ADOGRC
Governance, Risk & Compliance

BOC Group
Design Your Enterprise

Erfolgsfaktoren für DORA und NIS-2

Die erfolgreiche Umsetzung mit ADOGRC

Antonia Hubbermann

13.09.2024

Agenda

ADOGRC
Governance, Risk & Compliance
by boc-group.com

Rechtsakte für Cybersicherheit

Integration von DORA mit ADOGRC

Ausblick für NIS-2

Zusammenfassung

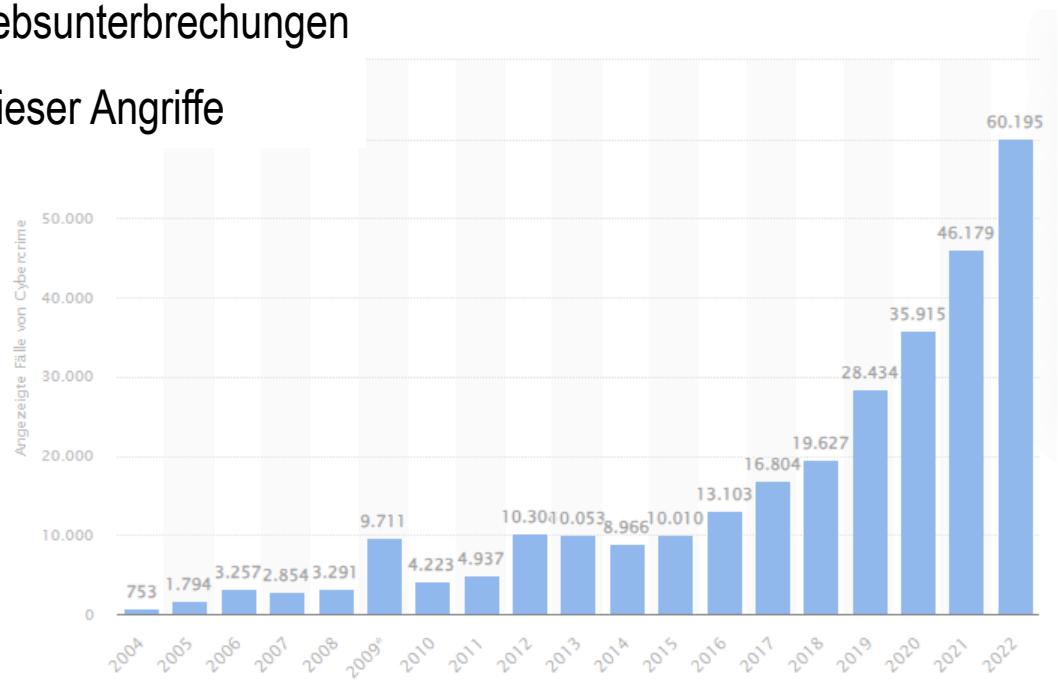
Rechtsakte für Cybersicherheit

ADOGRC
Governance, Risk & Compliance

Warum brauchen wir Gesetze für Cybersicherheit?

ADOGRC
Governance, Risk & Compliance
by boc-group.com

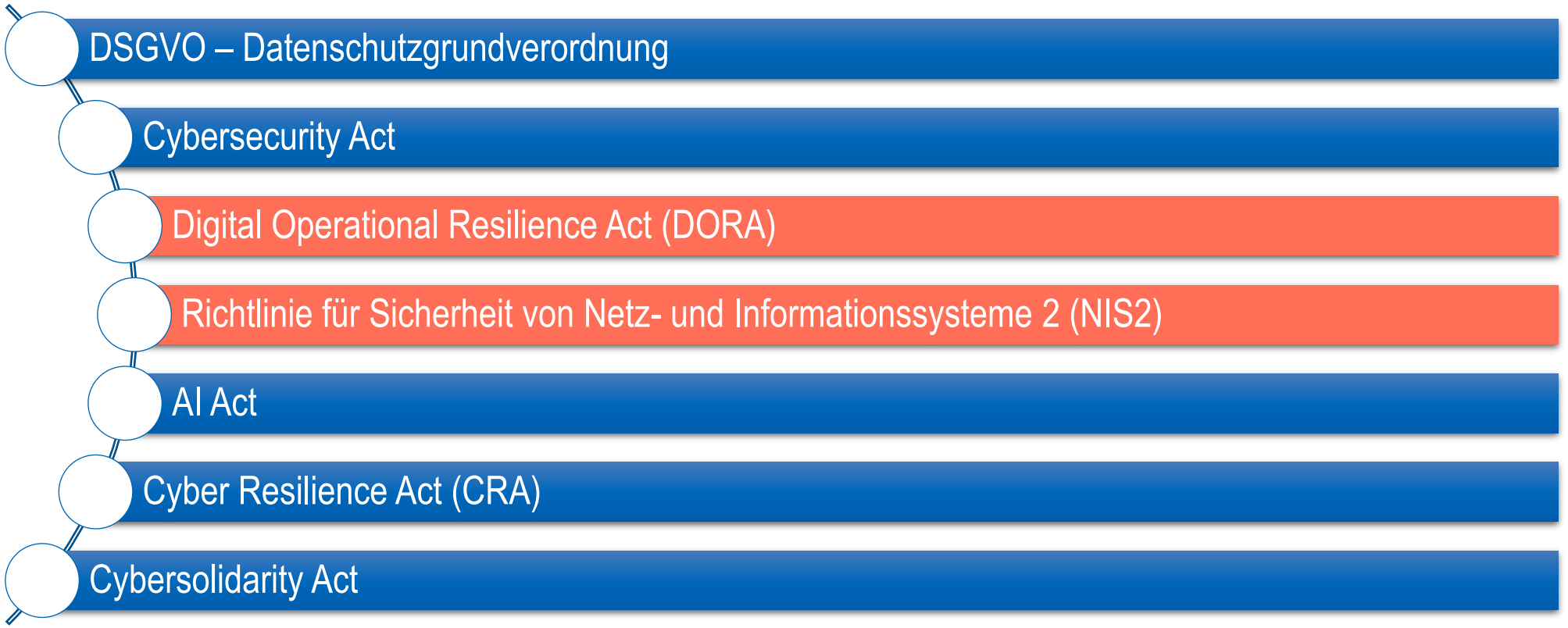
- 2023 erlebten **84,7% der Organisationen weltweit** mindestens einen Cyberangriff (Tendenz steigend)
- **Jeder 6. Cyber-Angriff ist erfolgreich (KPMG-Studie)**
- Anstieg von Ransomware-Angriffen in **Schadensausmaß und Häufigkeit**
  - 33% der Firmen in Österreich berichten von einwöchigen Betriebsunterbrechungen
- Vor allem kritische Infrastrukturen und KMUs sind zunehmend Ziel dieser Angriffe



Quelle:
https://parachute.cloud/cyber-attack-statistics-data-and-trends/
https://kpmg.com/at/de/home/media/press-releases/2024/04/kpmg-cybersecurity-studie-zeigt-keine-entspannung-fuer-heimische-unternehmen-in-sicht.html

Rechtsgrundlagen für Cybersicherheit

ADOGRC
Governance, Risk & Compliance
by boc-group.com



Vergleich der Gesetzgebungen

ADOGRC
Governance, Risk & Compliance
by boc-group.com

DORA-Verordnung

- IKT-Risikomanagement
- Management von IKT-bezogener Vorfällen
- Testen der digitalen operationellen Resilienz
- Management des Drittparteienrisikos
- Vereinbarungen über den Austausch von Informationen
- Aufsicht über kritische Drittdienstleister

NIS2-Richtline

- Risikoanalyse und Konzept für Sicherheit der Informationssysteme
- Management von Sicherheitsvorfällen
- Business Continuity und Krisenmanagement
- Sicherheit in der Lieferkette
- Sicherheitsmaßnahmen bei Erwerb/Entwicklung/Wartung von IKT-Anwendungen
- Richtlinien für Cyberhygiene, Zugriffskontrolle und Kryptographie

Vergleich der Gesetzgebungen

ADOGRC
Governance, Risk & Compliance
by boc-group.com

DORA-Verordnung

- IKT-Risikomanagement
- Management von IKT-bezogener Vorfällen
- Testen der digitalen operationellen Resilienz
- Management des Drittparteienrisikos
- Vereinbarungen über den Austausch von Informationen
- Aufsicht über kritische Drittdienstleister

NIS2-Richtline

- Risikoanalyse und Konzept für Sicherheit der Informationssysteme
- Management von Sicherheitsvorfällen
- Business Continuity und Krisenmanagement
- Sicherheit in der Lieferkette
- Sicherheitsmaßnahmen bei Erwerb/Entwicklung/Wartung von IKT-Anwendungen
- Richtlinien für Cyberhygiene, Zugriffskontrolle und Kryptographie

Stärkung der Widerstandsfähigkeit von europäischen Unternehmen gegen die Bedrohung durch Cyberangriffe

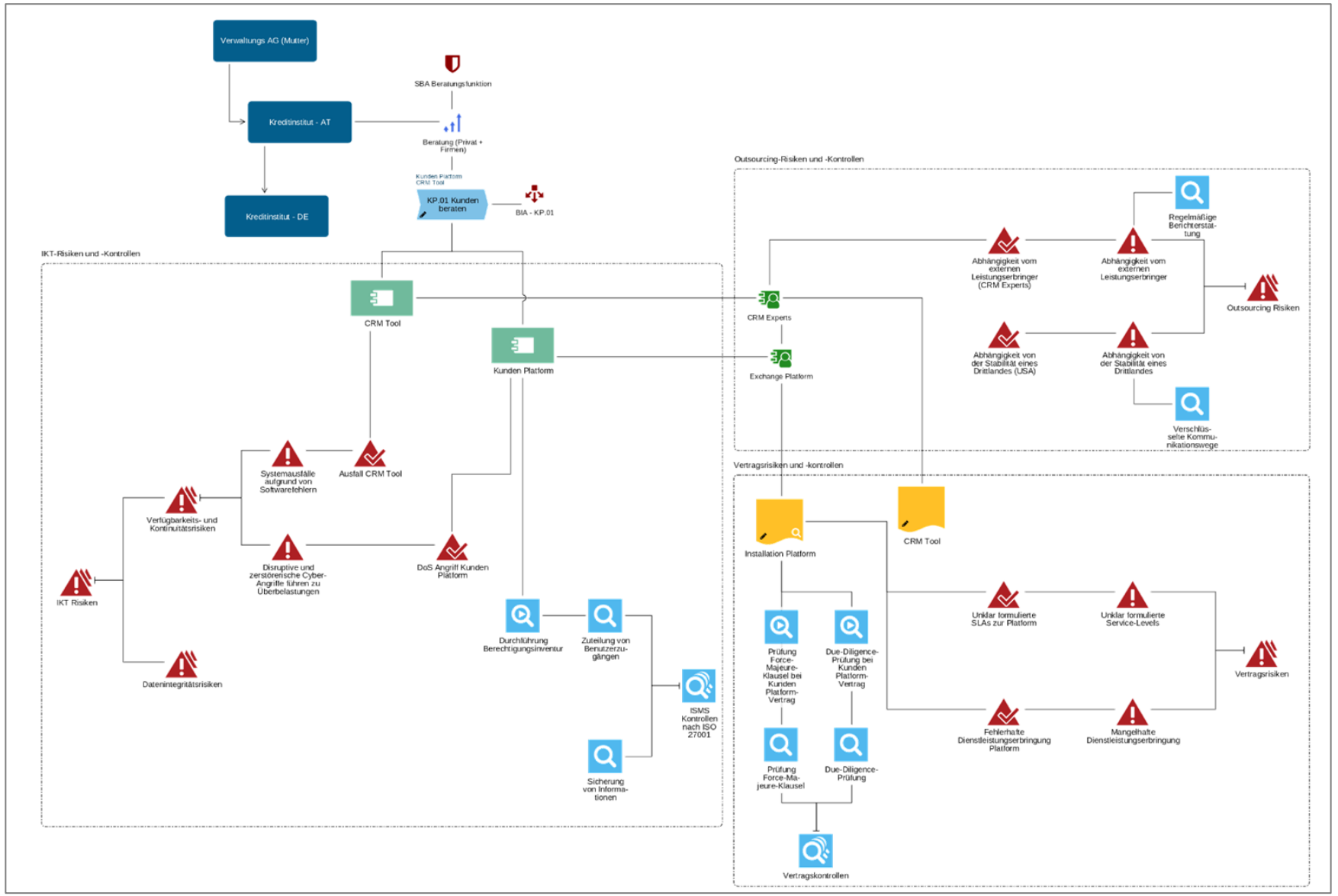
- Finanzmarkt
- Unternehmen, die Teil der kritischen Infrastruktur sind

Integration von DORA mit ADOGRC

ADOGRC
Governance, Risk & Compliance

DORA Lösung

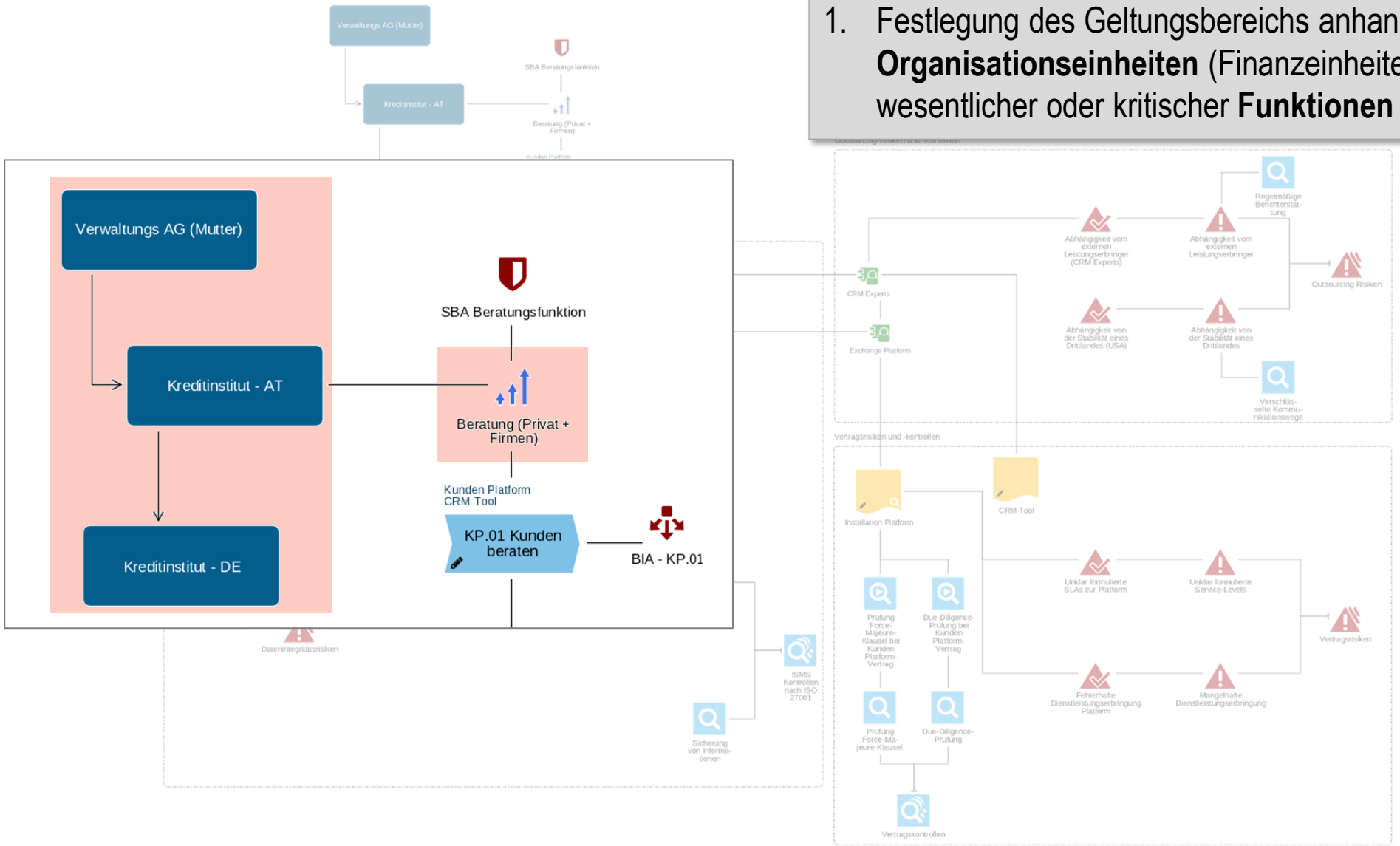
ADOGRC
Governance, Risk & Compliance
by boc-group.com



