ADOGRC
Governance, Risk & Compliance

BOC Group
Design Your Enterprise

Success Factors for DORA and NIS-2

Successful realisation with ADOGRC

Antonia Hubbermann

13.09.2024

Agenda

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

Legal acts for cyber security

Integration of DORA with ADOGRC

Prospects for NIS-2

Summary

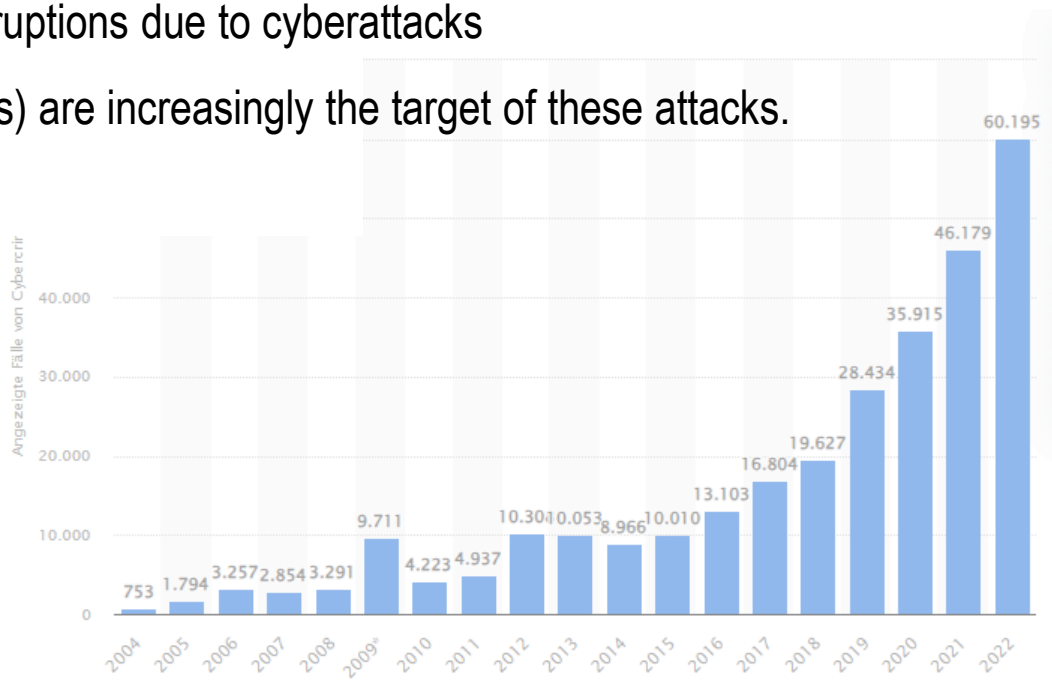
Legal acts for cyber security

ADOGRC
Governance, Risk & Compliance

Why do we need Cybersecruity Laws?

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

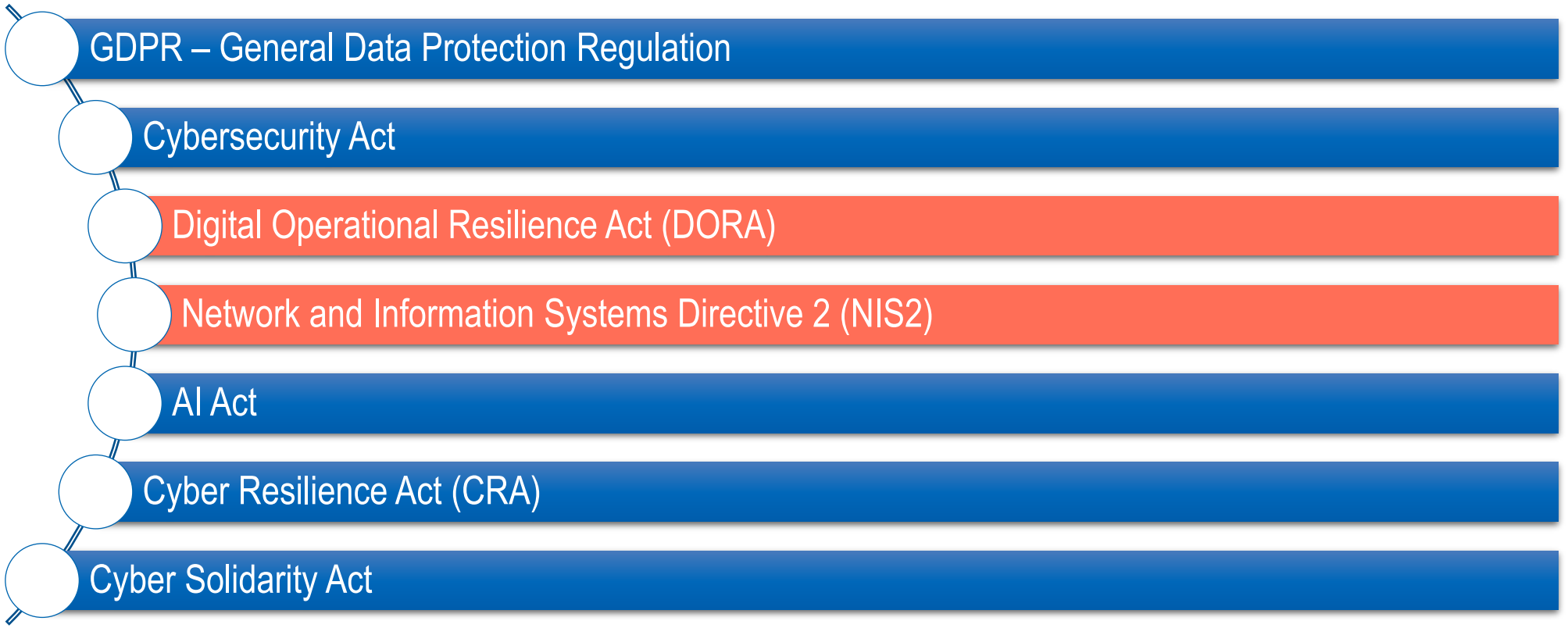
- In 2023, **84.7% of organizations globally** experienced at least one cyberattack (rising trend)
- **Every 6th cyberattack is successful (KPMG study)**
- Ransomware attacks are increasing both in **damage and frequency**
  - 33% of companies in Austria report one-week operational interruptions due to cyberattacks
- Critical infrastructure and SMEs (small and medium-sized enterprises) are increasingly the target of these attacks.



Sources:
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

Legal Framework for Cybersecruity

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



Comparison of Legislation

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

DORA

- ICT Risk Management
- Management of ICT-related incidents
- Testing digital operational resilience
- Managing ICT risks originating from third-party providers
- Agreements on information sharing
- Oversight of critical third-party providers

NIS2 Directive

- Risk analysis and concept for information system security
- Management of security incidents
- Business Continuity and Crisis Management
- Supply chain security
- Security measures for acquisition/ development/ maintenance of ICT applications
- Policies for cyber hygiene, access control and cryptography

Comparison of Legislation

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

DORA

- ICT Risk Management
- Management of ICT-related incidents
- Testing digital operational resilience
- Managing ICT risks originating from third-party providers
- Agreements on information sharing
- Oversight of critical third-party providers

NIS2 Directive

- Risk analysis and concept for information system security
- Management of security incidents
- Business Continuity and Crisis Management
- Supply chain security
- Security measures for acquisition/ development/ maintenance of ICT applications
- Policies for cyber hygiene, access control and cryptography

Strengthening the resilience of European companies against cyber threats

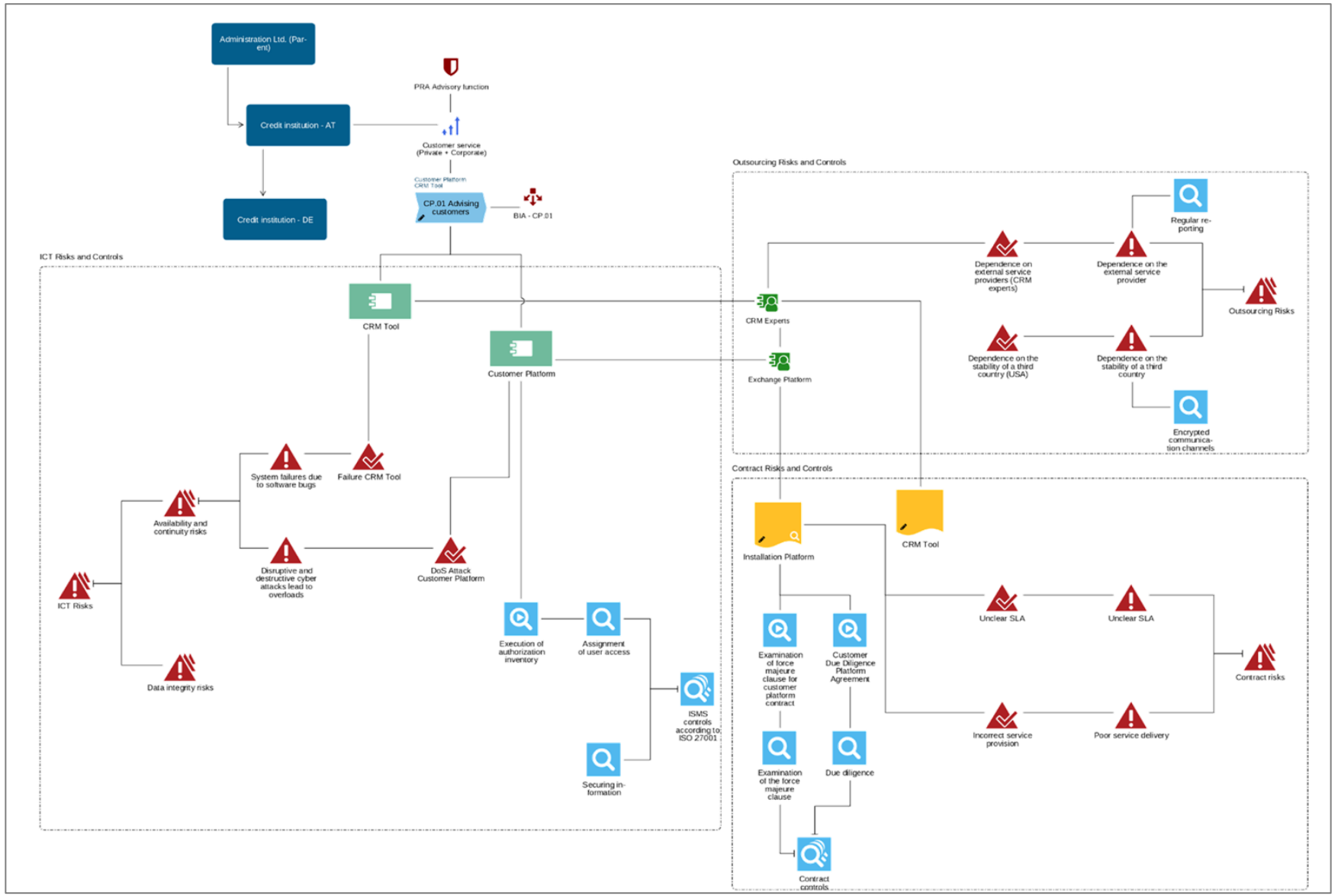
- Financial market
- Companies that are part of critical infrastructure

