chapter

Prozesse im IT Betrieb und Lines of defence

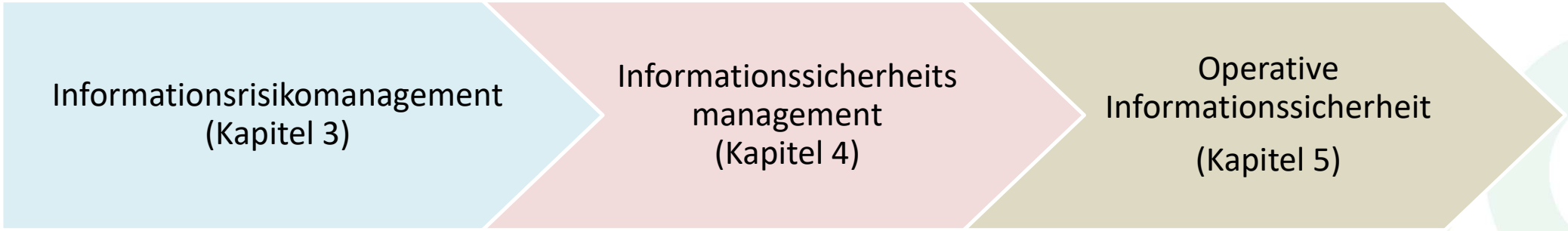


Darstellung zur Illustration nur auszugsweise und weder komplett noch abschließend

Quelle: eigene Darstellung nach unserer Interpretation der BAIT

ISACA Germany Chapter

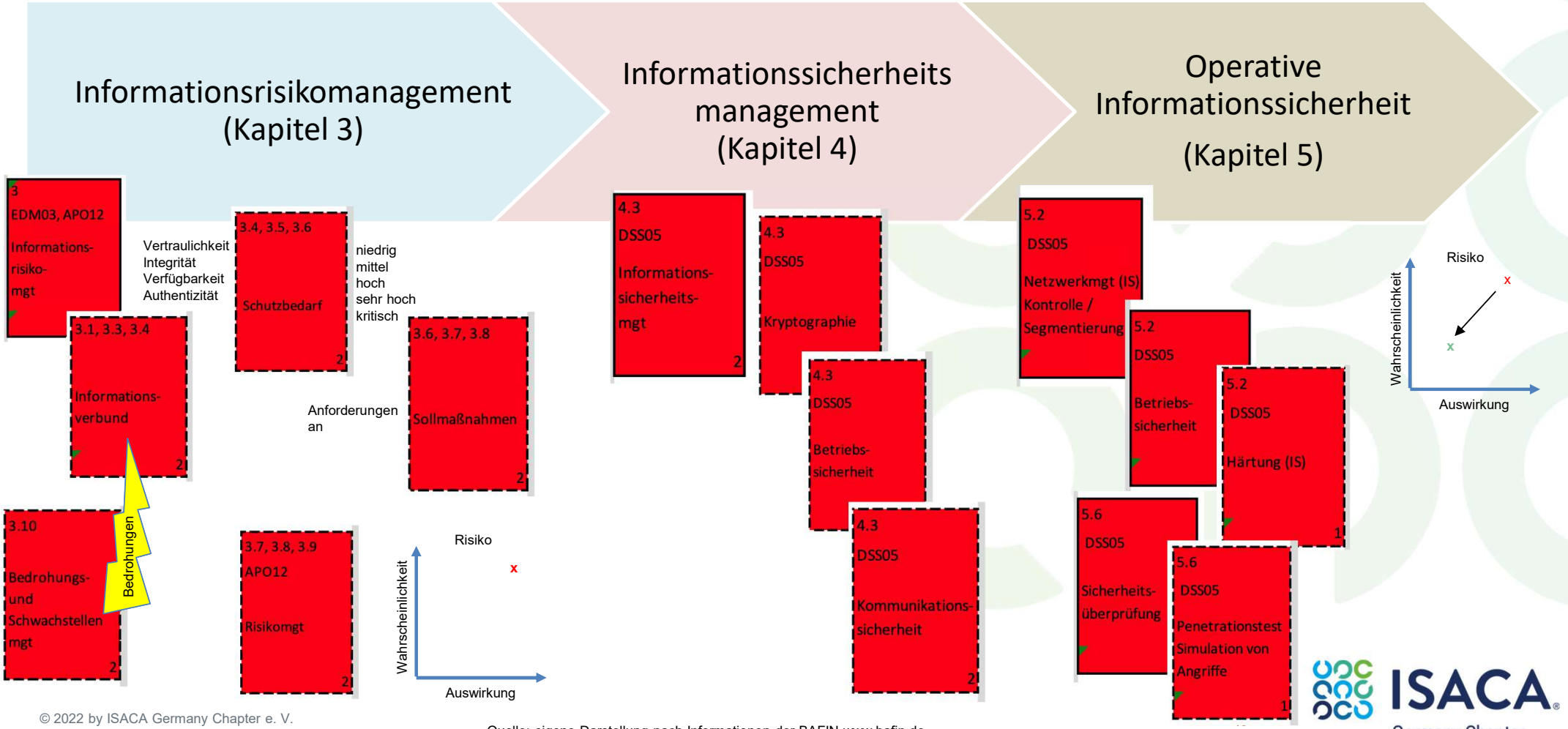
Zusammenspiel BAIT Kapitel 3 - 5



Quelle: eigene Darstellung nach Informationen der BAFIN www.bafin.de

ISACA Germany Chapter

Zusammenspiel BAIT Kapitel 3 – 5 (beispielhaft)



Quelle: eigene Darstellung nach Informationen der BAFIN www.bafin.de

ISACA Germany Chapter

Next steps

Weiterentwicklung der Prozesslandkarte BAIT

- Abhängigkeiten unter den Prozessen darstellen (in einer interaktiven Darstellung)
- Sekundäre Prozesse zusätzlich aufzeigen
- KPI‘S / KRI‘s als zusätzliche Informationen hinzufügen
- Rollen & Rollenmodelle als zusätzliche Informationen hinzufügen
- Gapanalyse zu DORA

Feedback

Feedback aus der Community erwünscht

Wo seht ihr Abweichungen von unserer Darstellung?
Welche Vorschläge habt ihr für die Themen, das Design der BAIT Landkarte?

Download der BAIT Landkarte unter:
https://www.isaca.de/de/FG_IT_Compliance_FV

Feedback an Emailadresse:
fg-it-compliance-fvw+bait-landkarte@isaca.de

FICF/0

ISACA Germany Chapter

Folie 21

FICF/0 Test erfolgreich

Fachgruppen IT-Compliance Fina; 2022-09-25T09:11:52.481

JL0 0 :-)

Joerg Lobbes; 2022-09-25T09:21:10.339

Backup Slides: Angewandte Methodik

"das Kleingedruckte"

1: Umsetzung der Anforderungen aus der BAIT erfolgt in Prozessen
Ansatz:
Expertenmeinung: Interpretation im Sinne KWG §25a und MaRisk AT5 als Minimalanforderung

2: Trennscharfe Unterscheidung in primäre und sekundäre Prozesse & Haupt- und Teilprozesse
Ansatz:
Im ersten Schritt sind nur primäre Prozesse aufgezeigt, diese jeweils unterschieden in Haupt- und Teilprozesse

ISACA Germany Chapter

ISACA®

Germany Chapter