Geltungsbereich

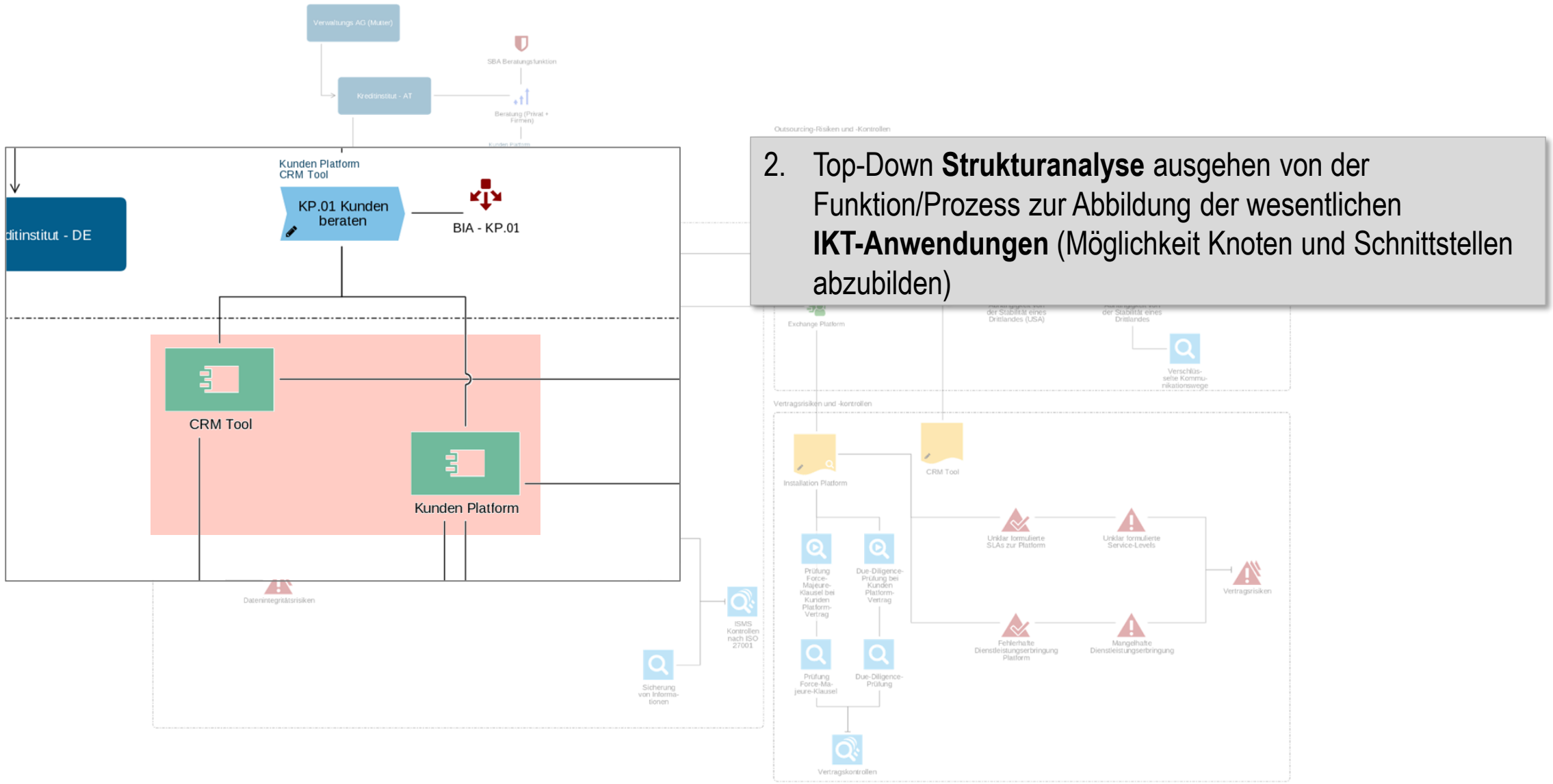
ADOGRC
Governance, Risk & Compliance
by boc-group.com

1. Festlegung des Geltungsbereichs anhand von **Organisationseinheiten** (Finanzeinheiten) und wesentlicher oder kritischer **Funktionen** oder Prozesse



Strukturanalyse von IKT-Anwendungen

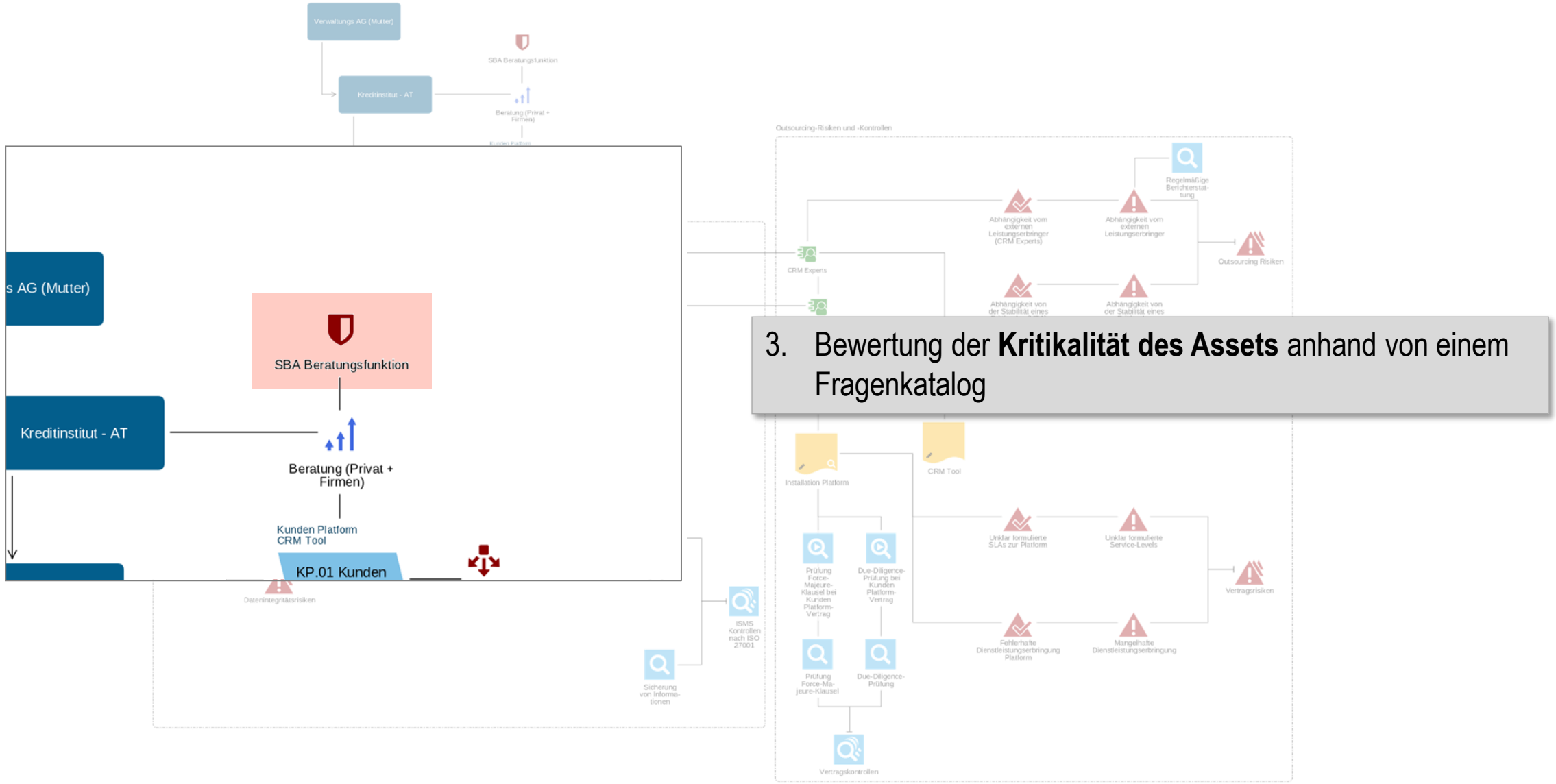
ADOGRC
Governance, Risk & Compliance
by boc-group.com



2. Top-Down **Strukturanalyse** ausgehen von der Funktion/Prozess zur Abbildung der wesentlichen **IKT-Anwendungen** (Möglichkeit Knoten und Schnittstellen abzubilden)

Bewertung Kritikalität des Assets

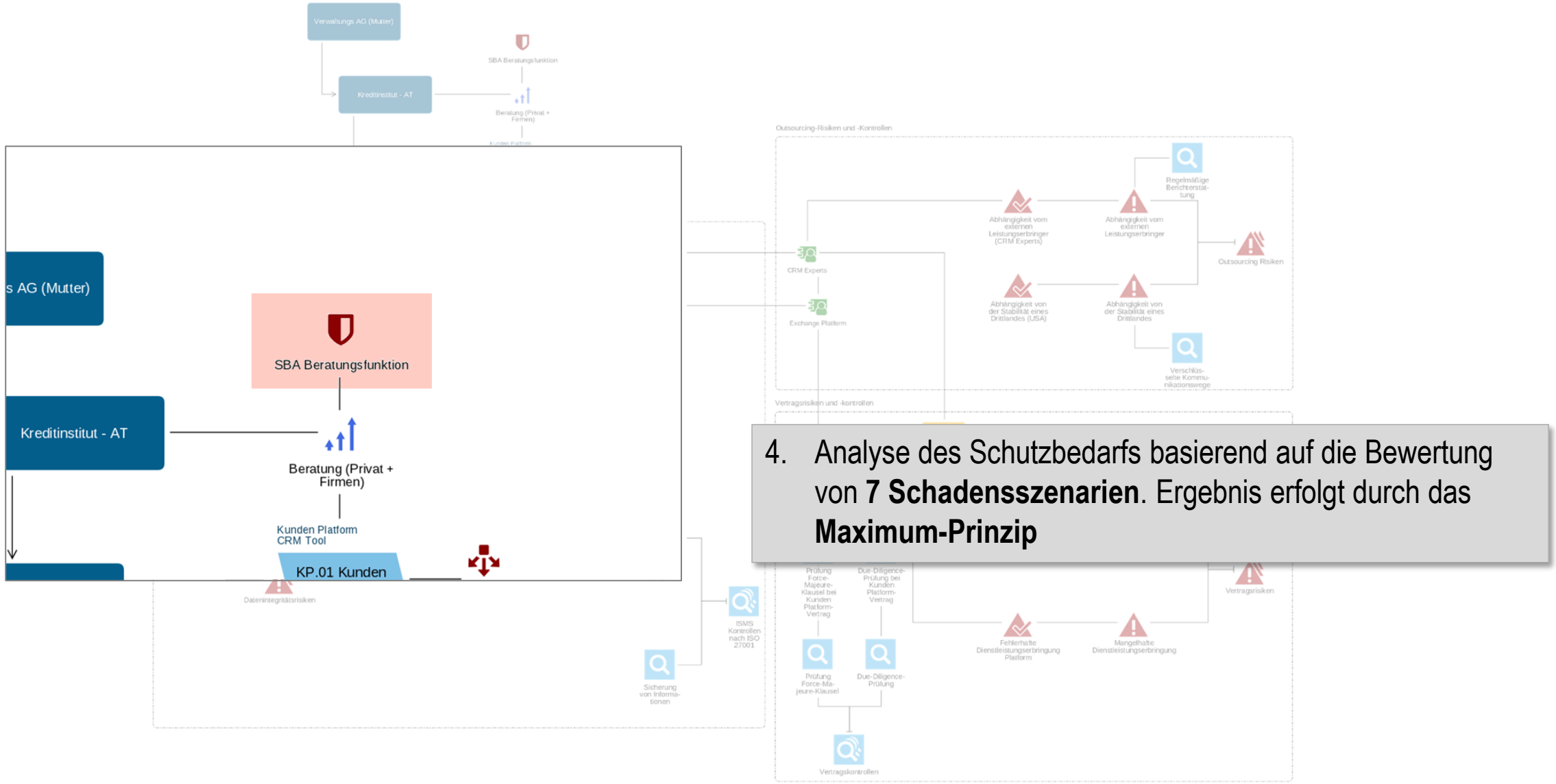
ADOGRC
Governance, Risk & Compliance
by boc-group.com