Integration of DORA with ADOGRC

ADOGRC
Governance, Risk & Compliance

DORA Solution

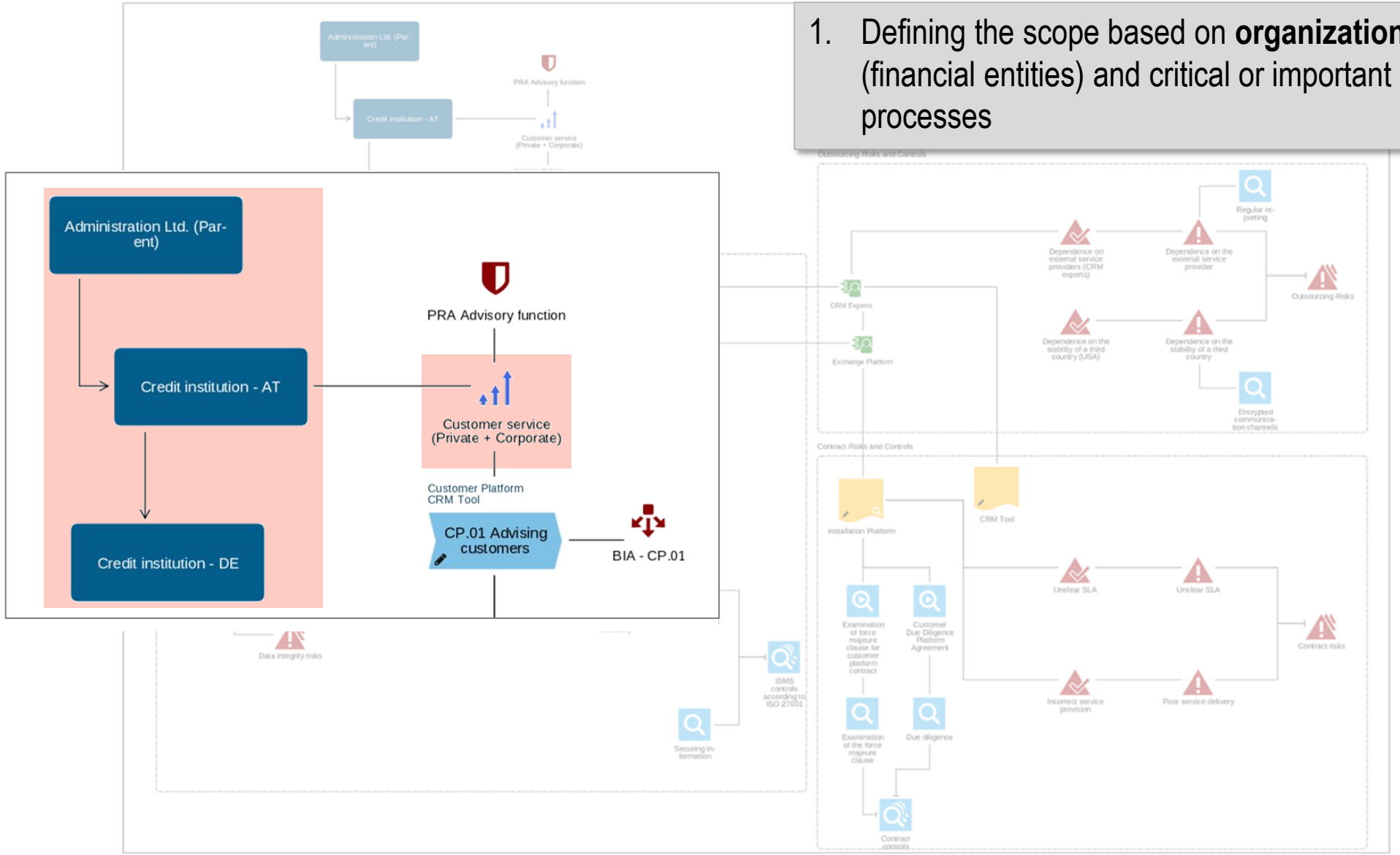
ADOGRC
Governance, Risk & Compliance
by boc-group.com



Scope Determination

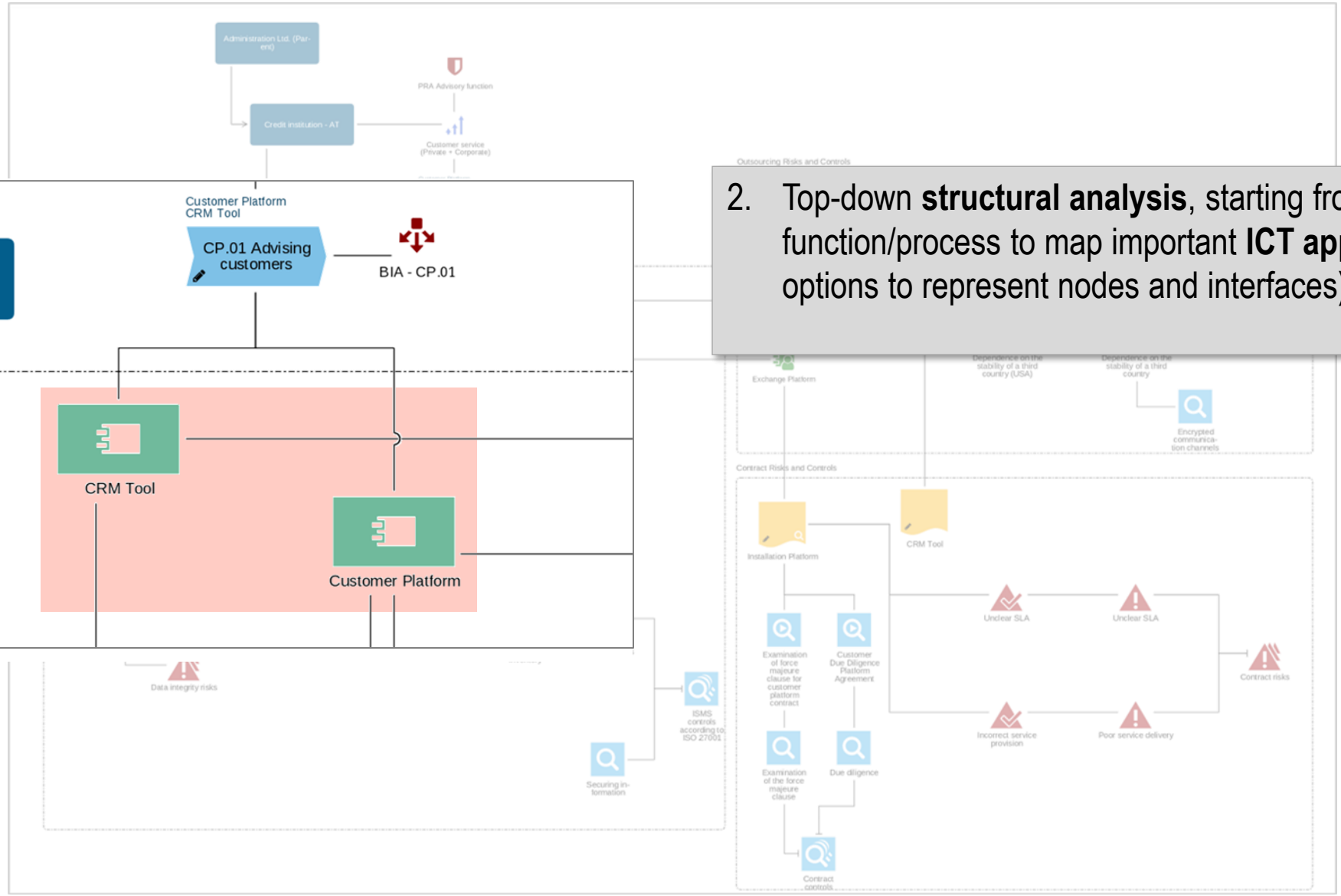
ADOGRC
Governance, Risk & Compliance
by boc-group.com

1. Defining the scope based on **organizational units** (financial entities) and critical or important **functions** or processes



Structural analysis of ICT Application

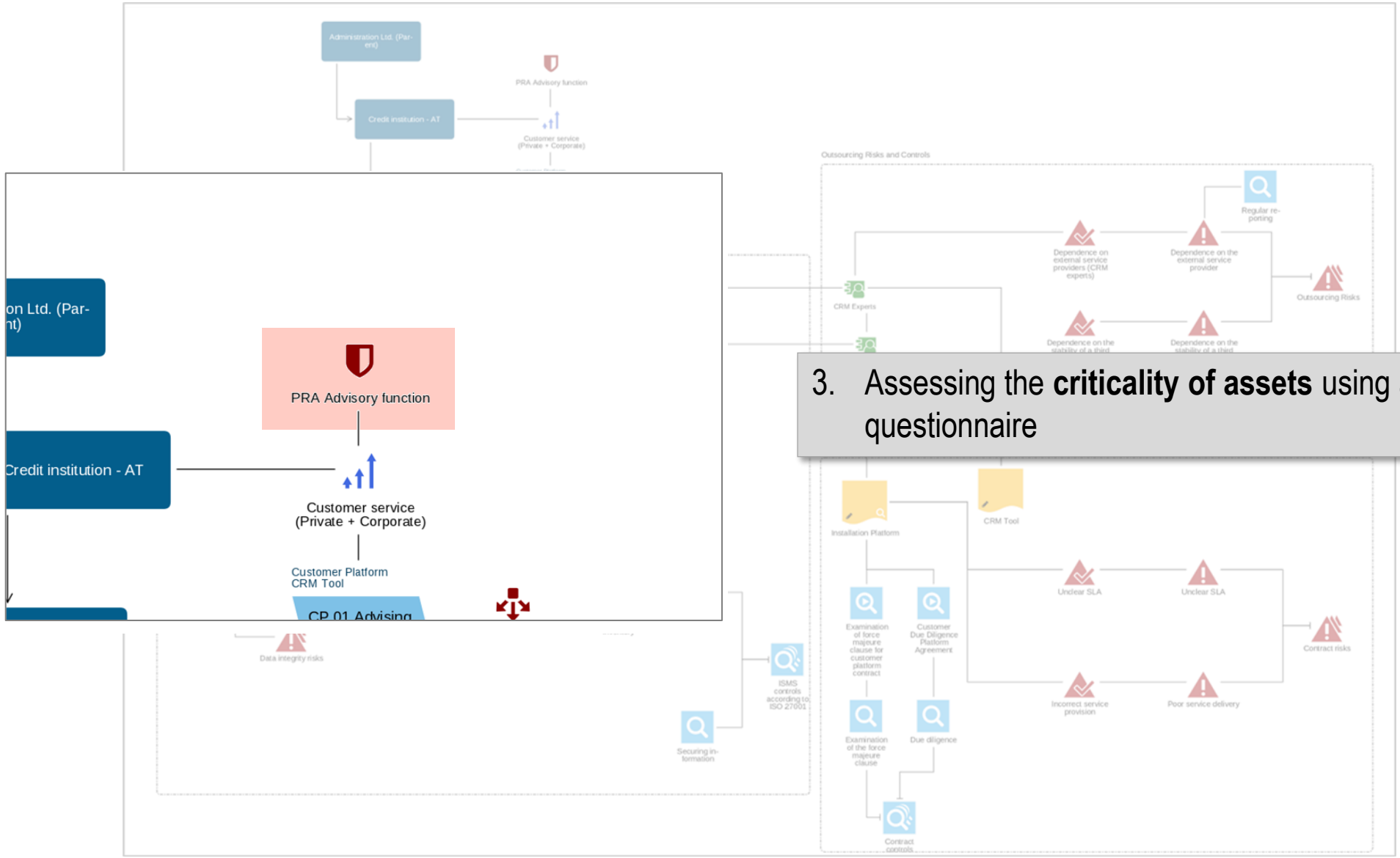
ADOGRC
Governance, Risk & Compliance
by boc-group.com



2. Top-down **structural analysis**, starting from the function/process to map important **ICT applications** (with options to represent nodes and interfaces)

Asset Criticality Assessment

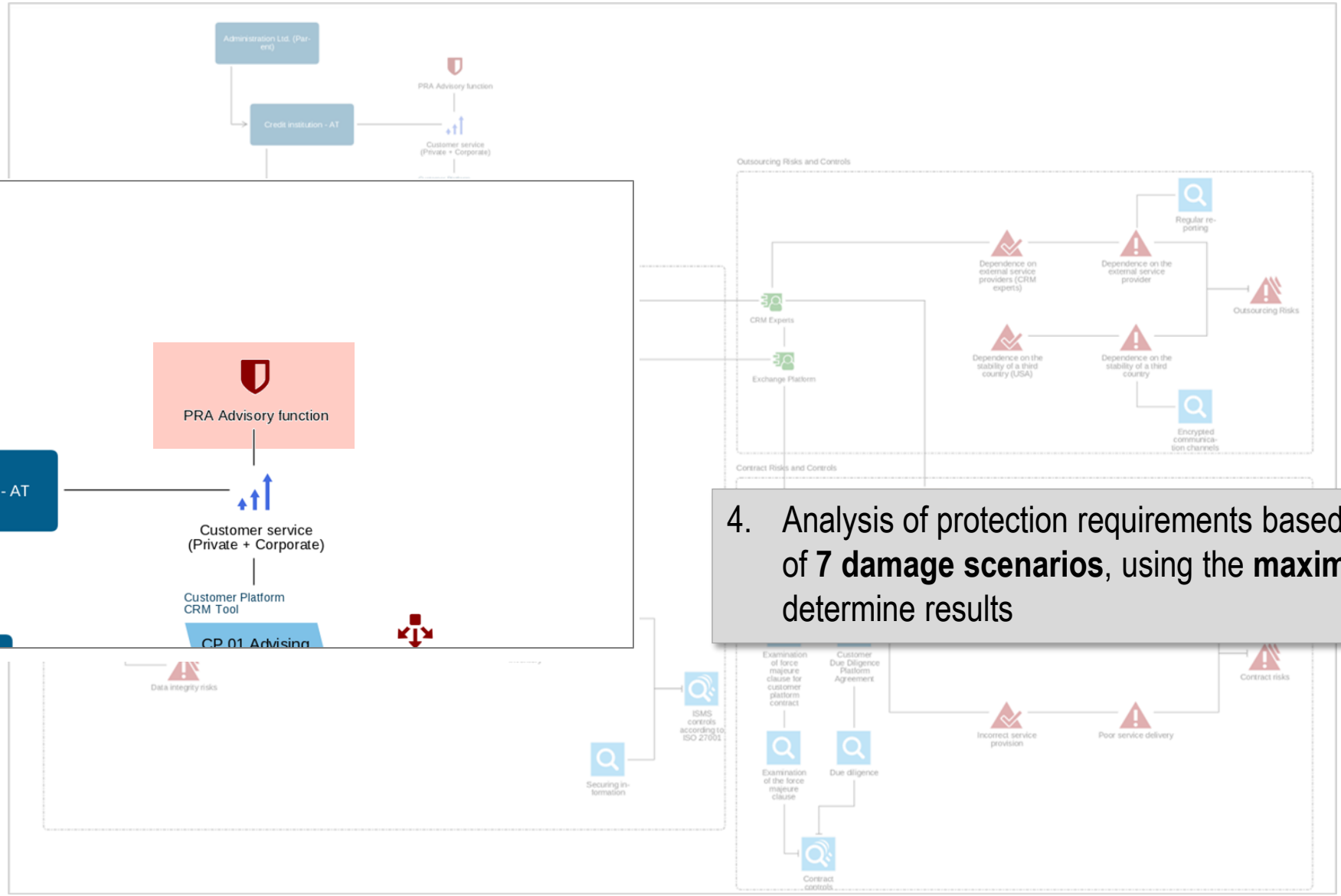
ADOGRC
Governance, Risk & Compliance
by boc-group.com



3. Assessing the **criticality of assets** using a predefined questionnaire

Protection Requirements Analysis

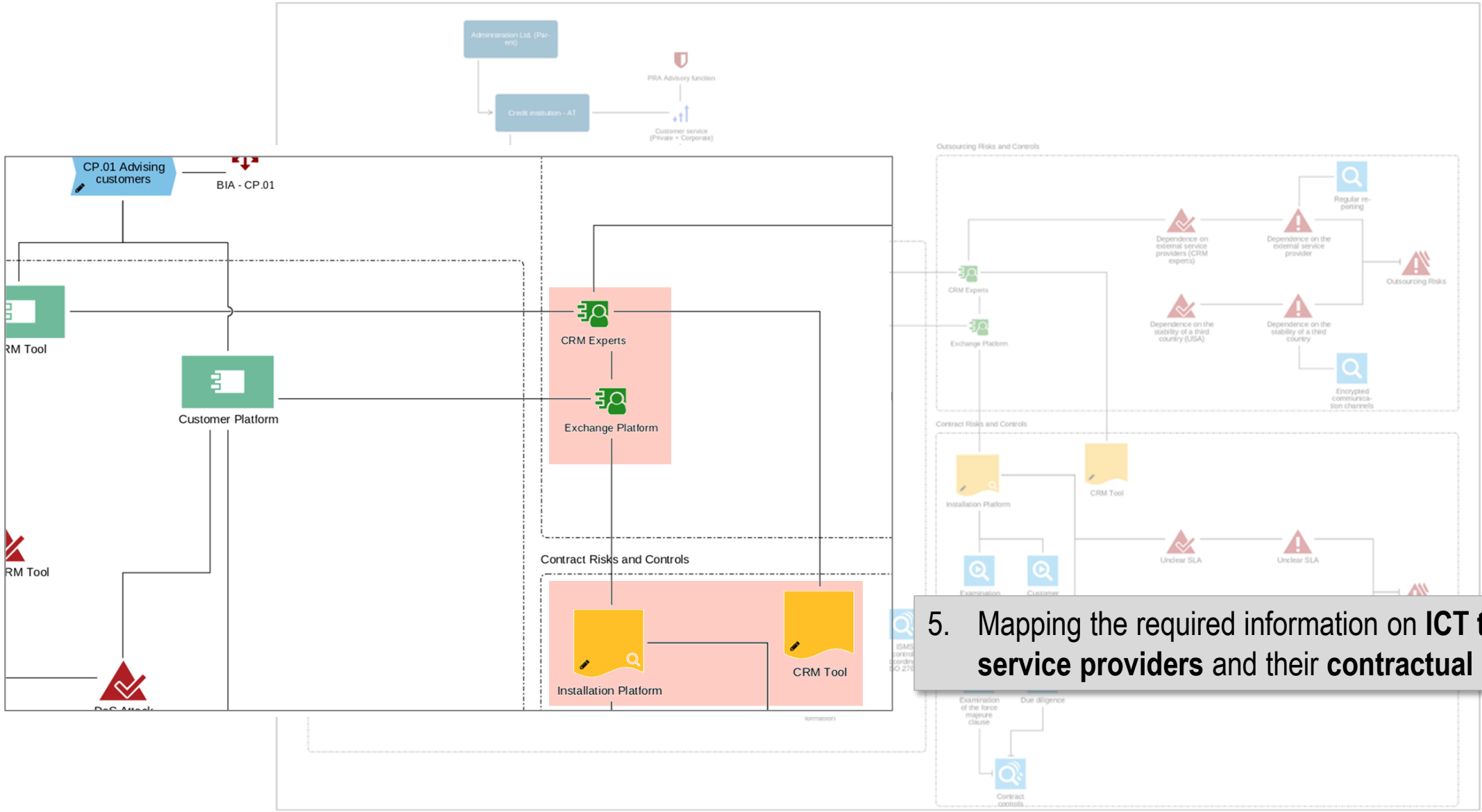
ADOGRC
Governance, Risk & Compliance
by boc-group.com



4. Analysis of protection requirements based on the evaluation of **7 damage scenarios**, using the **maximum principle** to determine results

ICT Third-Party Provider and contractual Arrangements

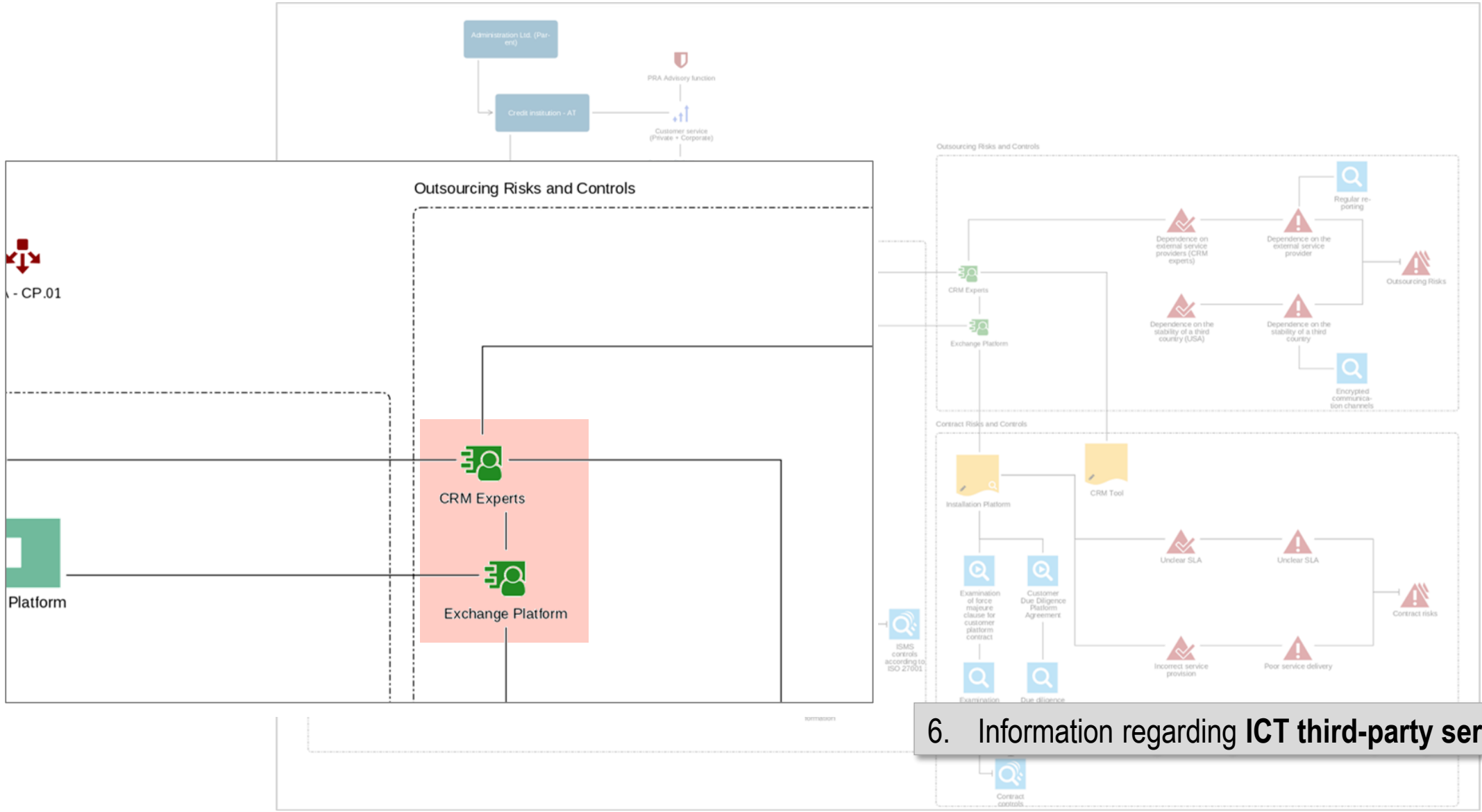
ADOGRC
Governance, Risk & Compliance
by boc-group.com