3. Bewertung der **Kritikalität des Assets** anhand von einem Fragenkatalog

Schutzbedarfsanalyse

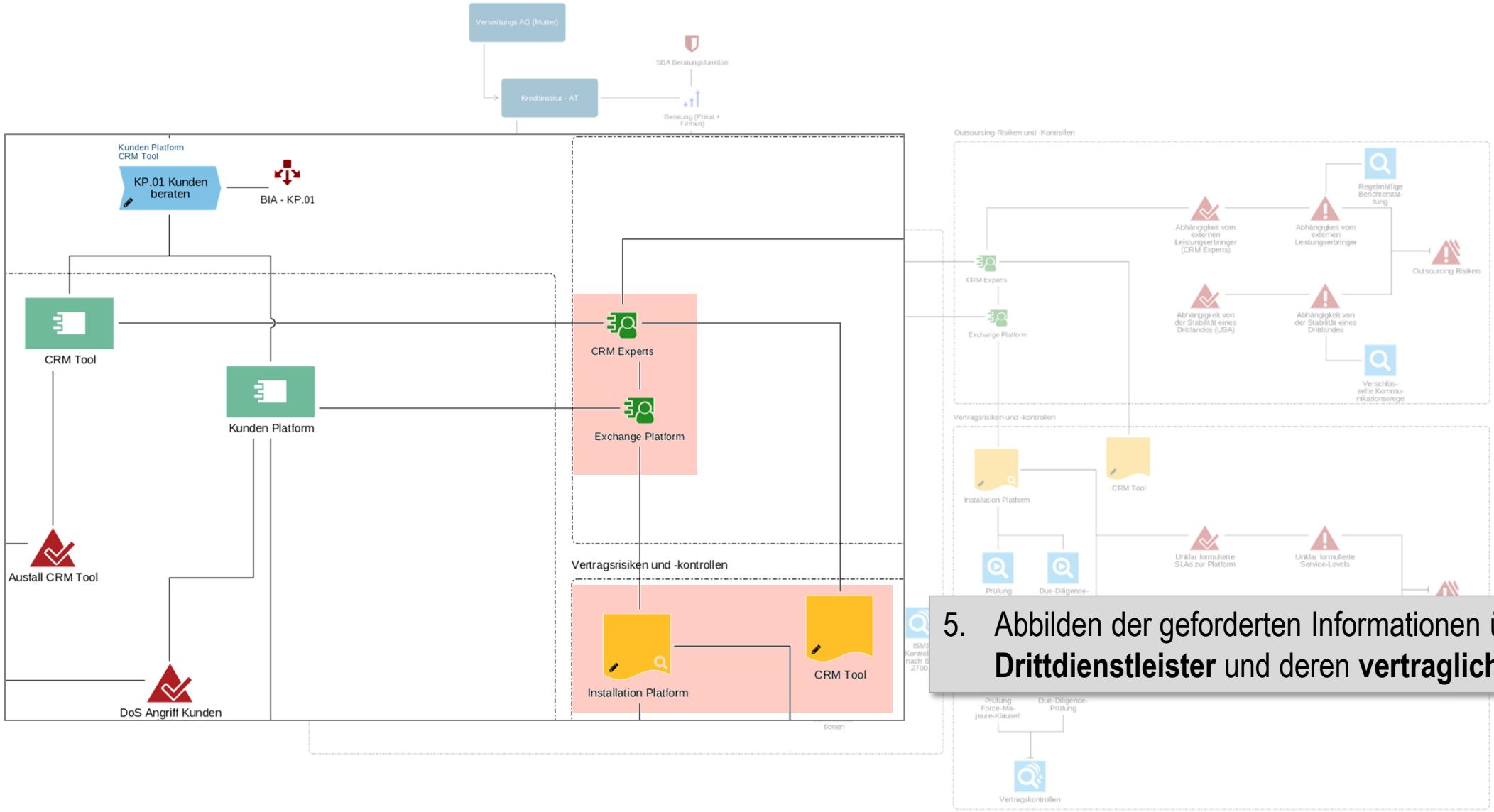
ADOGRC
Governance, Risk & Compliance
by boc-group.com



4. Analyse des Schutzbedarfs basierend auf die Bewertung von **7 Schadensszenarien**. Ergebnis erfolgt durch das **Maximum-Prinzip**

IKT-Drittdienstleister und vertragliche Vereinbarungen

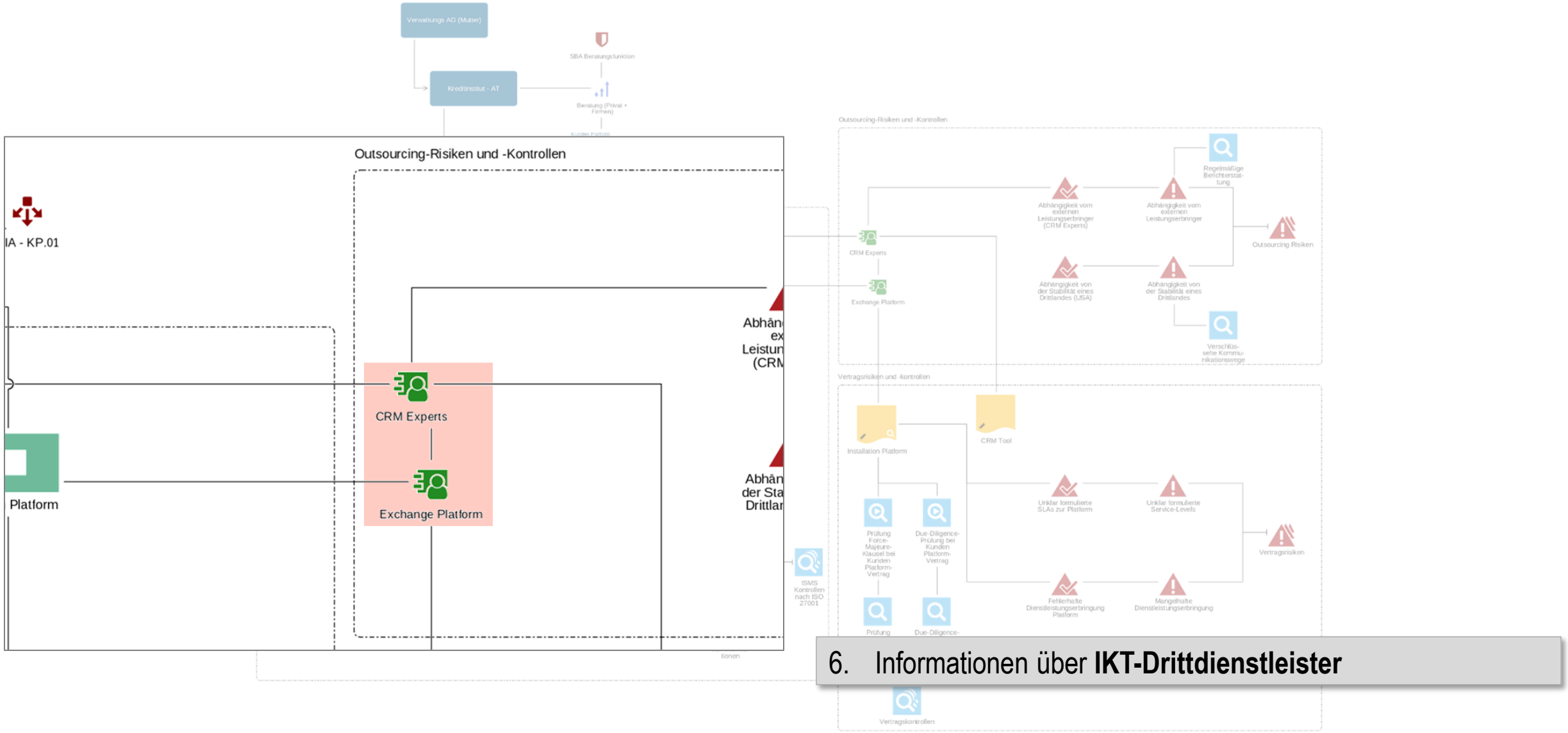
ADOGRC
Governance, Risk & Compliance
by boc-group.com



5. Abbilden der geforderten Informationen über **IKT-Drittdienstleister** und deren **vertragliche Vereinbarungen**

IKT-Drittdienstleister

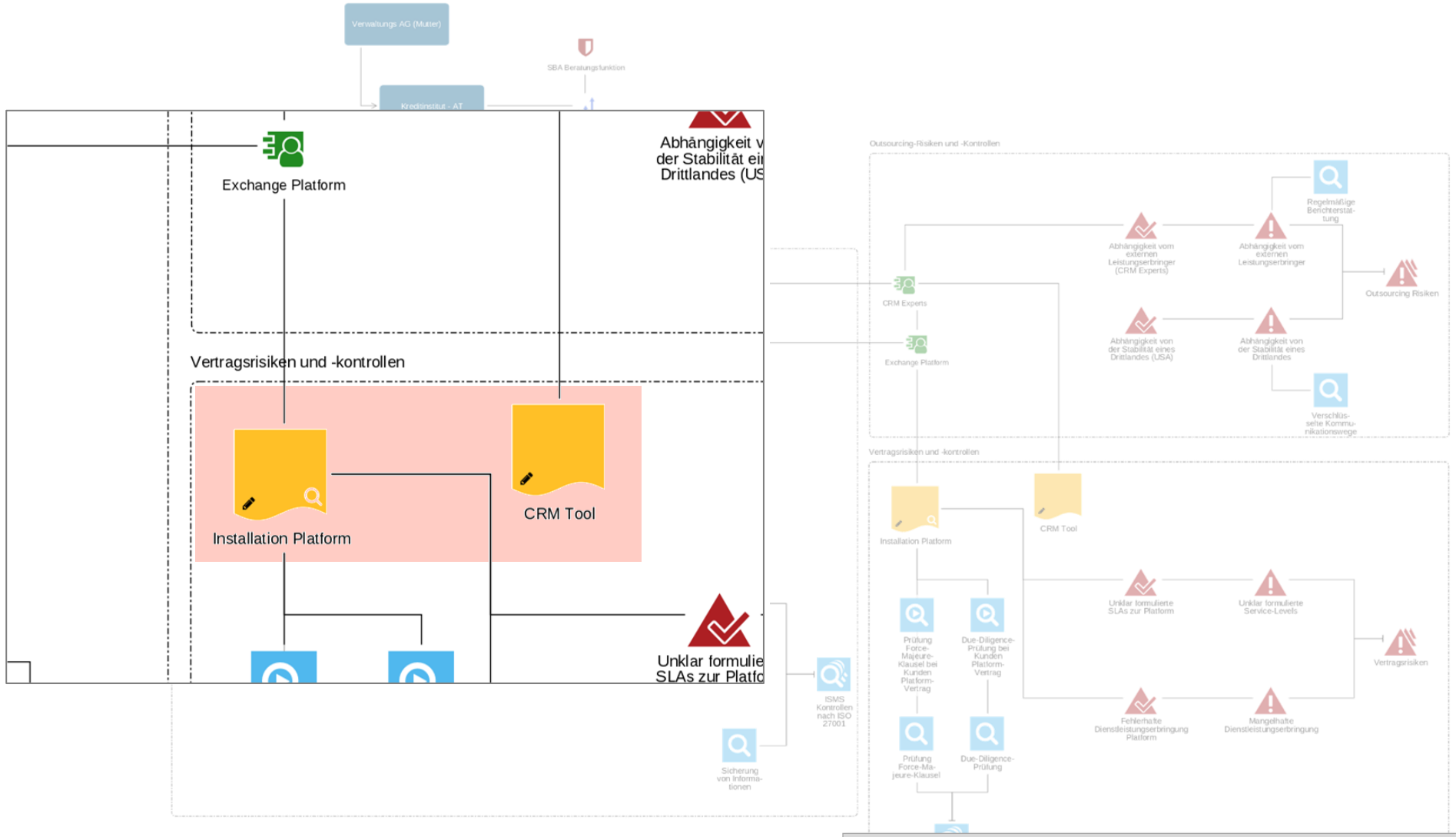
ADOGRC
Governance, Risk & Compliance
by boc-group.com



6. Informationen über **IKT-Drittdienstleister**

Vertragliche Vereinbarung

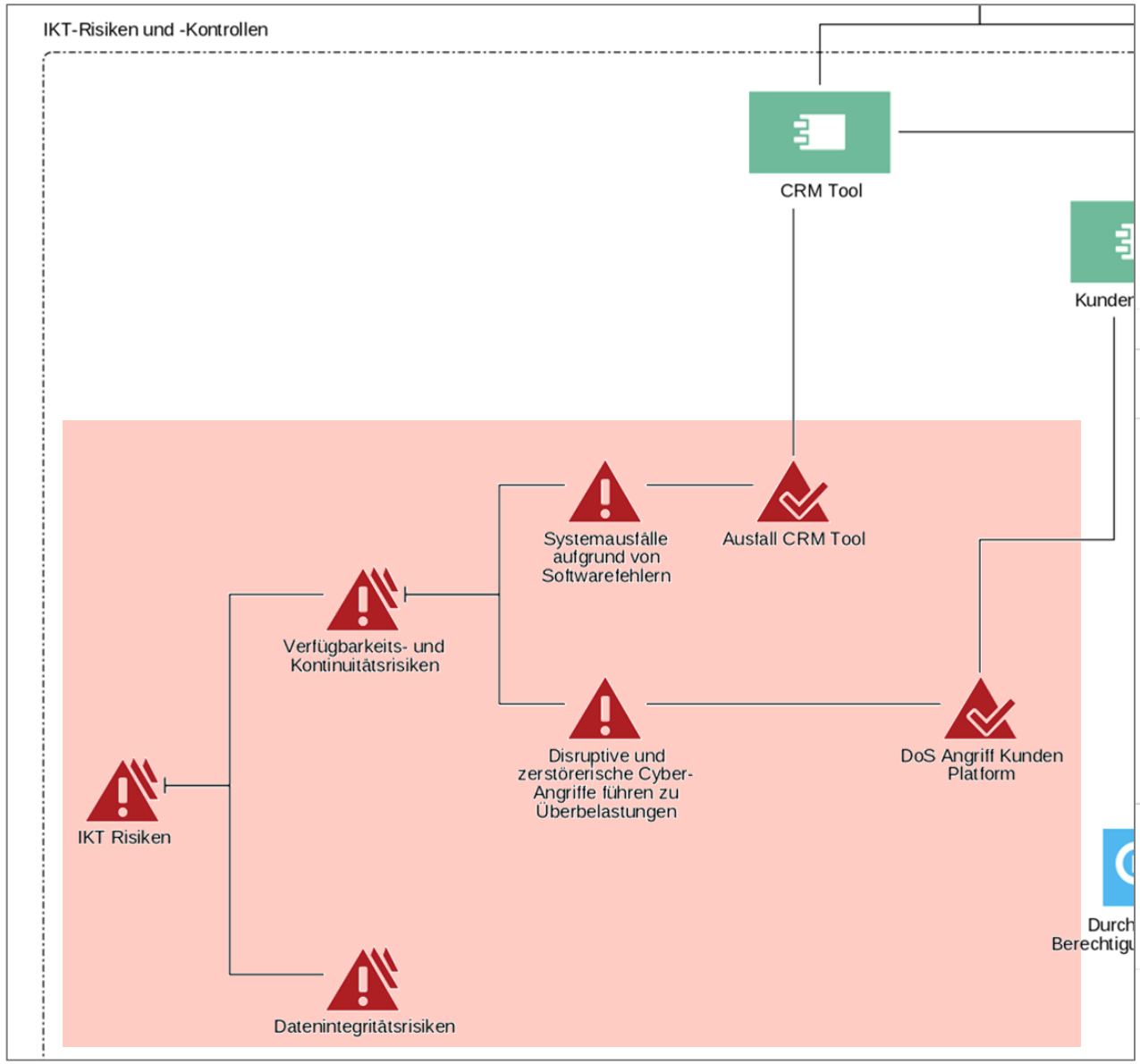
ADOGRC
Governance, Risk & Compliance
by boc-group.com



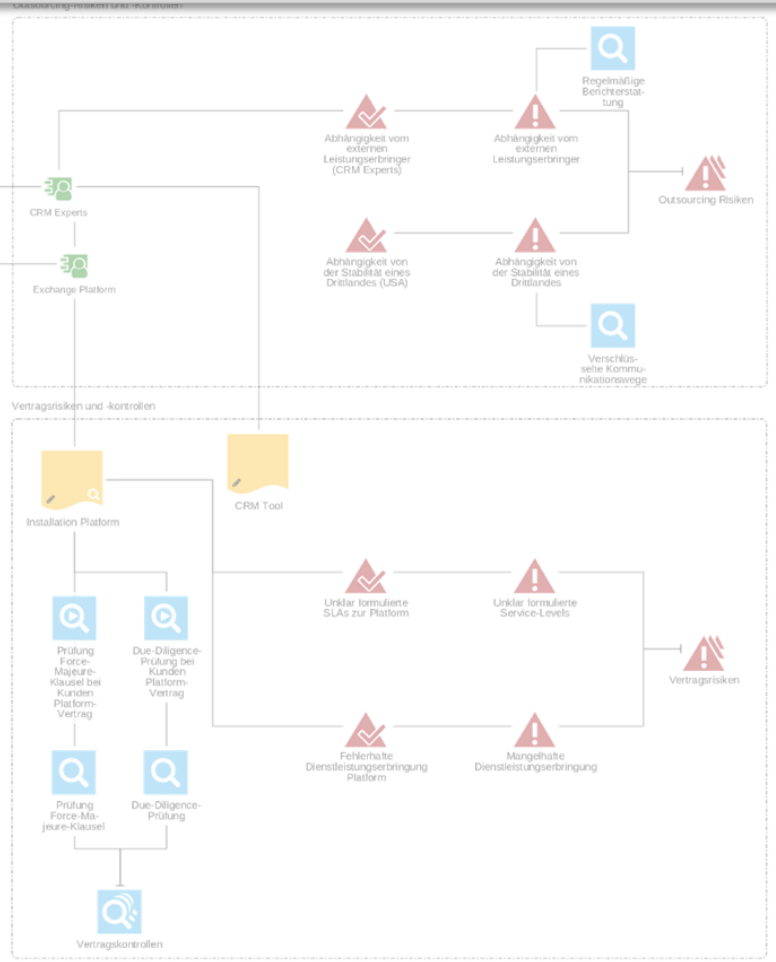
7. Informationen über **vertragliche Vereinbarungen**

IKT-Risikomanagement

ADOGRC
Governance, Risk & Compliance
by boc-group.com

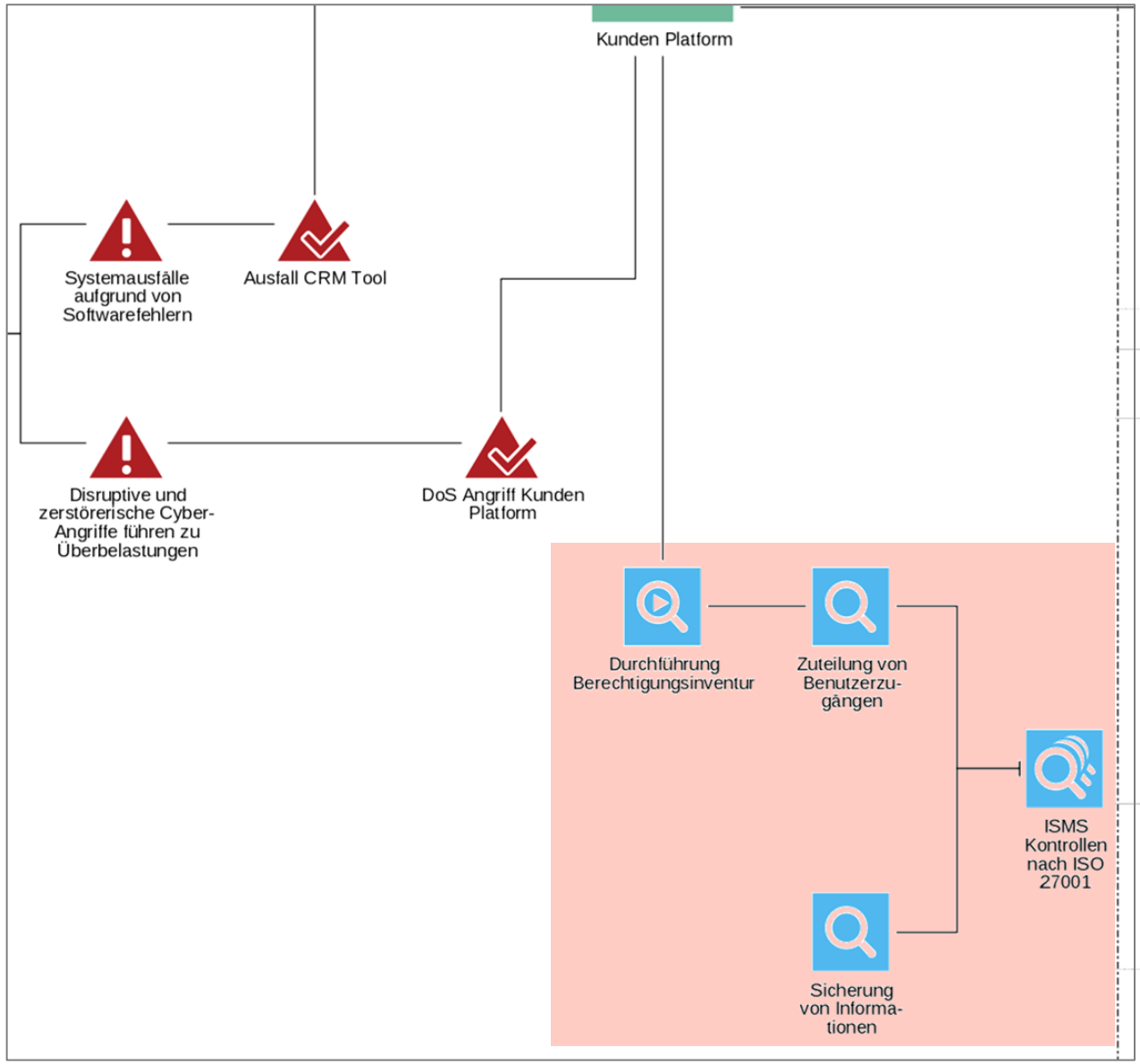


8. Mit den bestehende Risikoklassen (**Stammdaten und Bewertung**) und den zusätzlichen Informationen wird das **Risikomanagement** DORA-konform erweitert