5. Mapping the required information on **ICT third-party service providers** and their **contractual agreements**

ICT Third-Party Provider

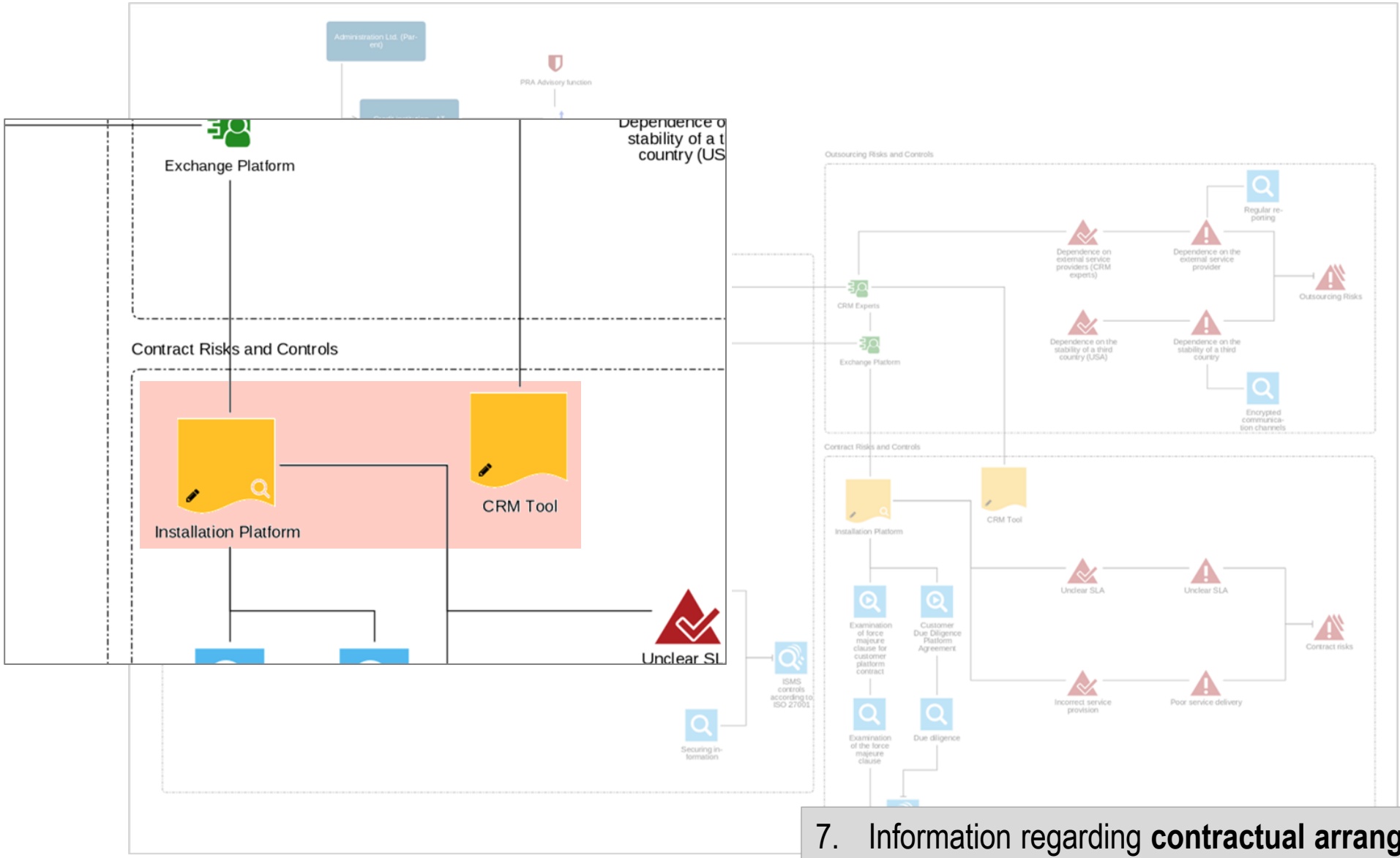
ADOGRC
Governance, Risk & Compliance
by boc-group.com



6. Information regarding **ICT third-party service providers**

Contractual Arrangements

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

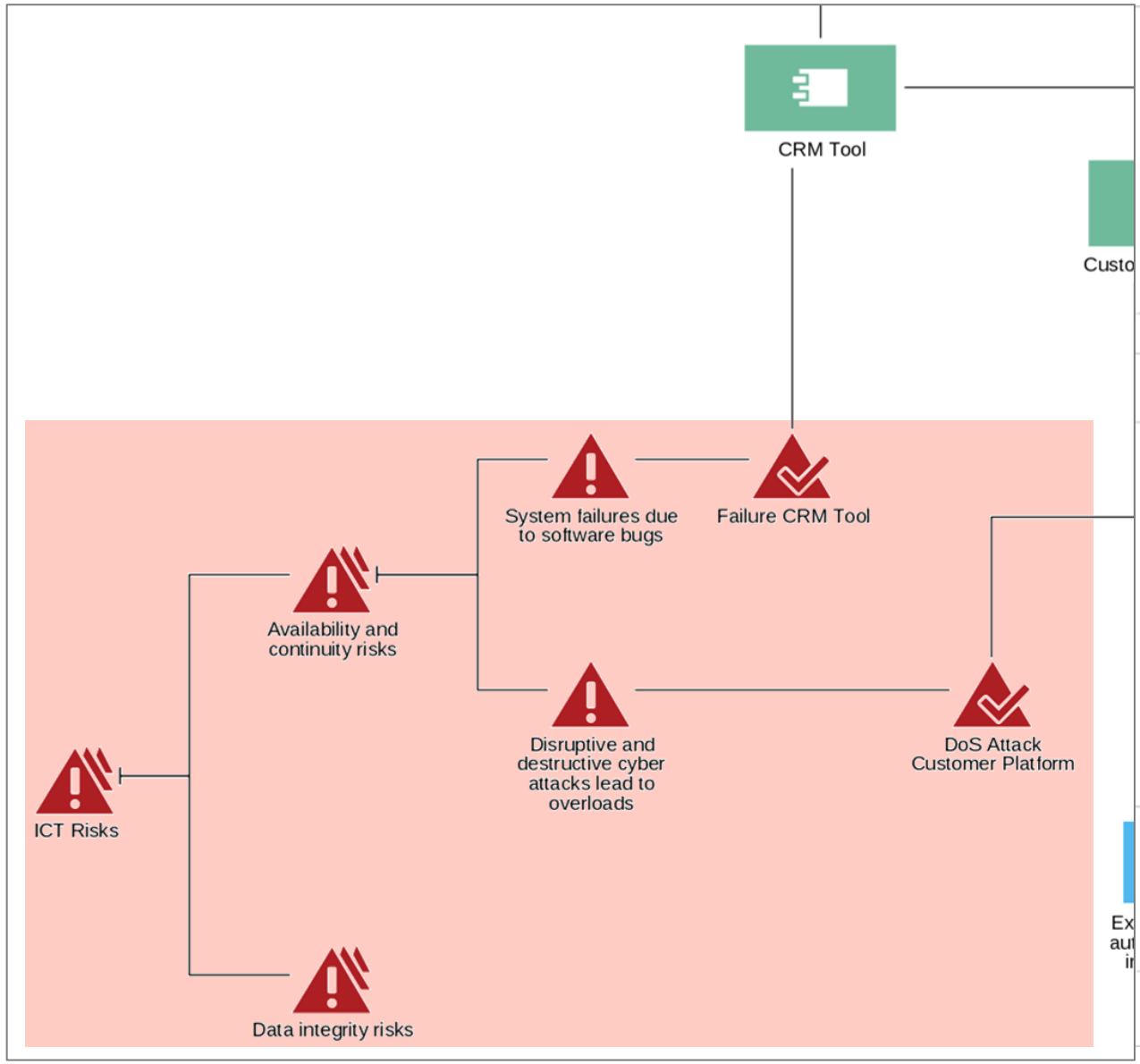


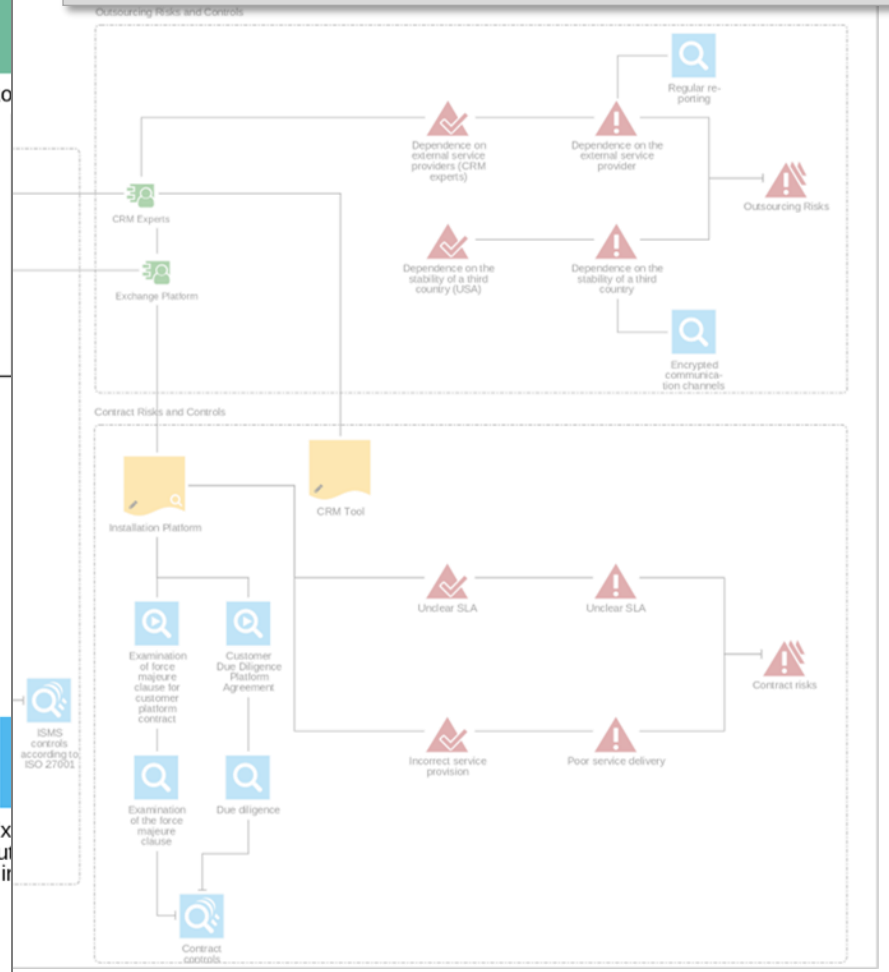
7. Information regarding **contractual arrangements**