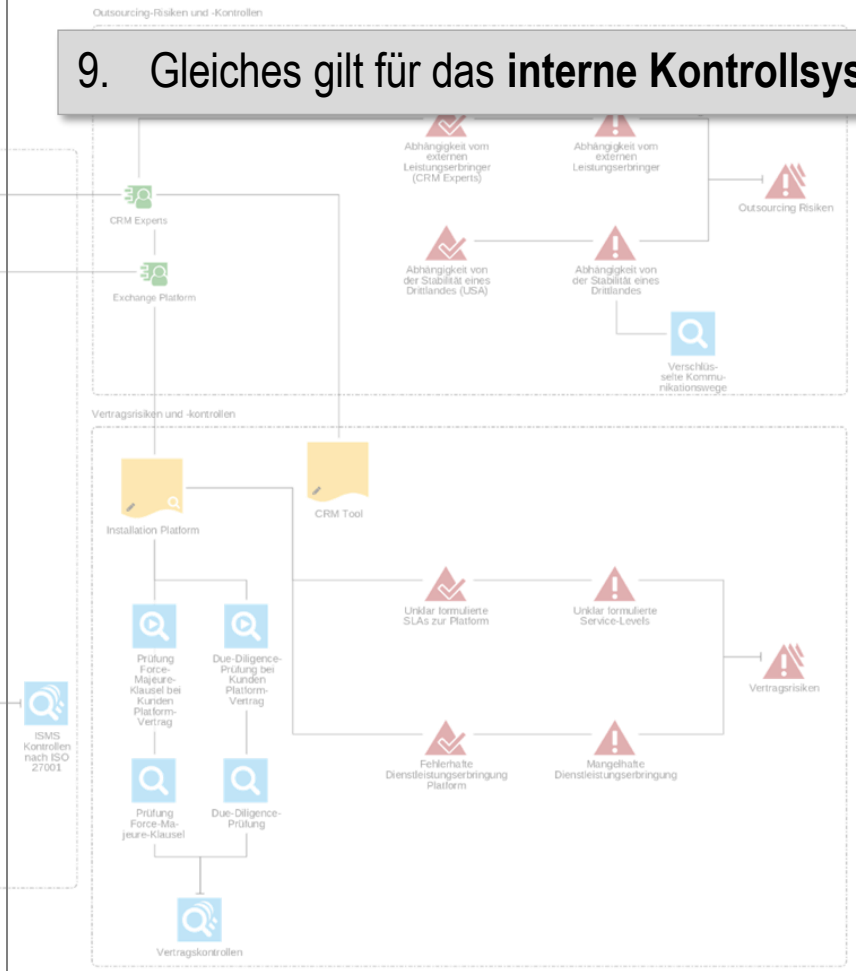


IKS-Ergänzung durch IKT-Kontrollobjekte

ADOGRC
Governance, Risk & Compliance
by boc-group.com

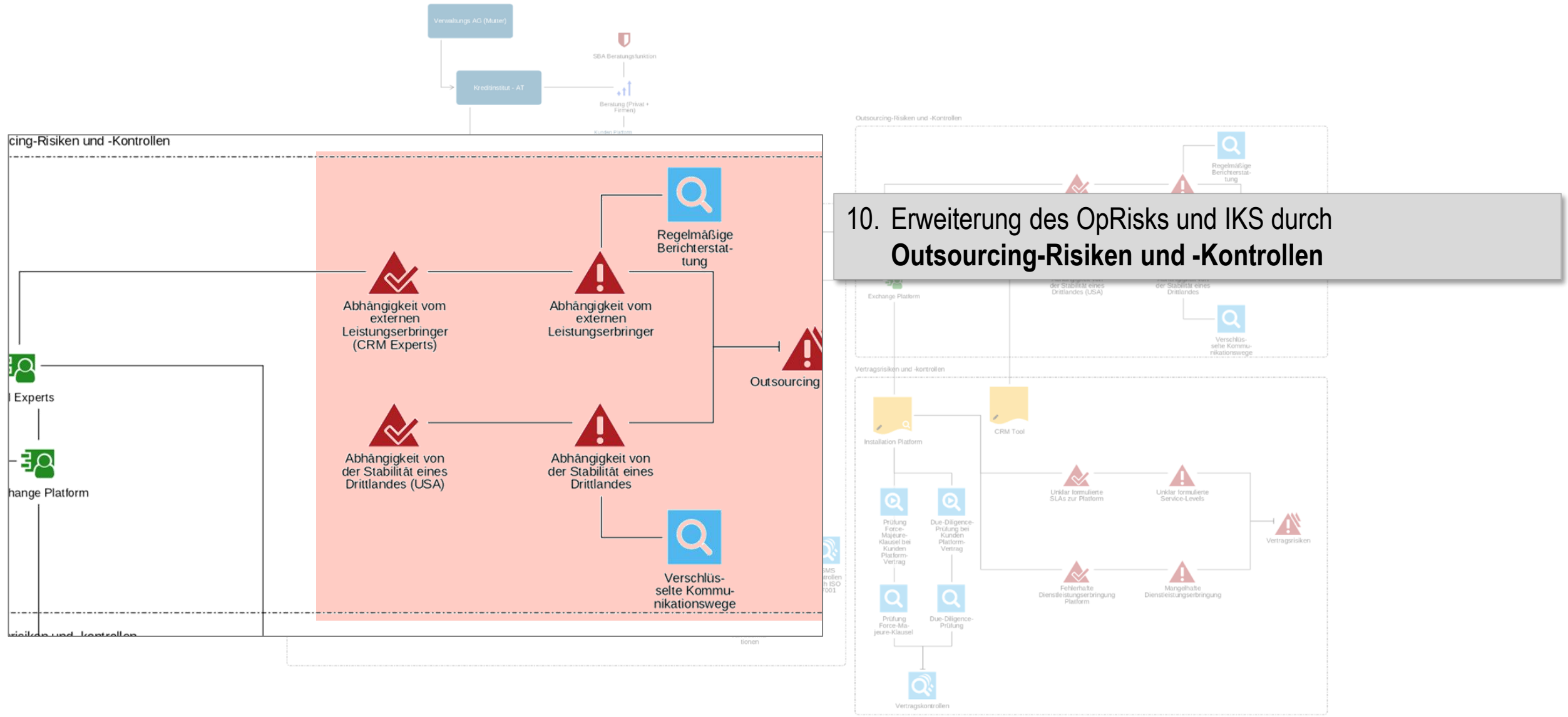


9. Gleiches gilt für das **interne Kontrollsystem (IKS)**



Outsourcing-Risiken und -Kontrollen

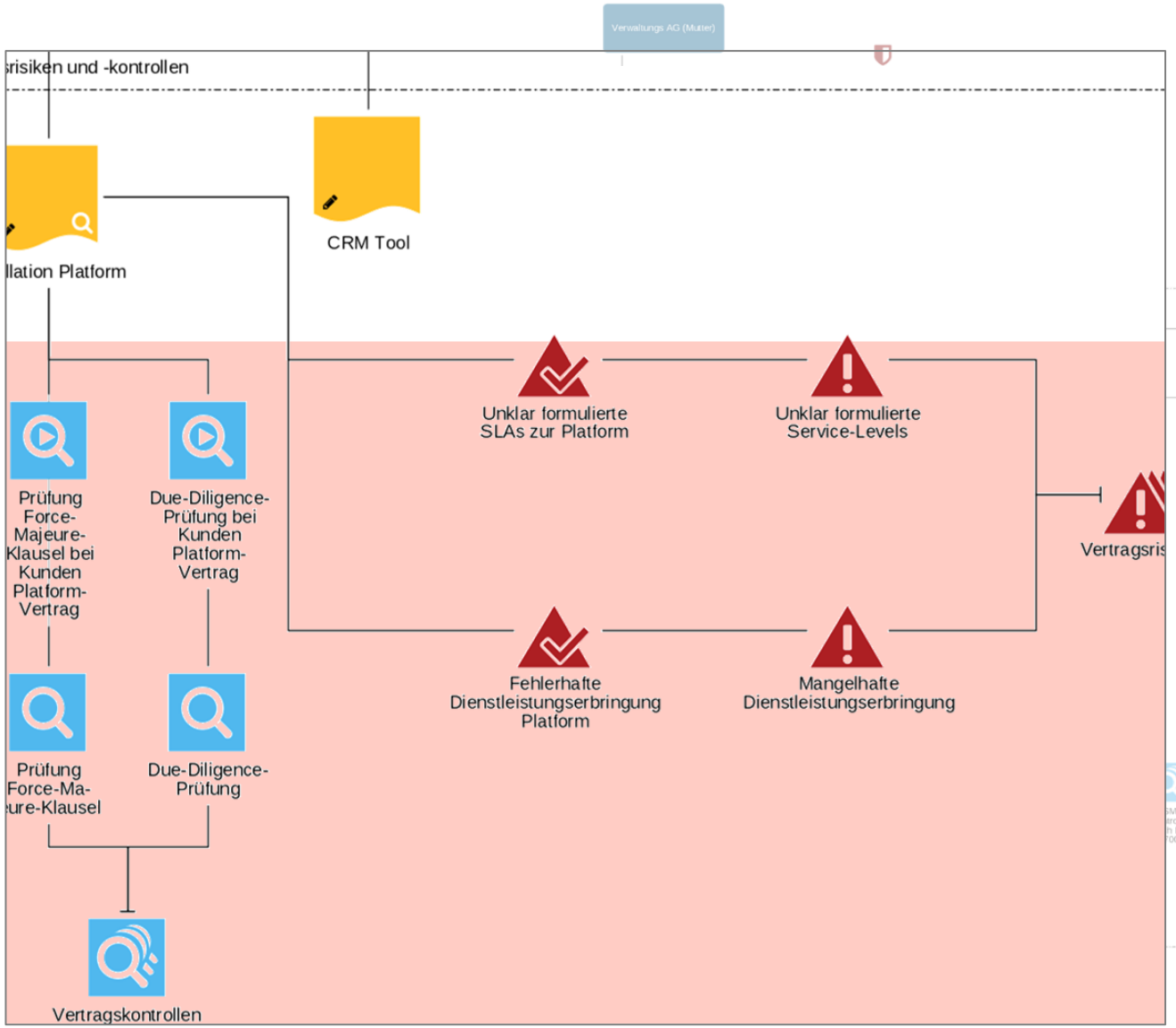
ADOGRC
Governance, Risk & Compliance
by boc-group.com

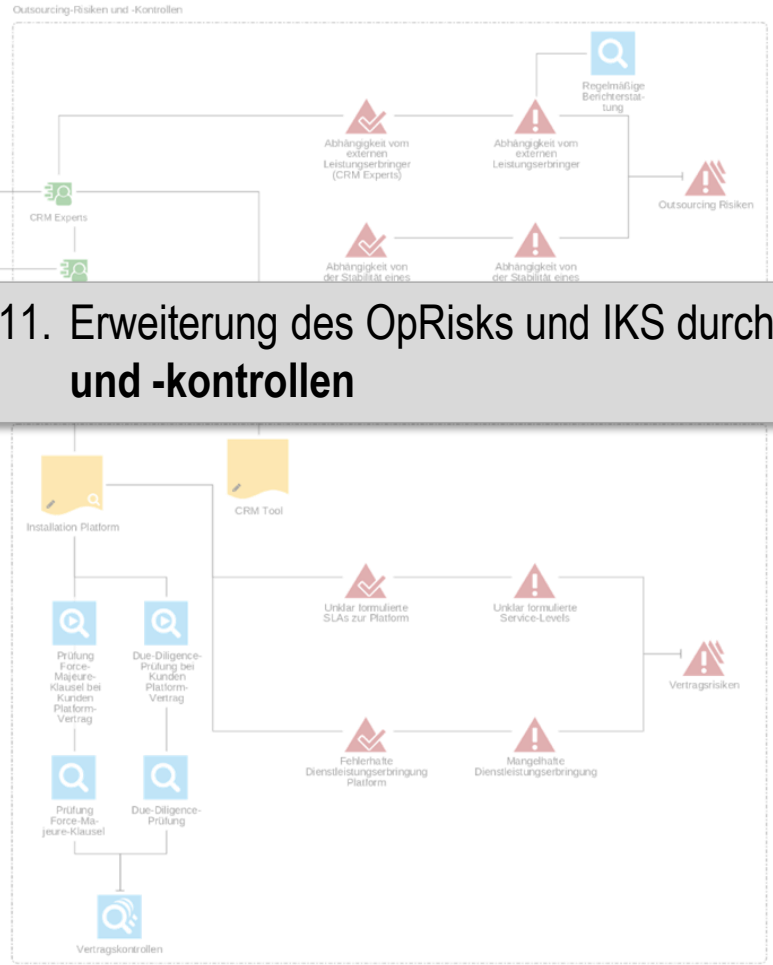


10. Erweiterung des OpRisks und IKS durch **Outsourcing-Risiken und -Kontrollen**

Vertragsrisiken und -kontrollen

ADOGRC
Governance, Risk & Compliance
by boc-group.com





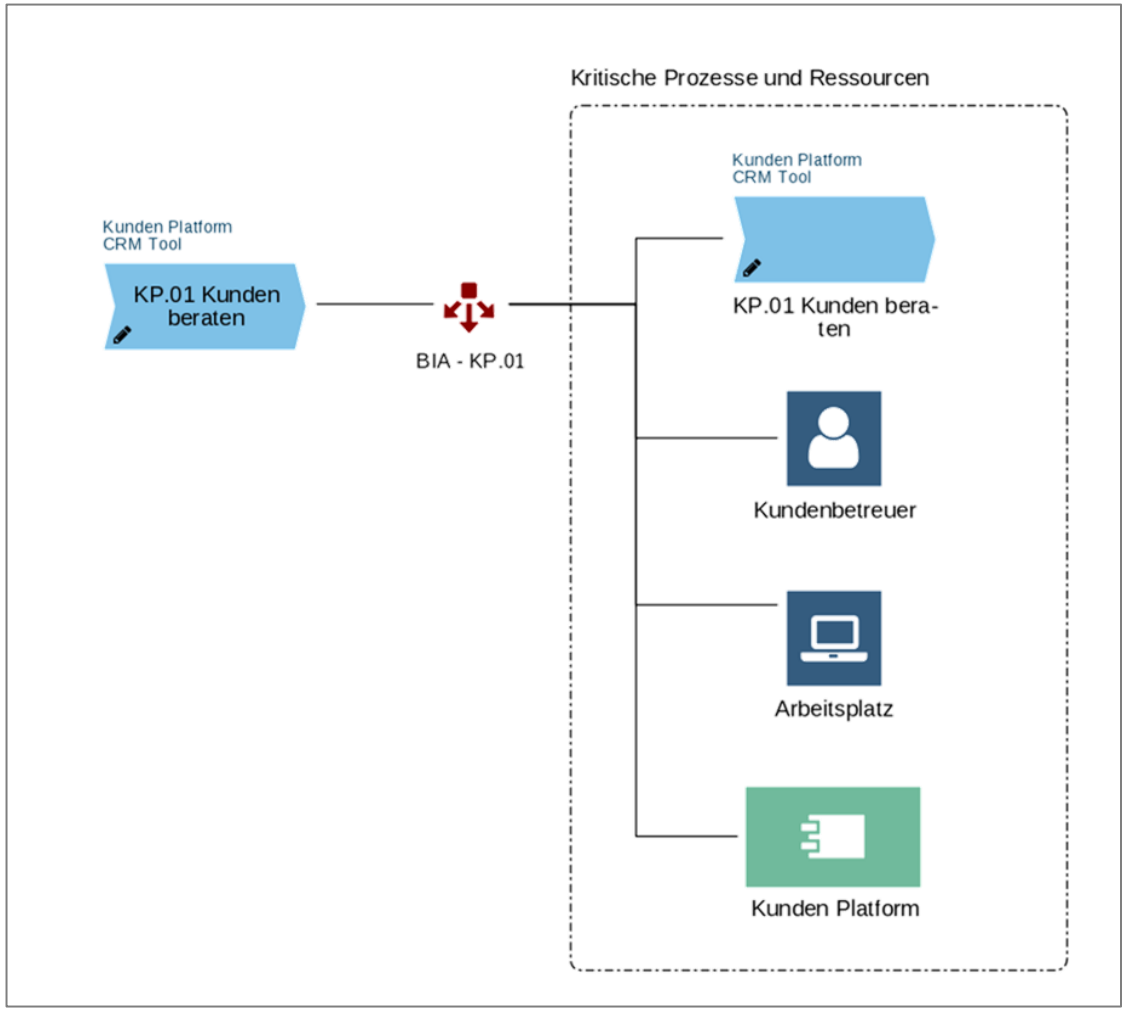
11. Erweiterung des OpRisks und IKS durch **Vertragsrisiken und -kontrollen**

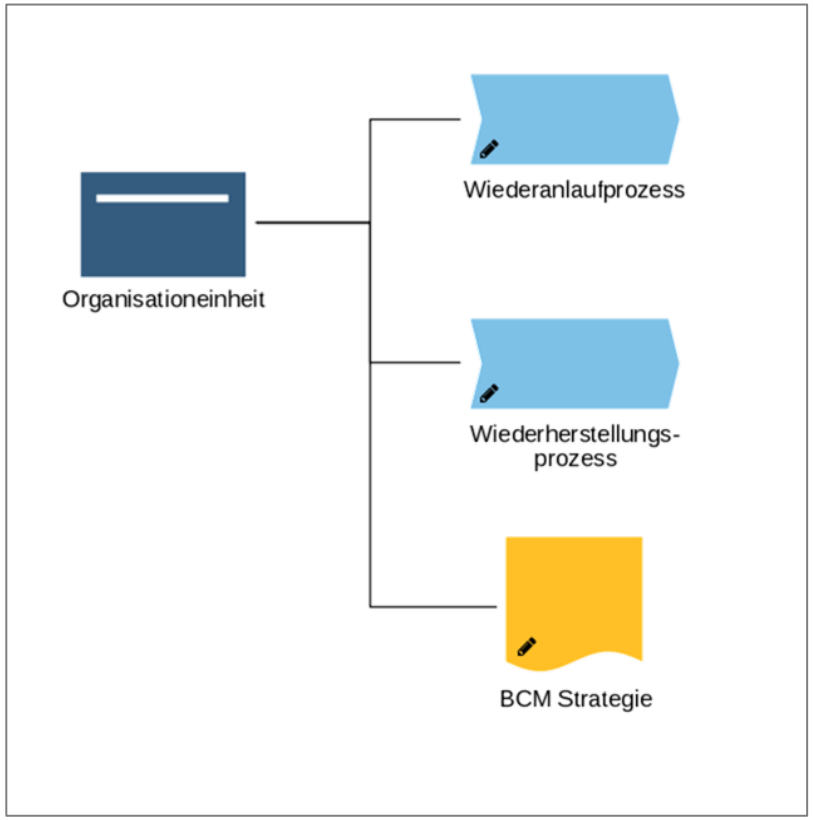
Business Continuity Management

ADOGRC
Governance, Risk & Compliance

BCM als Teil der DORA Lösung

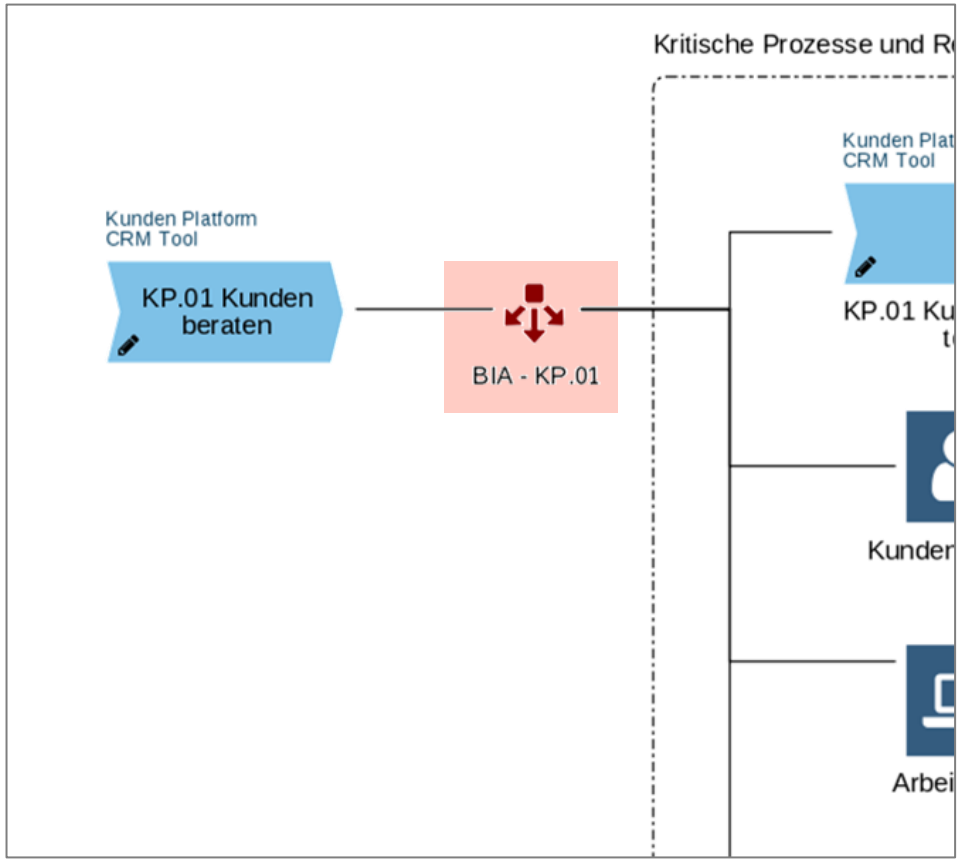
ADOGRC
Governance, Risk & Compliance
by boc-group.com