ICT Risk Management

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

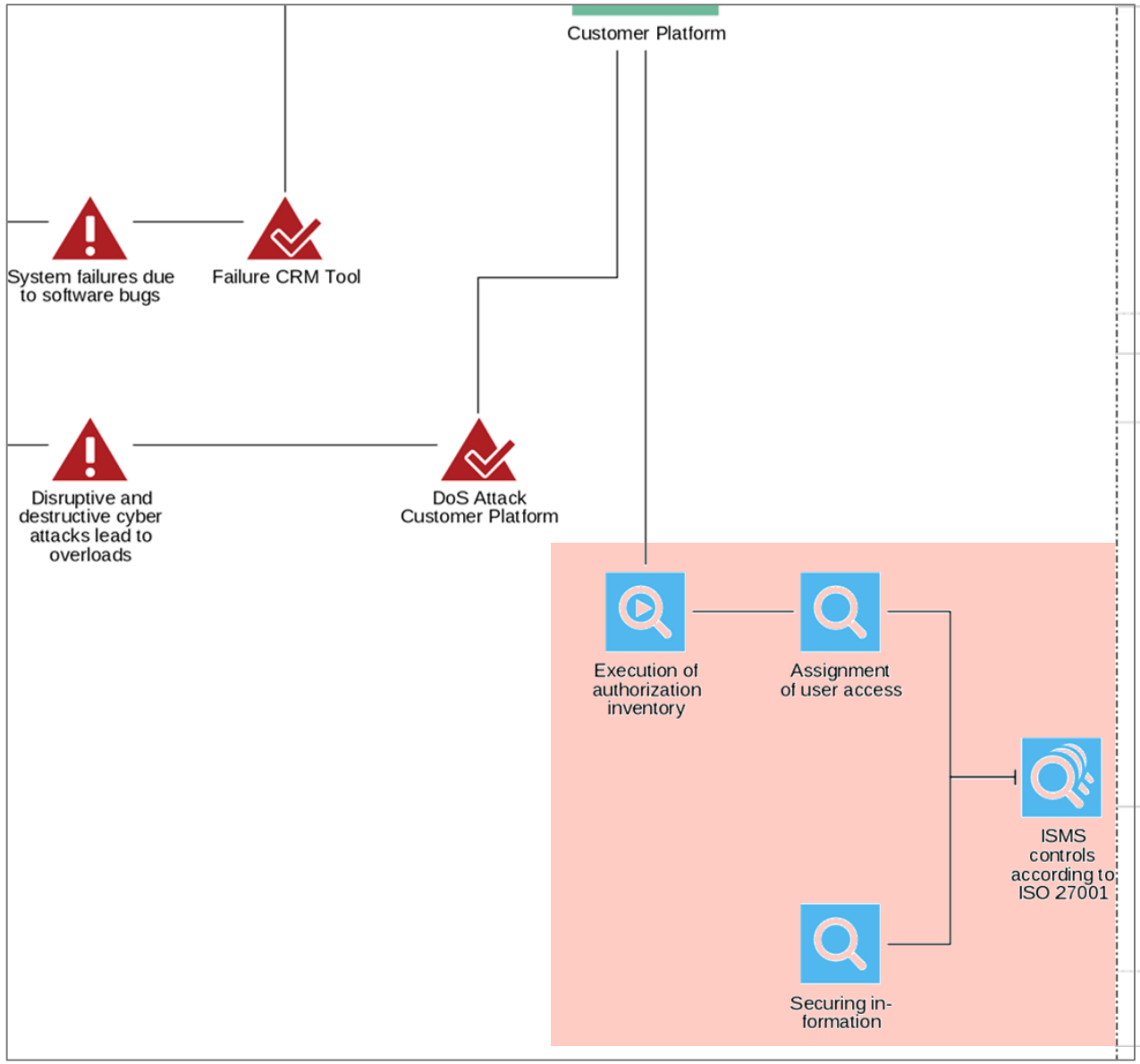
8. Using existing risk classes (**master data and assessments**), the **risk management** is expanded to comply with DORA



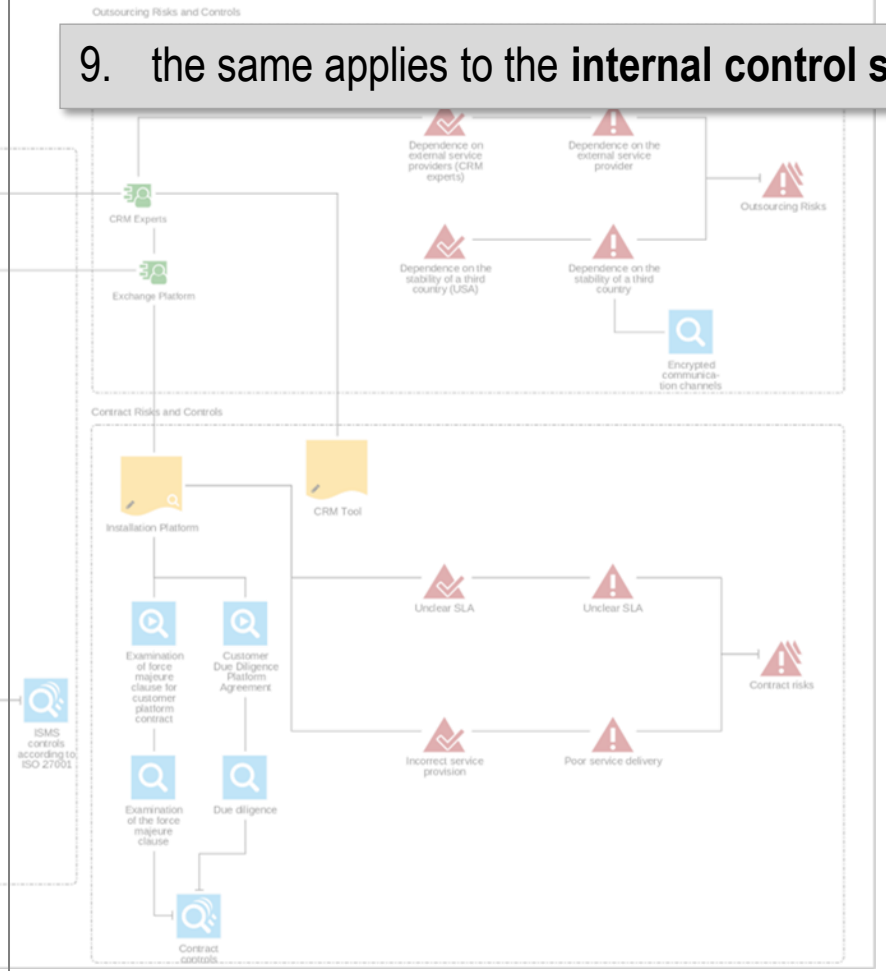


Supplementing ICS with ICT Controls

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

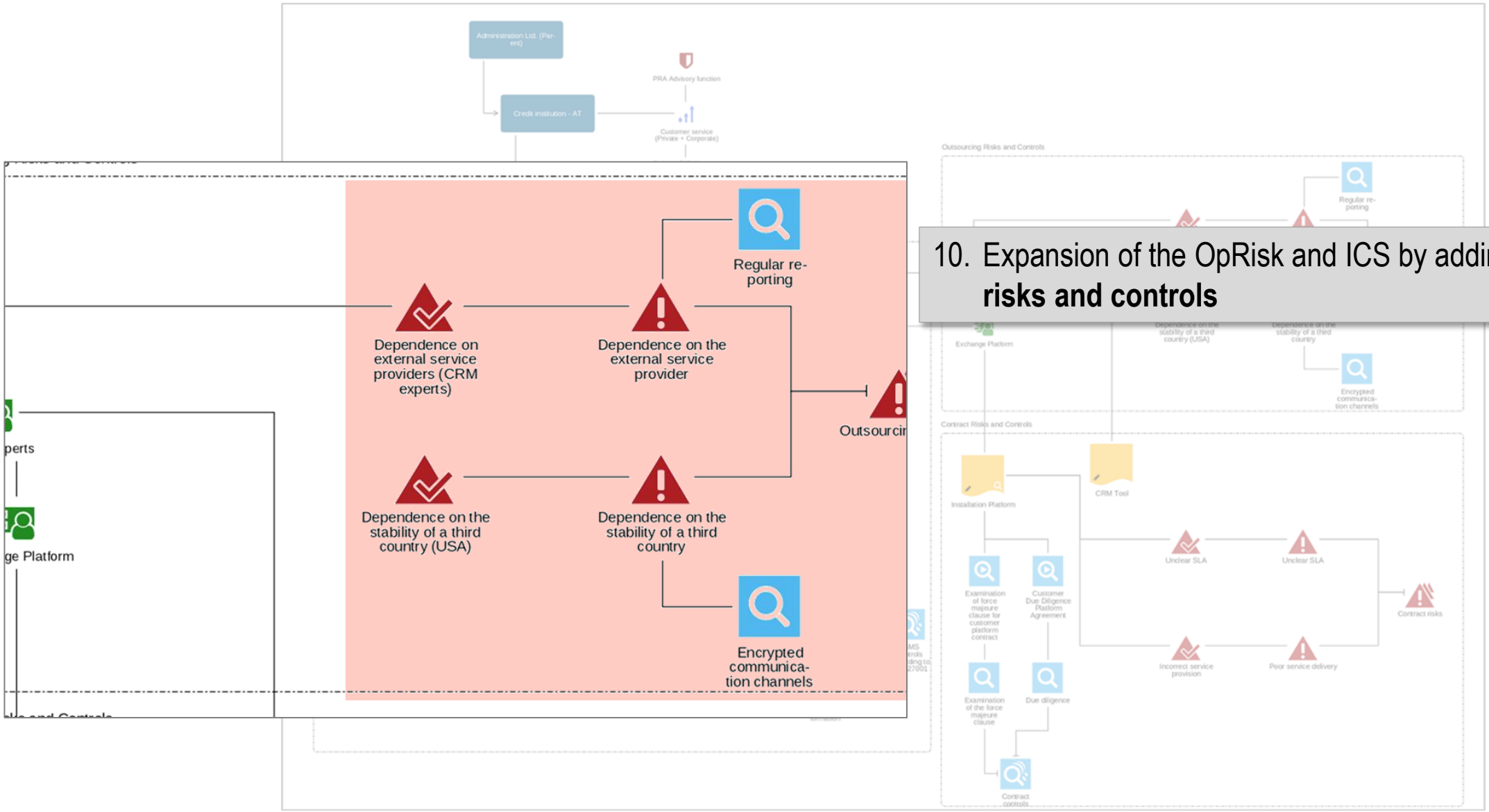


9. the same applies to the **internal control system** (ICS)