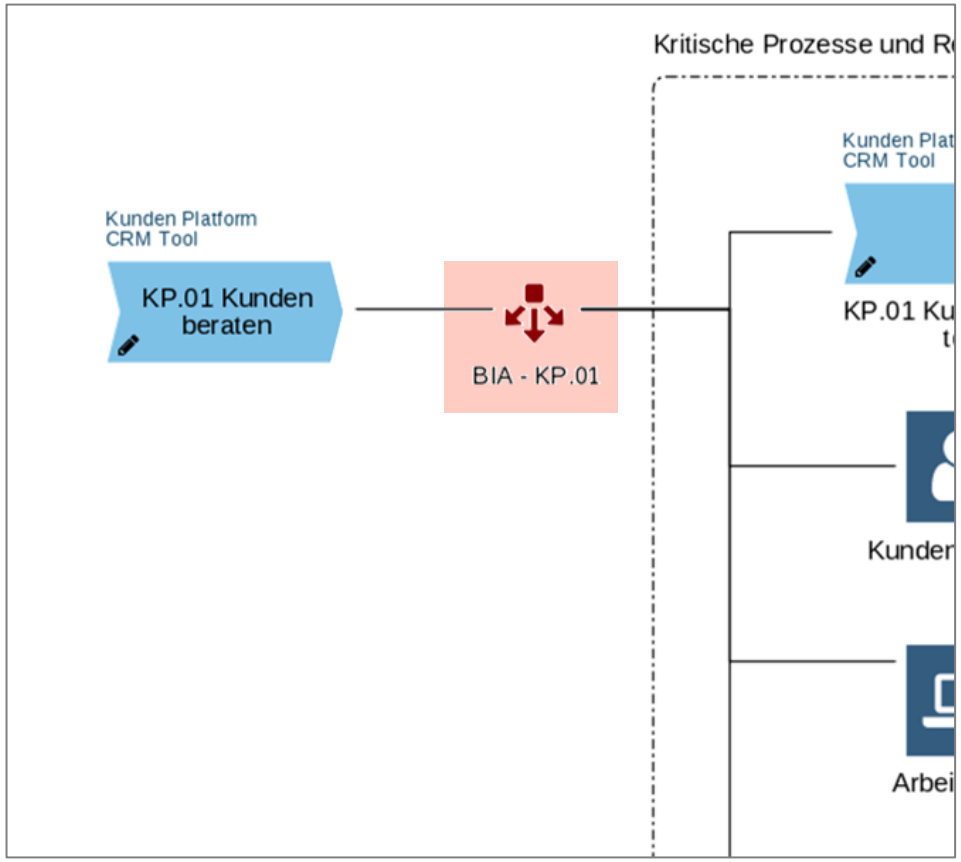
Business Impact Analyse

ADOGRC
Governance, Risk & Compliance
by boc-group.com



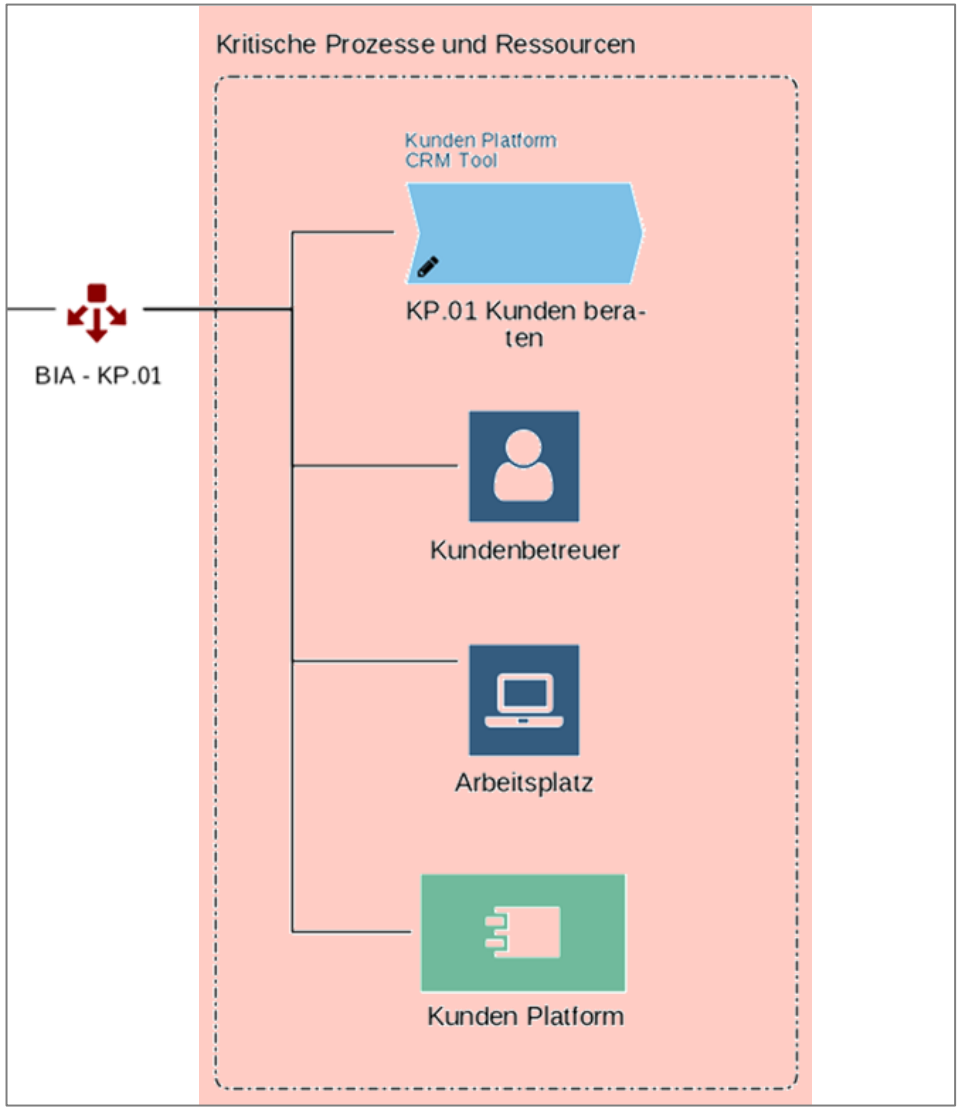
1. Analyse basiert auf der Bewertung von **5 Auswirkungskategorien** über **5 Zeitdimensionen**. Ergebnis erfolgt durch das **Maximum-Prinzip**

Kenngrößen in der BIA definieren



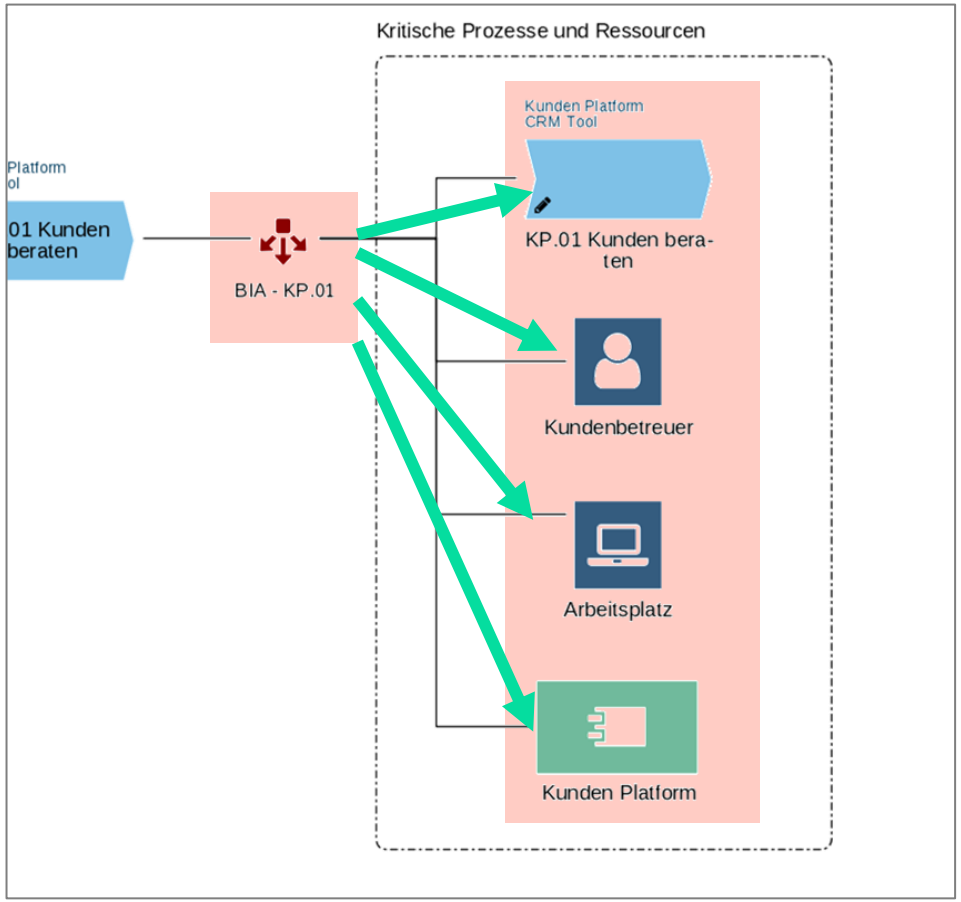
2. Festlegung der Kennzahlen **maximal tolerierbare Ausfallzeit**, **geforderte Wiederanlaufzeit** und **maximal zulässiger Datenverlust**

Kritische Elemente für den Notbetrieb



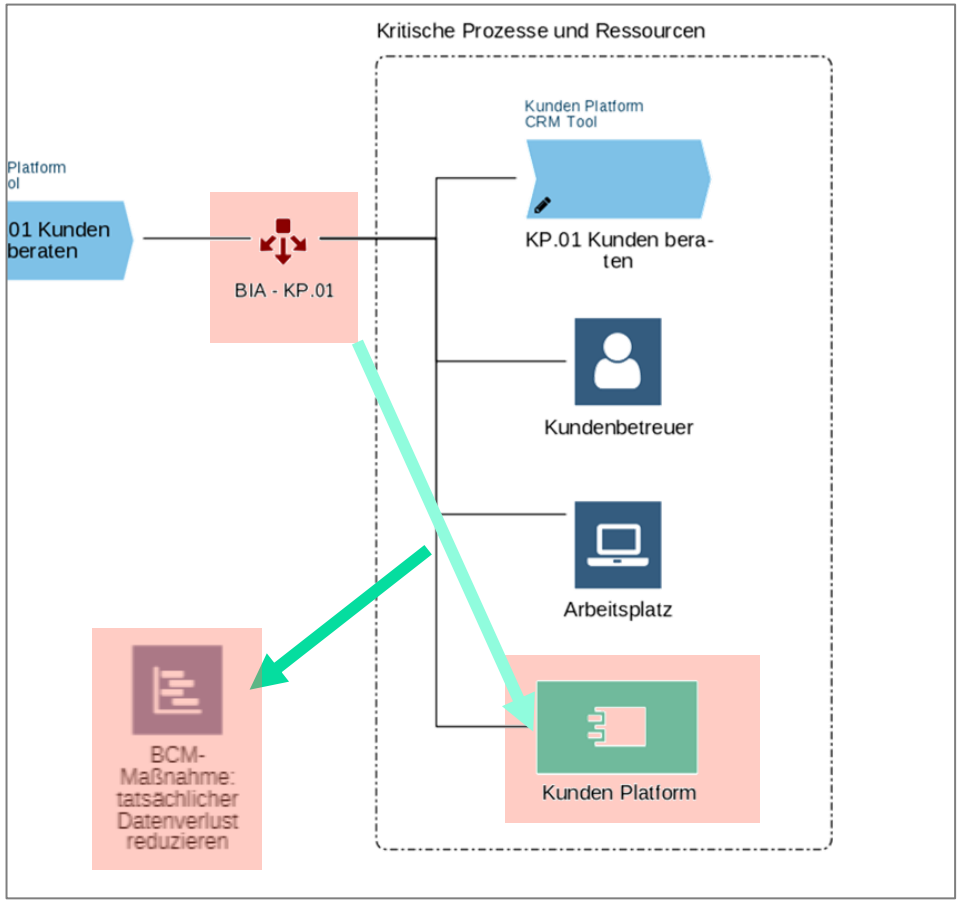
3. **Kritische Prozesse** und **Ressourcen** für den Notbetrieb können **definiert** werden (informationsbasierte und nicht-informationsbasierte Assets)

Soll-Ist-Vergleich



4. **Soll-Ist-Vergleich** zwischen maximal tolerierbare Ausfallzeit, geforderte Wiederanlaufzeit und maximal zulässiger Datenverlust mit den **tatsächlichen** Werten für **Ausfallzeit**, **Wiederanlaufzeit** und **Datenverlust** definiert in den **kritischen Prozessen** und **Ressourcen**

Maßnahmen bei Lücken

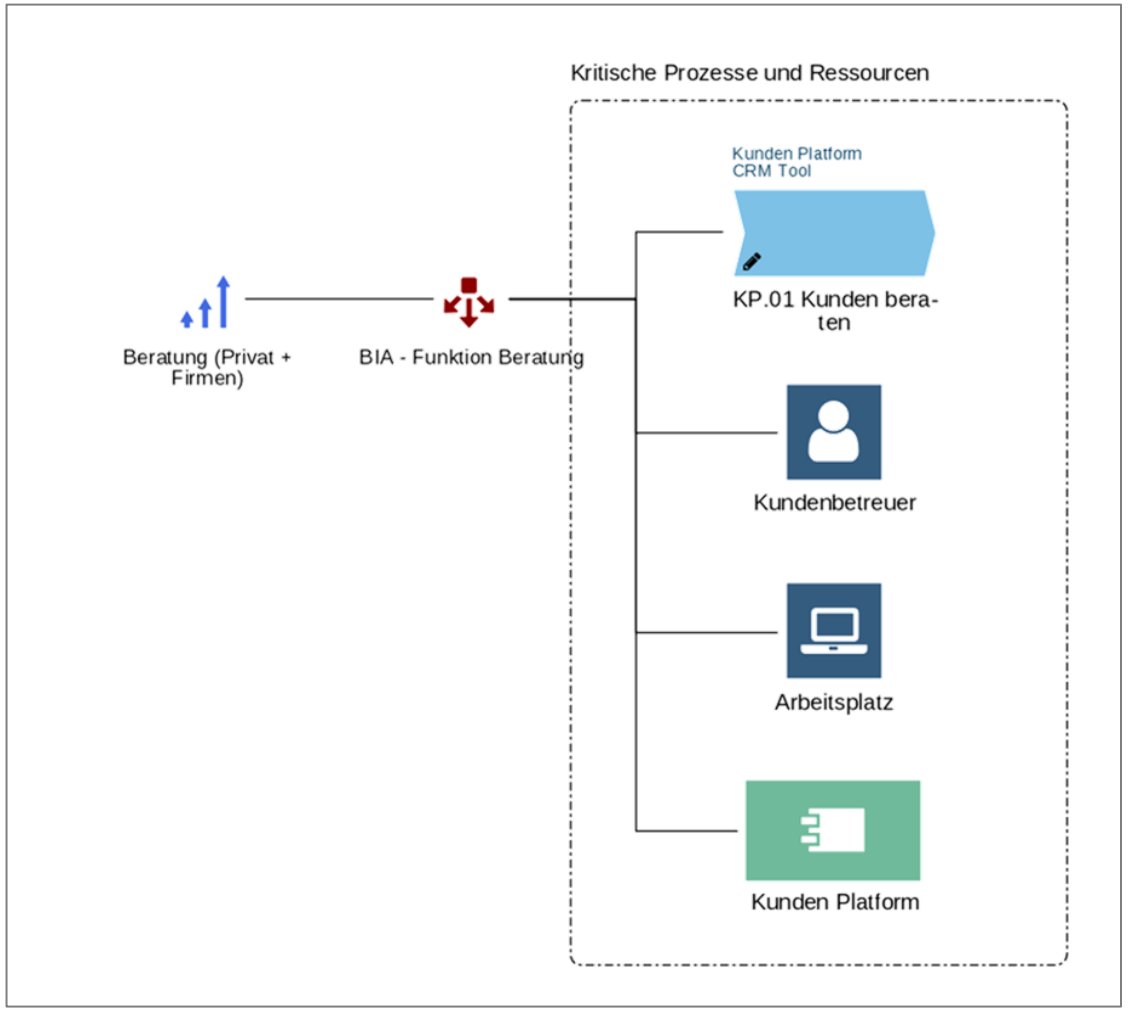


5. Nach Identifizierung von Lücken, **Maßnahmen** für die Verbesserung anlegen

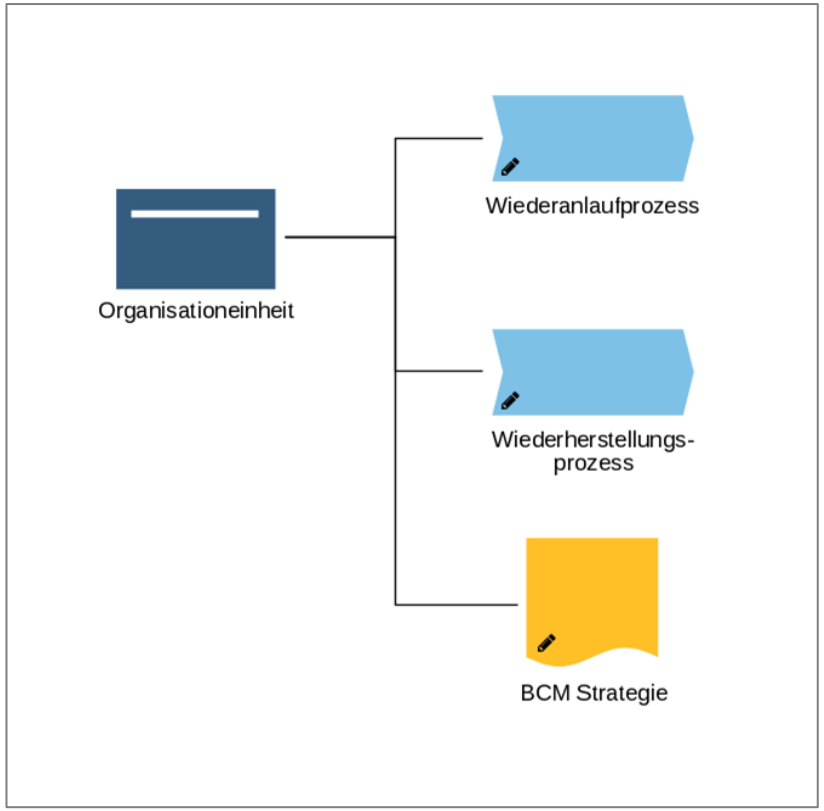
Gleiches Prinzip für Funktionen

ADOGRC
Governance, Risk & Compliance
by boc-group.com

6. Das Konzept gilt auch für **Funktionen**



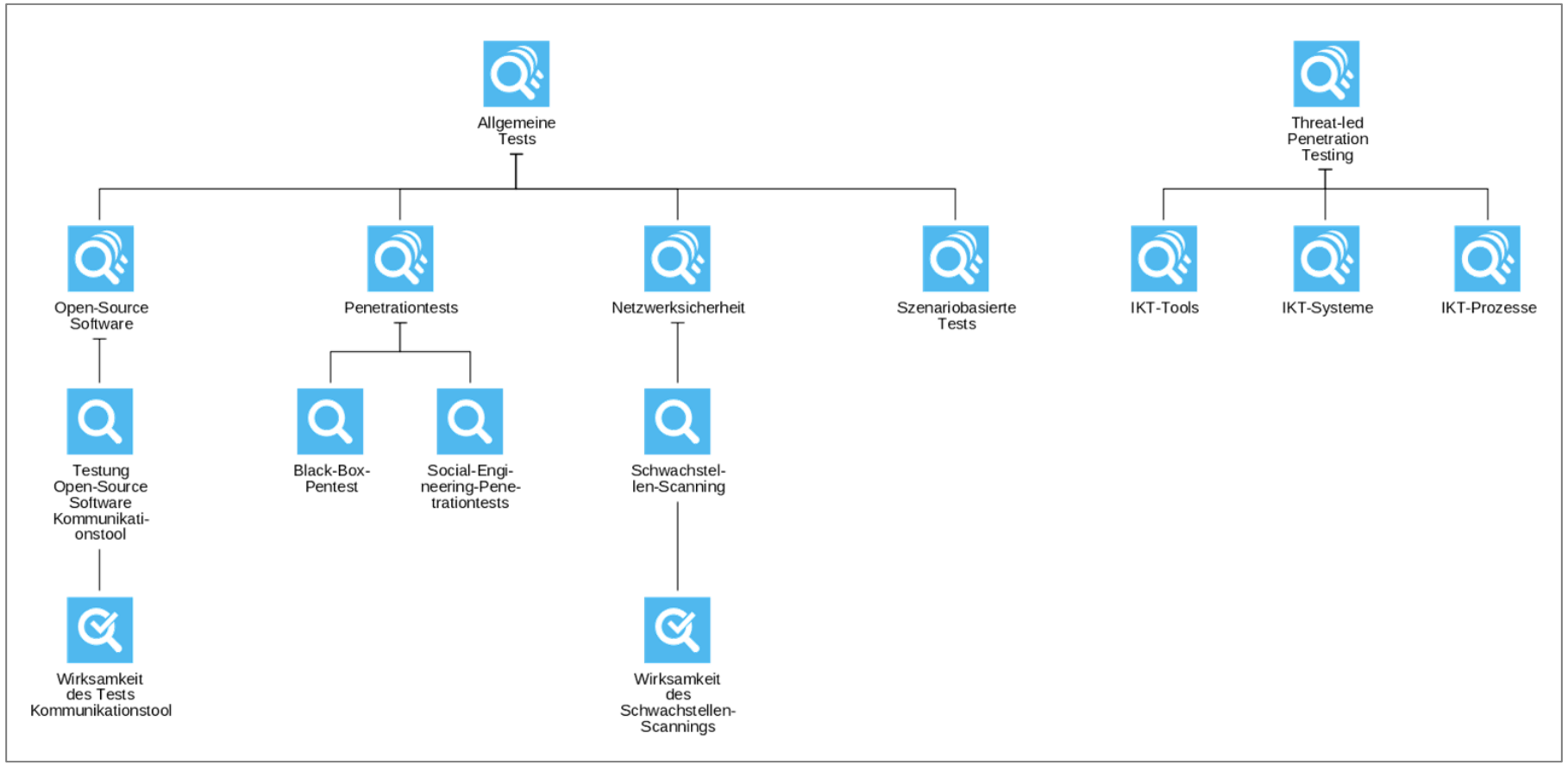
Planungen auf OE-Ebene



7. Planung des **Wiederanlaufs- und Wiederherstellungsprozess** findet auf OE-Ebene statt, genauso wie die Definition der **BCM-Strategie**

Testen der digitalen operationellen Resilienz

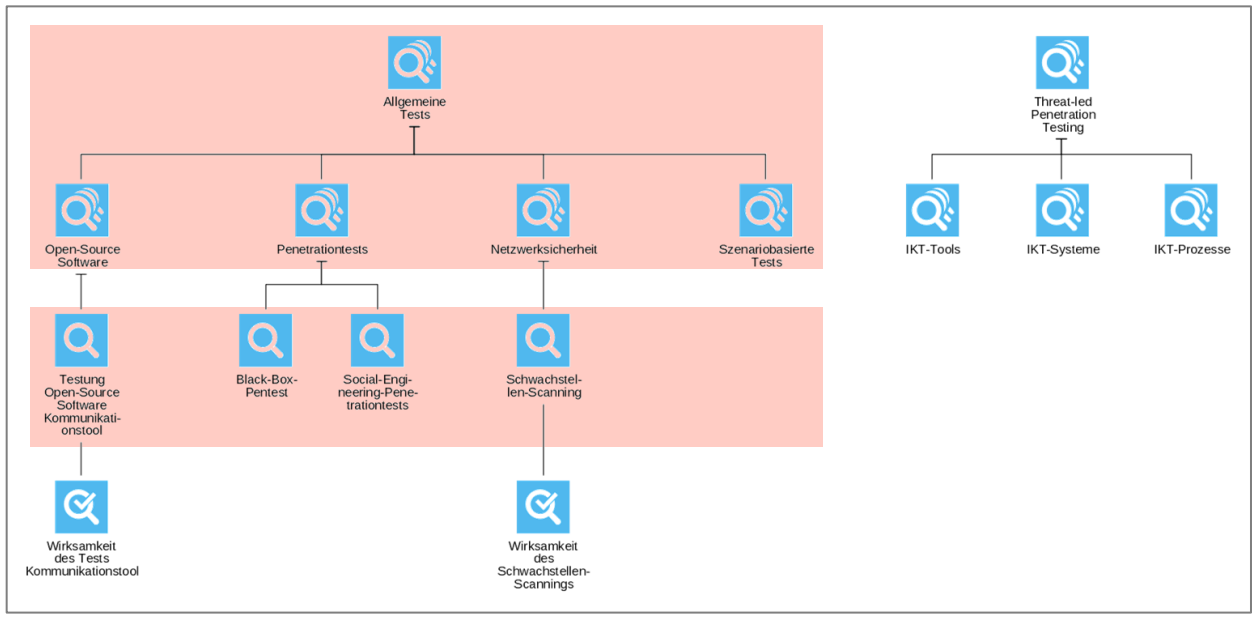
ADOGRC
Governance, Risk & Compliance
by boc-group.com



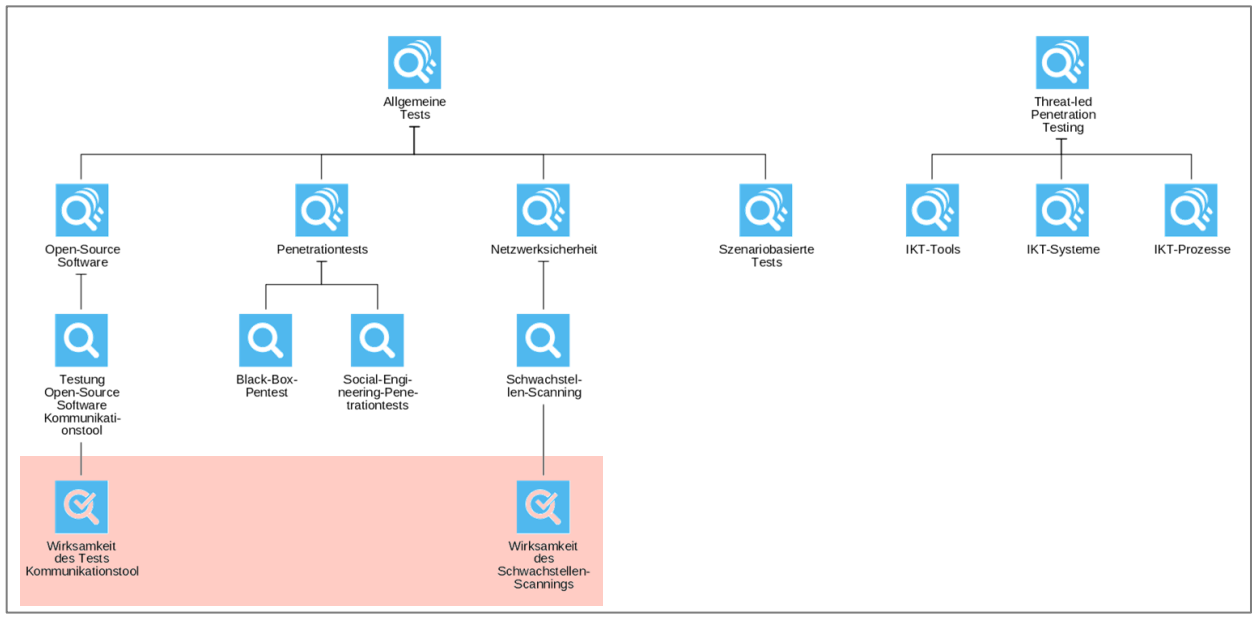
Teststrategie

ADOGRC
Governance, Risk & Compliance
by boc-group.com

1. Über **Kontrollgruppen** und **Kontrollen** besteht die Möglichkeit das **Testkonzept** abzubilden

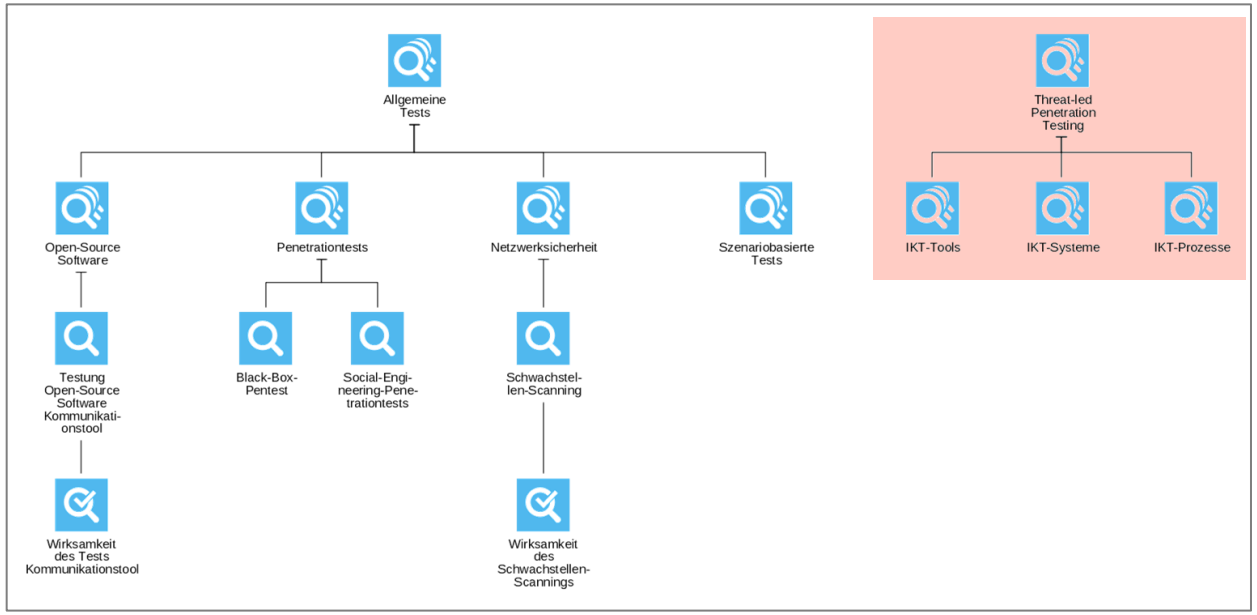


Wirksamkeit der Tests



2. Mit dem **Kontrolltest** wird die **Wirksamkeit des Tests** überprüft und dokumentiert

Threat-led Penetration Testing



3. Falls erforderlich kann das **TLPT** nach dem gleichen Prinzip abgebildet und bewertet werden

DORA-Reporting

ADOGRC
Governance, Risk & Compliance
by boc-group.com

Verfügbare REST-XLS_Reports

RT.01.