Outsourcing Risks und Controls

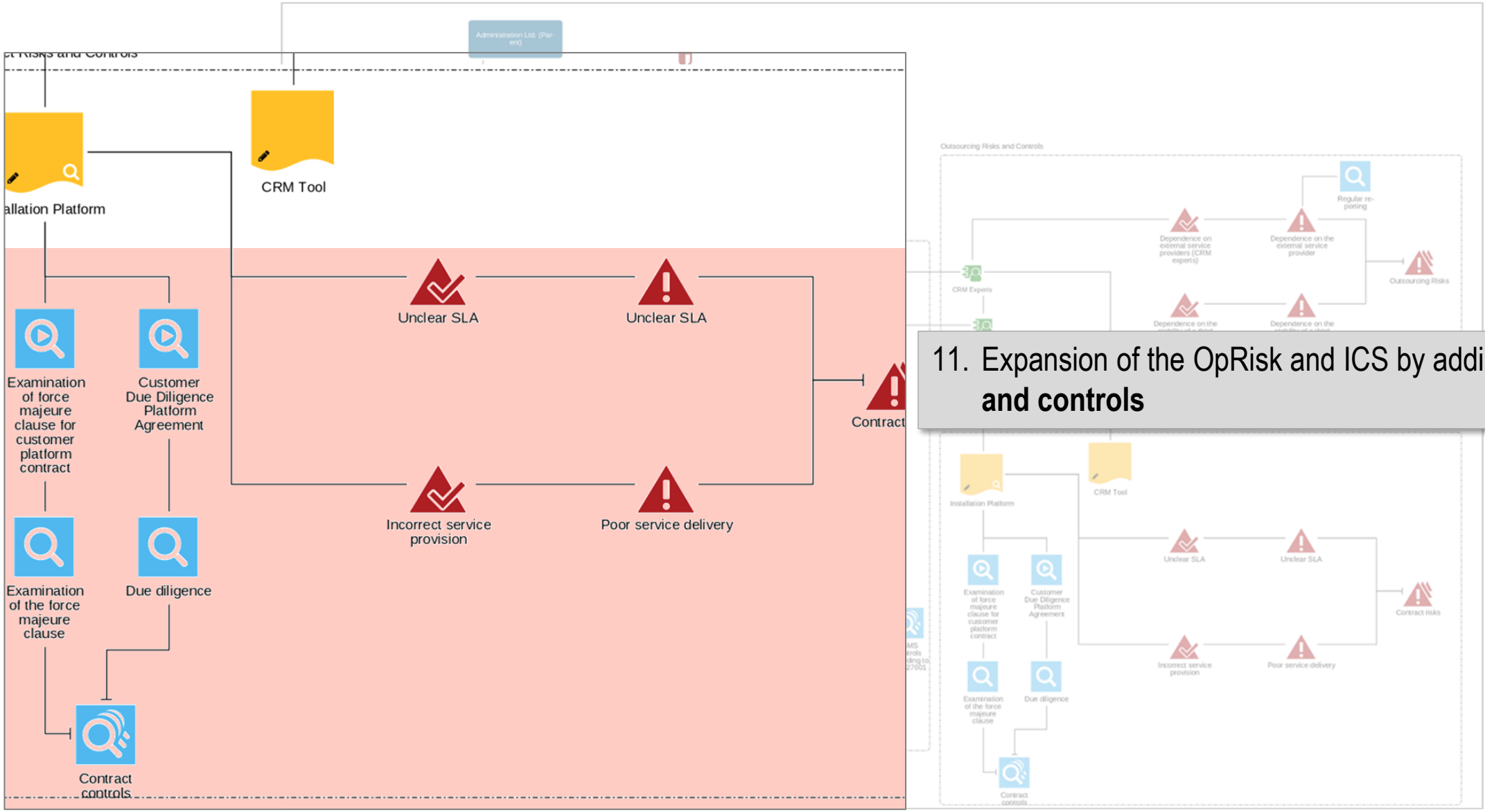
ADOGRC
Governance, Risk & Compliance
by boc-group.com



10. Expansion of the OpRisk and ICS by adding **outsourcing risks and controls**

Contract Risks and Controls

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



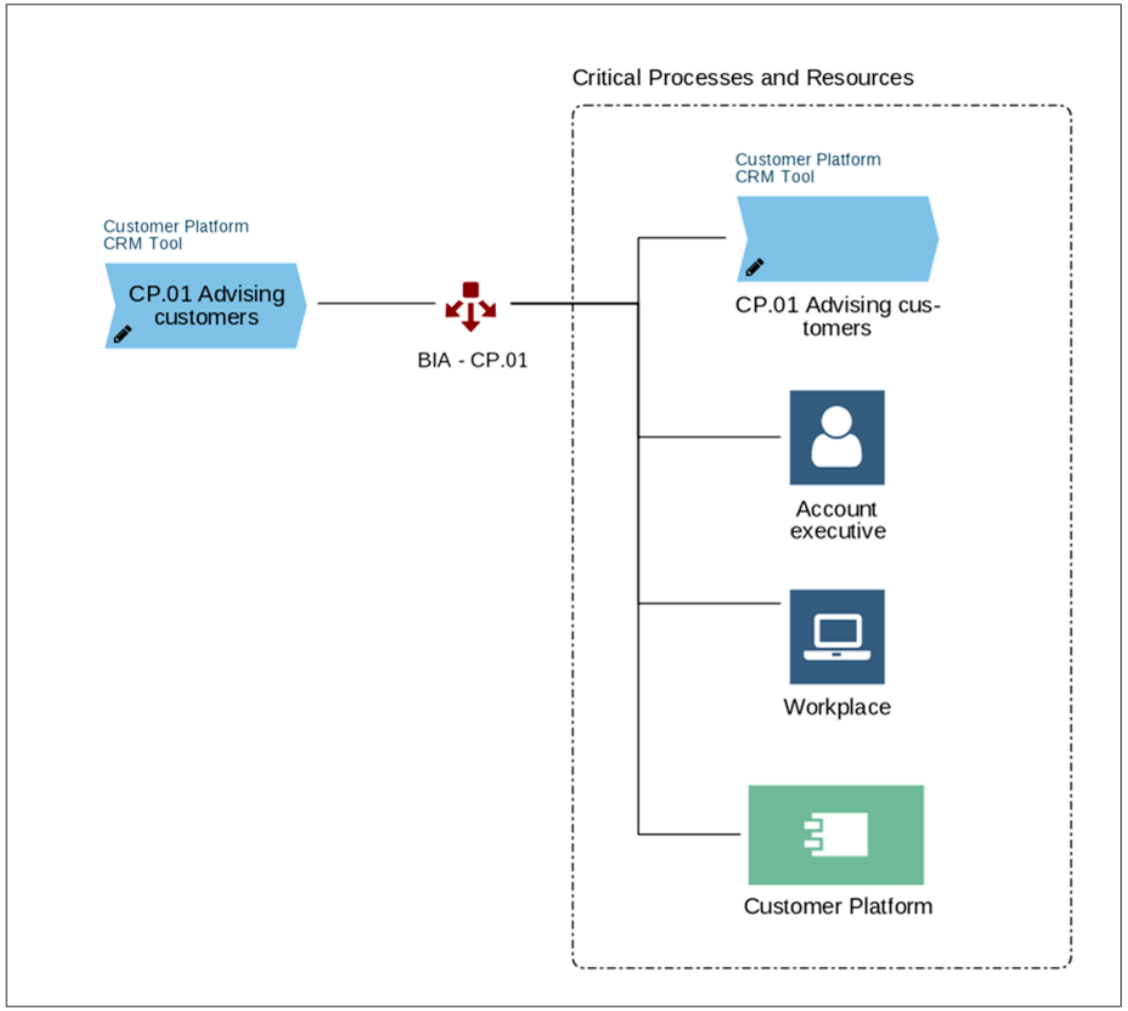
11. Expansion of the OpRisk and ICS by adding **contract risks and controls**

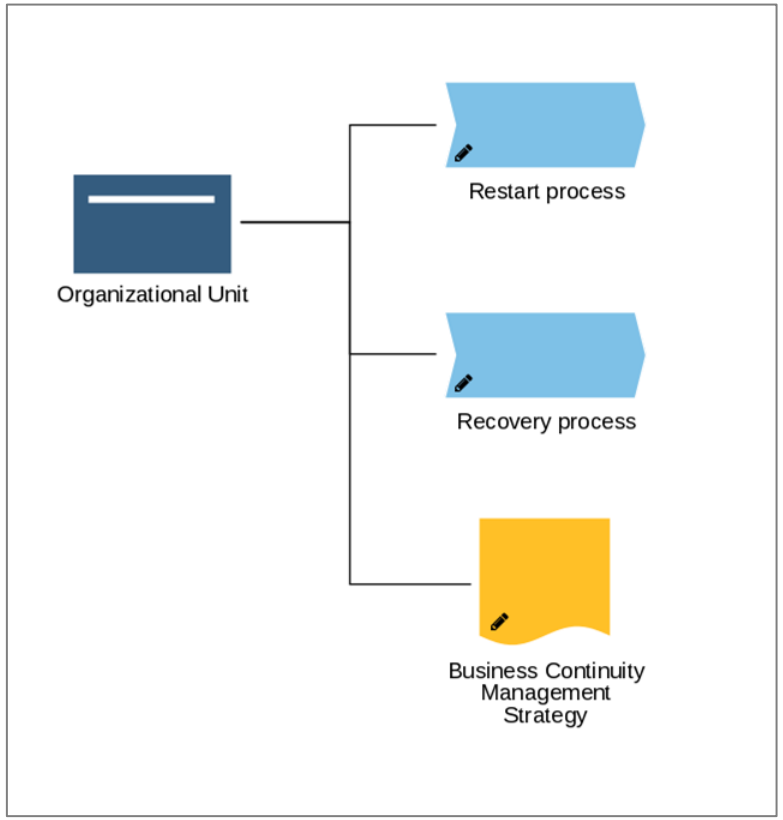
Business Continuity Management

ADOGRC
Governance, Risk & Compliance

BCM as Part of the DORA Solution

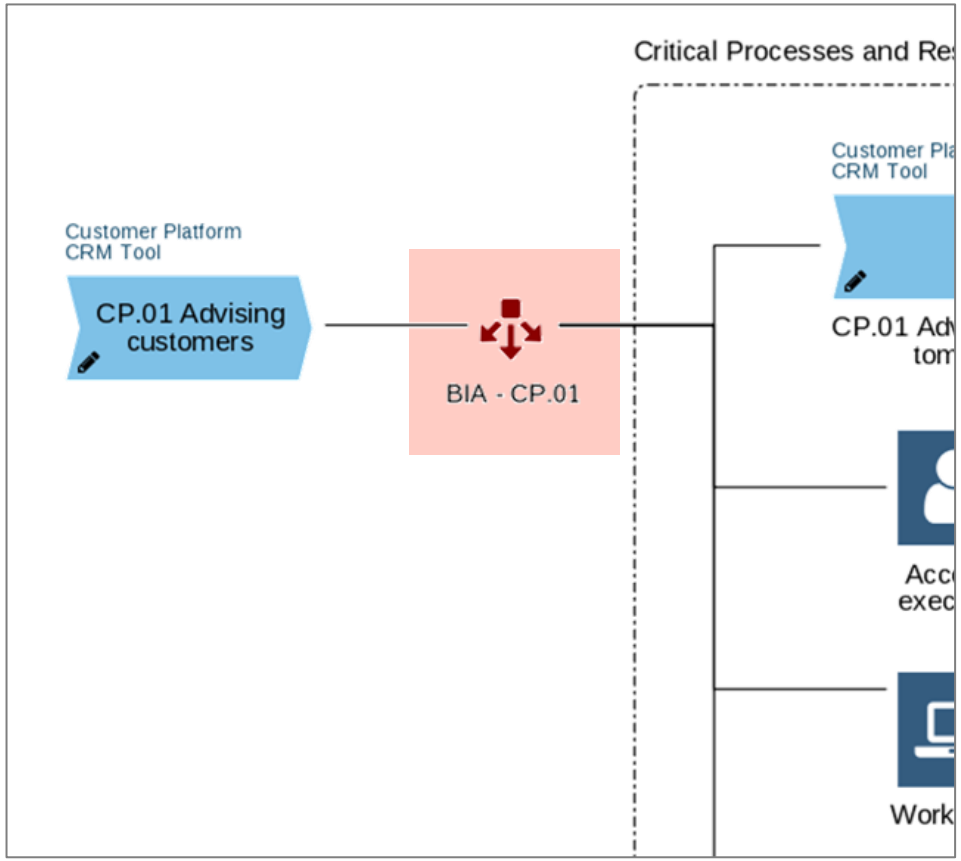
ADOGRC
Governance, Risk & Compliance
by boc-group.com