- RT.01.01: Entity maintaining the register of information
- RT.01.02: List of entities within the scope of the register of information
- RT.01.03: List of branches

RT.02.

- RT.02.01: Contractual arrangements – General Information
- RT.02.02: Contractual arrangements – Specific information
- RT.02.03: List of intra-group contractual arrangements

RT.03.

- RT.03.01: Entities signing the Contractual arrangements for receiving ICT service(s) or on behalf of the entities making use of the ICT service(s)
- ICT third-party service providers signing the Contractual arrangements for providing ICT service(s)
- RT.03.03: Entities signing the Contractual arrangements for provid

RT.04.

- RT.04.01: Entities making use of the ICT services

RT.05.

- RT.05.01: ICT third-party service provider
- RT.05.02: ICT service supply chains

RT.06.

- RT.06.01: Functions identification

RT.07.

- RT.07.01: Assessment of the ICT services
- RT.99.01: Definitions from Entities making use of the ICT Services

D	E	F	G	H
Identification code of the ICT third-party service provider	Start date of the contractual arrangement Misc	Type of code to identify the ICT third-party service provider	Function identifier	Type of ICT services
AT_ATU56497348	01.01.2024	Country Code_VAT	F2	eba_TA:S15
AT_ATU56497348	01.01.2024	Country Code_VAT	F2	eba_TA:S13
AT_ATU56497348	01.01.2024	Country Code_VAT	F4	eba_TA:S13
AT_ATU56497348	01.01.2024	Country Code_VAT	F3	eba_TA:S13
AT_ATU56497348	01.01.2024	Country Code_VAT	F4	eba_TA:S15
AT_ATU56497348	01.01.2024	Country Code_VAT	F3	eba_TA:S15
AT_ATU56497348	01.01.2024	Country Code_VAT	F1	eba_TA:S15
AT_ATU56497348	01.01.2024	Country Code_VAT	F1	eba_TA:S13
AT_ATU56497348	02.06.2024	Country Code_VAT	Not applicable	eba_TA:S13
GB_FC025288	04.02.2024	Country Code_CRN	F10	eba_TA:S11
GB_FC025288	04.02.2024	Country Code_CRN	F9	eba_TA:S11
GB_FC025288	04.02.2024	Country Code_CRN	F8	eba_TA:S11
GB_FC025288	04.02.2024	Country Code_CRN	F7	eba_TA:S11
GB_FC025288	04.02.2024	Country Code_CRN	F6	eba_TA:S11
GB_FC025288	04.02.2024	Country Code_CRN	F5	eba_TA:S11
GB_FC025288	04.02.2024	Country Code_CRN	F7	eba_TA:S04
GB_FC025288	04.02.2024	Country Code_CRN	F9	eba_TA:S04
GB_FC025288	04.02.2024	Country Code_CRN	F8	eba_TA:S04
GB_FC025288	04.02.2024	Country Code_CRN	F10	eba_TA:S04
GB_FC025288	04.02.2024	Country Code_CRN	F6	eba_TA:S04
GB_FC025288	04.02.2024	Country Code_CRN	F5	eba_TA:S04
GB_FC025288	01.07.2024	Country Code_CRN	Not applicable	eba_TA:S15

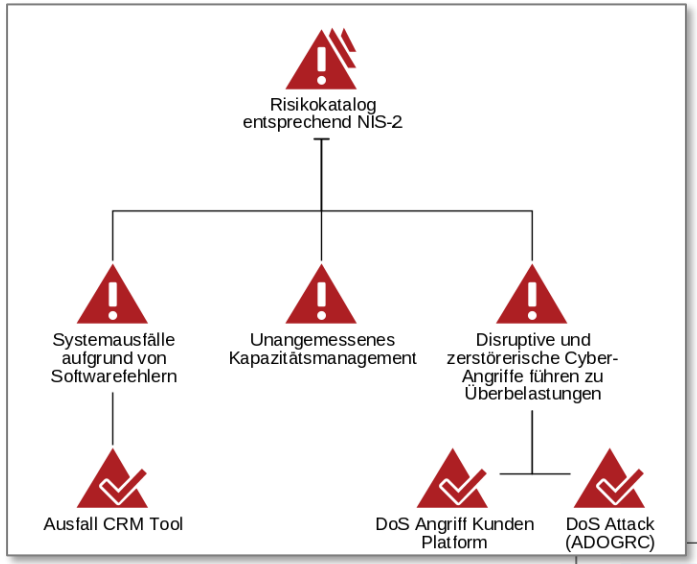
Ausblick für NIS-2

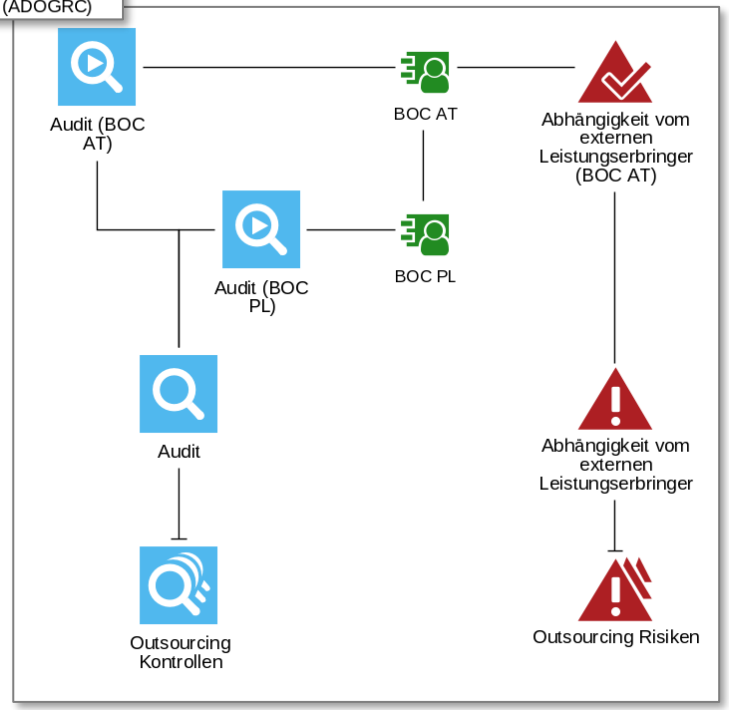
ADOGRC
Governance, Risk & Compliance

NIS2-Richtline

ADOGRC
Governance, Risk & Compliance
by boc-group.com

- Risikoanalyse und Konzept für Sicherheit der Informationssysteme
- Management von Sicherheitsvorfällen
- Sicherheit in der Lieferkette
- Business Continuity und Krisenmanagement
- Sicherheitsmaßnahmen bei Erwerb/Entwicklung/Wartung von IKT-Anwendungen
- Richtlinien für Cyberhygiene, Zugriffskontrolle und Kryptographie

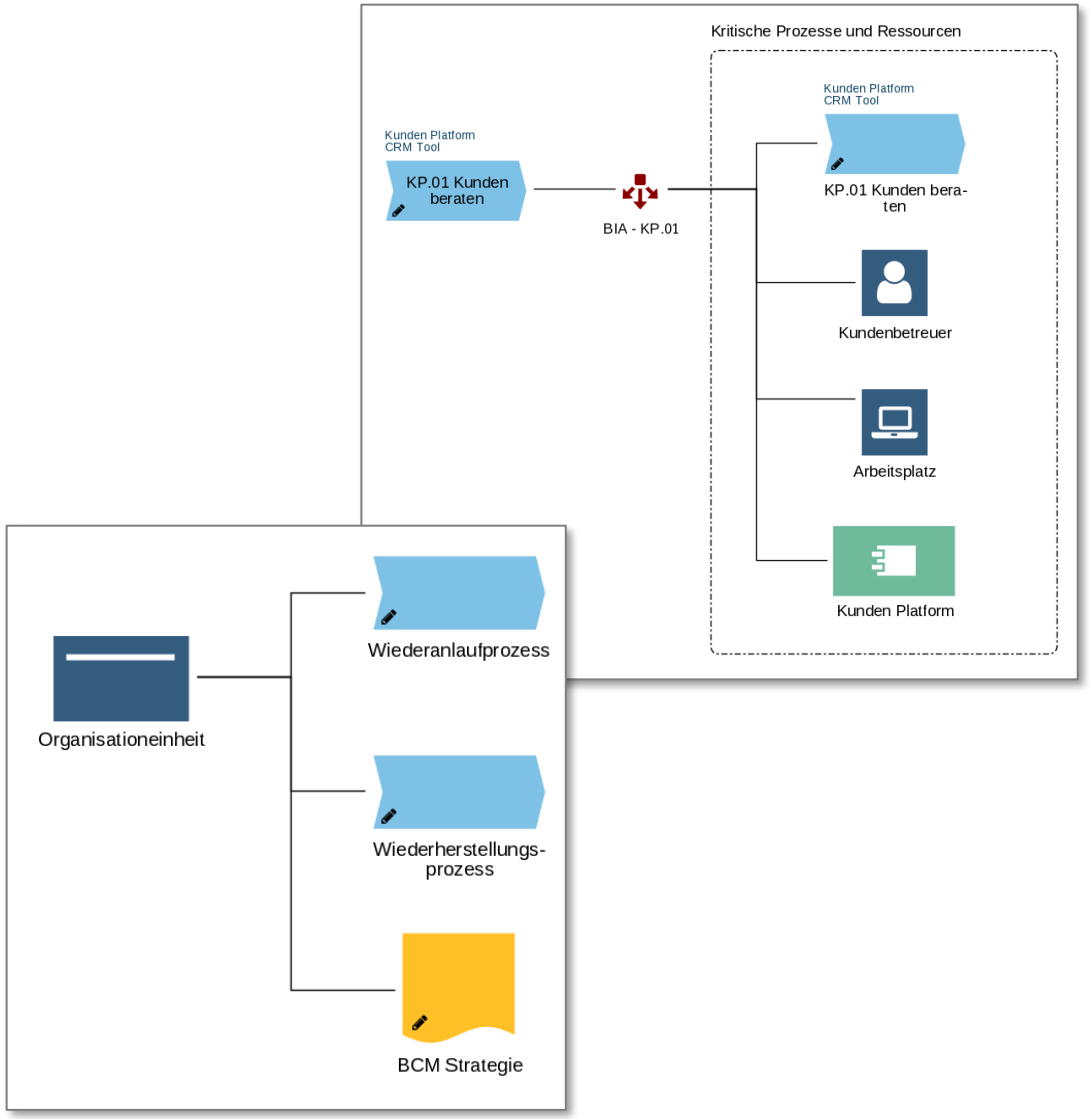




NIS2-Richtline

ADOGRC
Governance, Risk & Compliance
by boc-group.com

- Risikoanalyse und Konzept für Sicherheit der Informationssysteme
- Management von Sicherheitsvorfällen
- Sicherheit in der Lieferkette
- **Business Continuity und Krisenmanagement**
- Sicherheitsmaßnahmen bei Erwerb/Entwicklung/Wartung von IKT-Anwendungen
- Richtlinien für Cyberhygiene, Zugriffskontrolle und Kryptographie



Zusammenfassung

ADOGRC
Governance, Risk & Compliance

ADOGRC unterstützt Sie bei

ADOGRC
Governance, Risk & Compliance
by boc-group.com

DORA

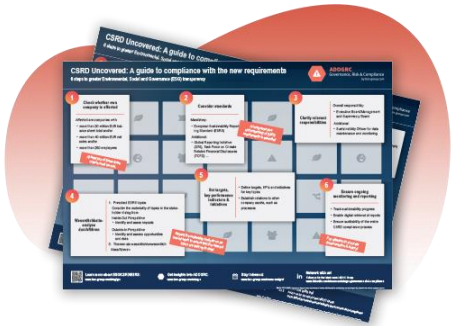
- IKT-Risikomanagement (inkl BCM)
- Management des Drittparteienrisikos (inkl Informationsregister)
- Testen der digitalen operationellen Resilienz
- Management von IKT-bezogener Vorfällen
- Vereinbarungen über den Austausch von Informationen
- Aufsicht über kritische Drittdienstleister

NIS 2

- Risikoanalyse und Konzept für Sicherheit der Informationssysteme
- Business Continuity und Krisenmanagement
- Sicherheit in der Lieferkette
- Management von Sicherheitsvorfällen
- Sicherheitsmaßnahmen bei Erwerb/Entwicklung/Wartung von IKT-Anwendungen
- Richtlinien für Cyberhygiene, Zugriffskontrolle und Kryptographie

Choose your next steps

ADOGRC
Governance, Risk & Compliance
by boc-group.com



Poster

ESG: 6 Simple Steps you Need to Consider – Poster

All relevant CSRD information at a glance. Includes the procedure for meeting ESG requirements.

Scan, to download the poster

See ADOGRC in action

Get a demo of our Governance, Risk & Compliance Suite

Meet risks and controls sustainably and increase the efficiency, effectiveness and success of your company. From small businesses to large enterprises – build a unique competitive edge.

Scan, to learn more about ADOGRC

Get in touch!