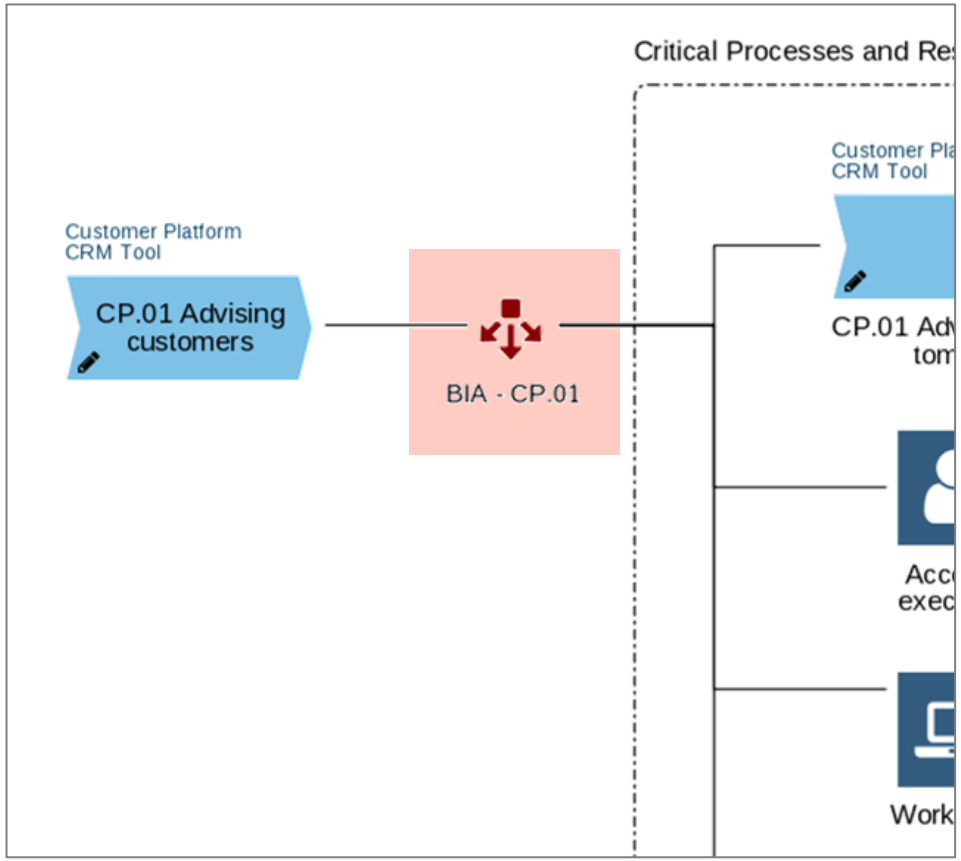
Business Impact Analysis

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



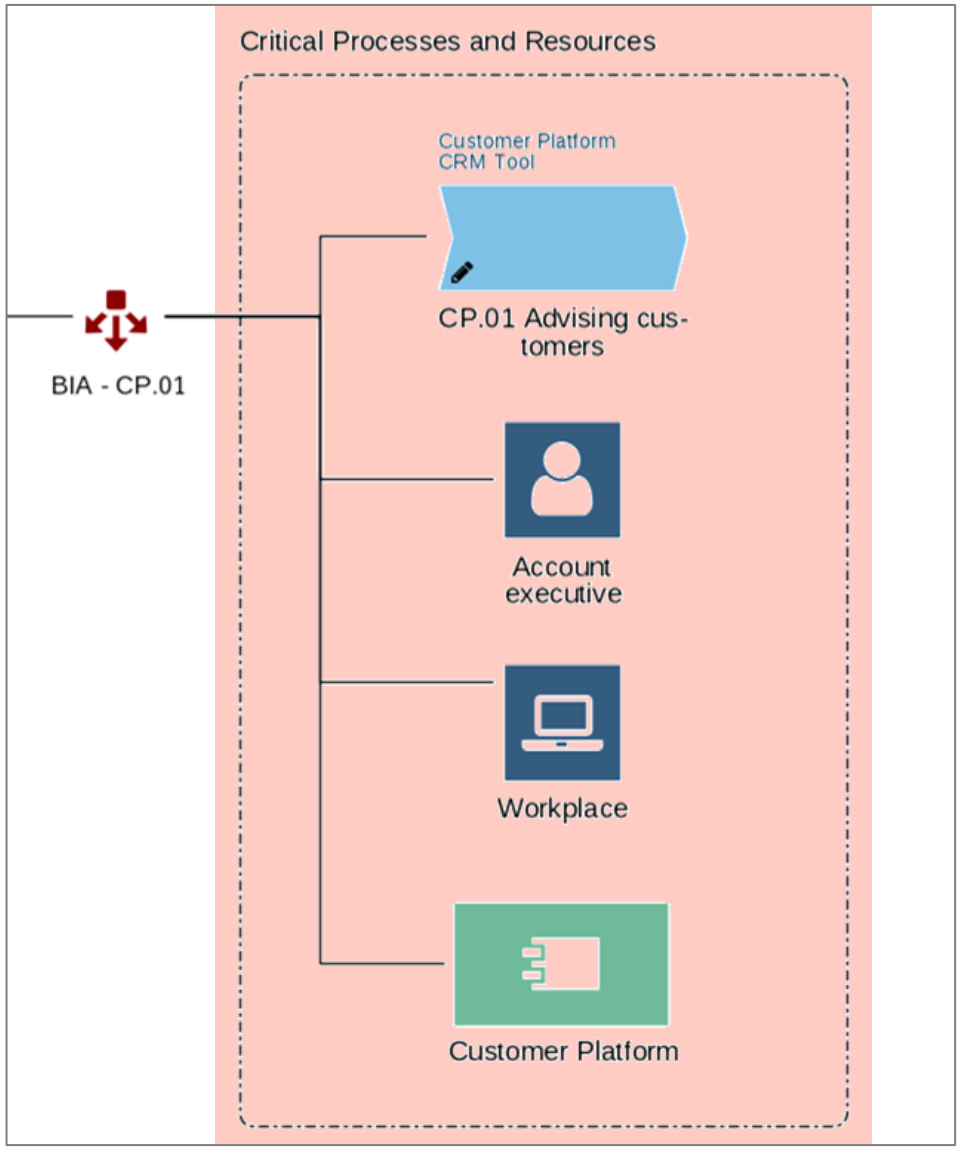
1. Analysis is based on the evaluation of **5 impact categories** over **5 time dimensions**. The result is based on the **maximum principle**

Defining Key Figures in BIA



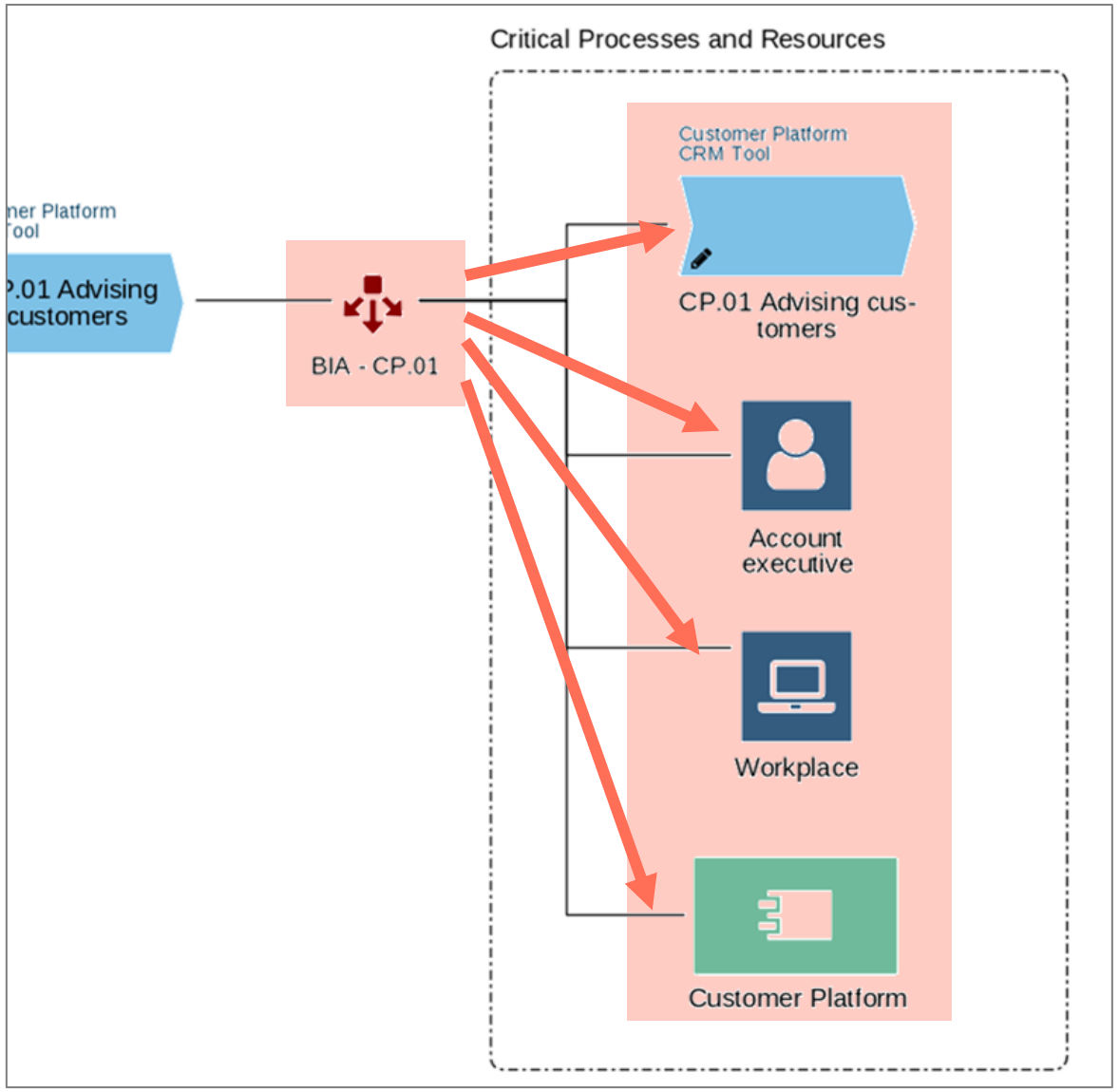
2. Establishing key figures such **as maximum tolerable period of disruption, Recovery Time Objective,** and **Recovery Point Objective**

Critical elements for emergency operation



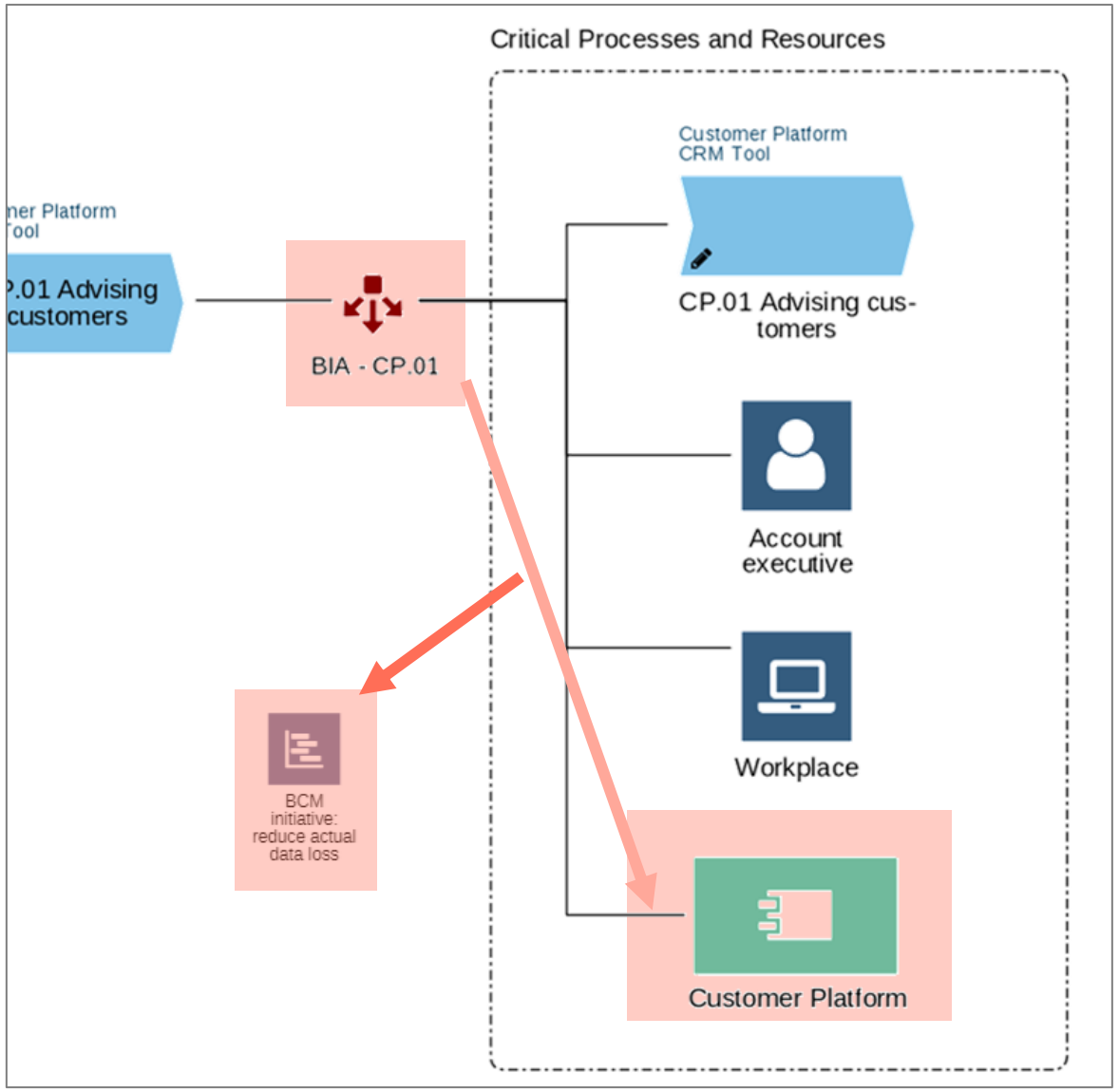
3. **Critical processes** and **resources** for emergency operations can be **defined** (information-based and non-information-based assets)

Comparison Target vs. Actual



4. **Comparison of target and actual** values for period of disruption, Recovery Time Objective, and Recovery Point Objective against the **actual period of disruption**, **recovery time**, and r**ecovery point** defined in **critical processes** and **resources**

Initiative according to Gap Analysis

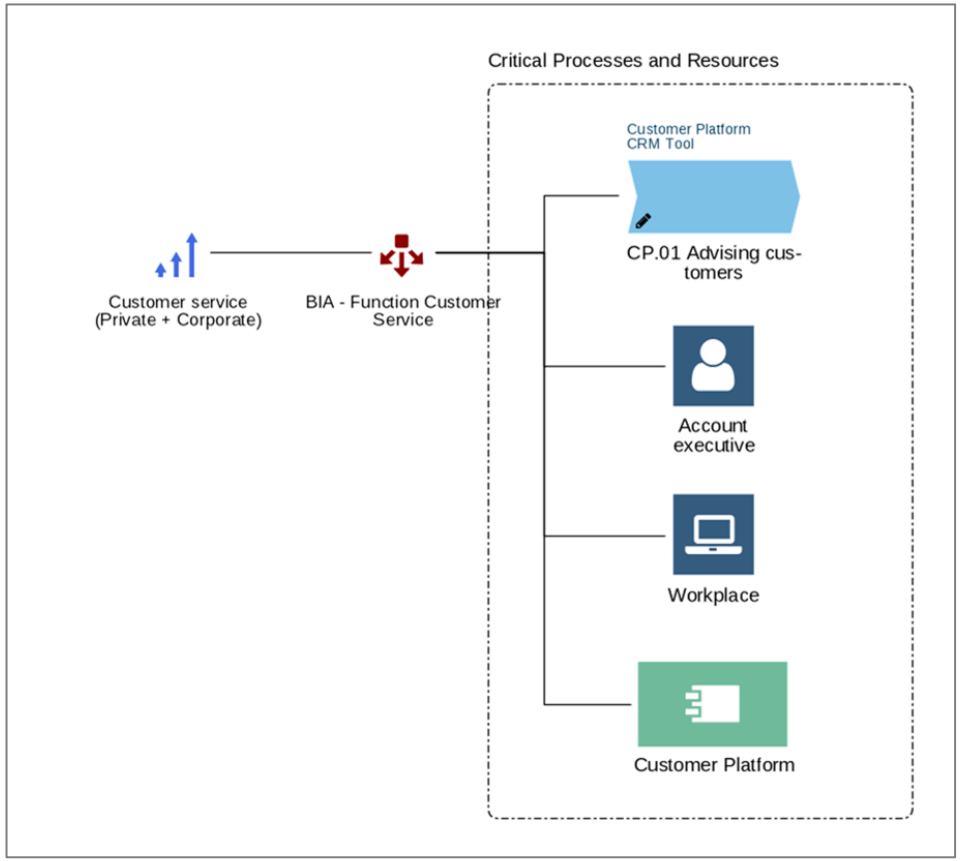


5. After identifying gaps, **actions** can be developed to address and improve these areas

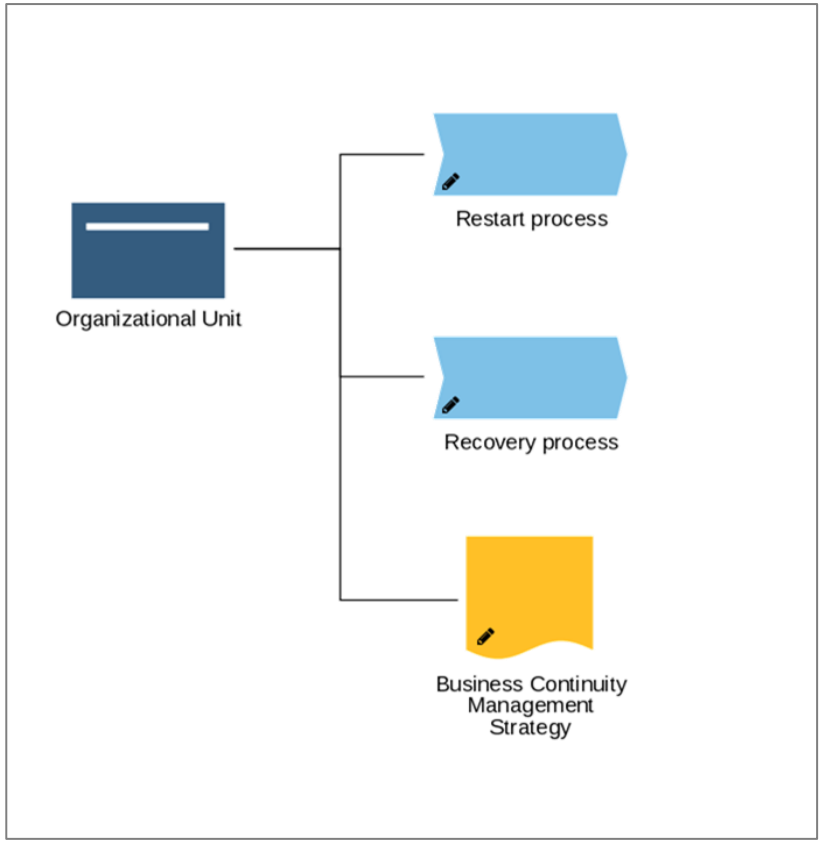
Same Principle for Function

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

6. The concept also applies to **functions**



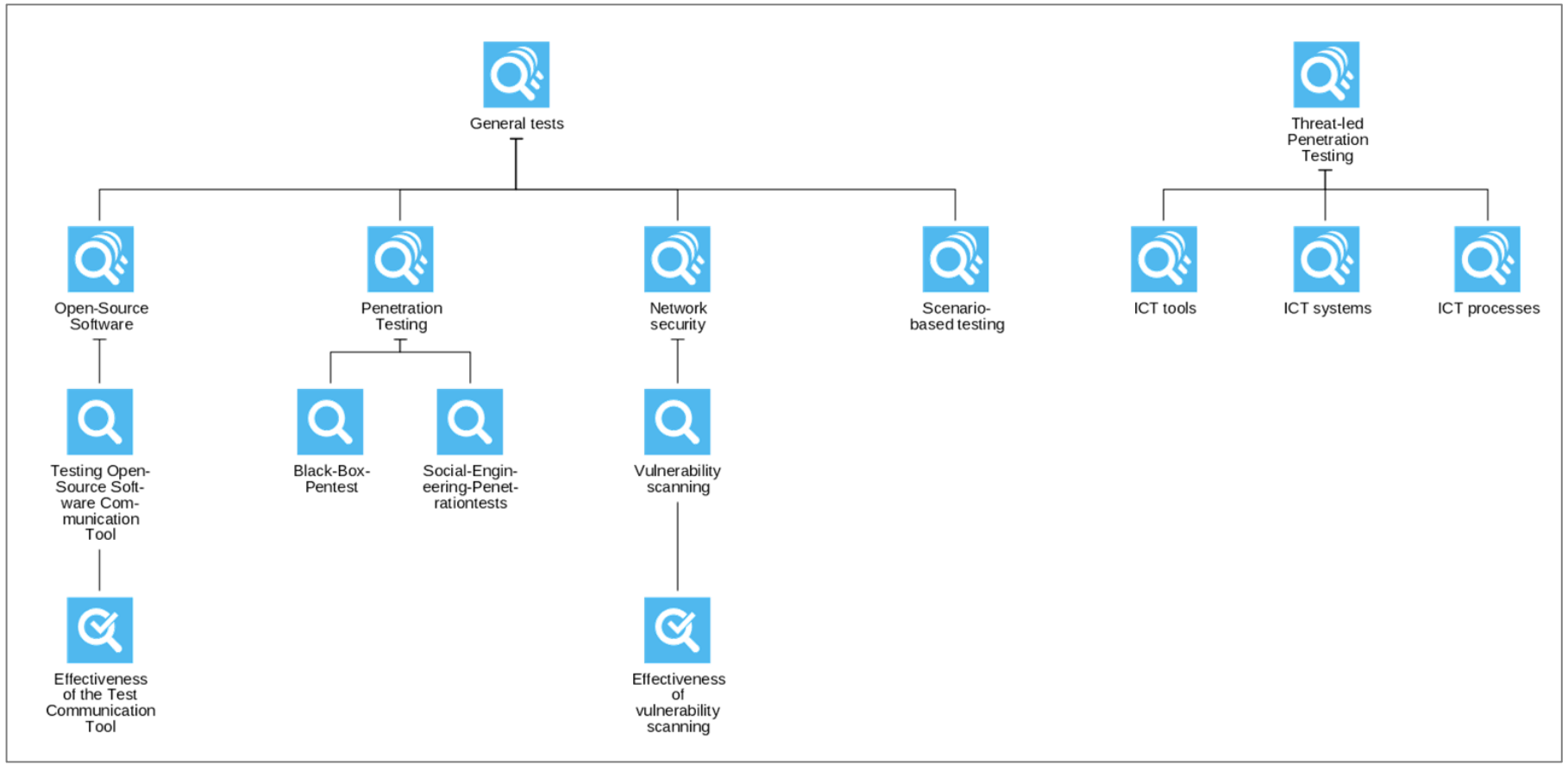
Planning at the OU Level



7. The **restarting and recovery process planning** takes place at the organizational unit level, along with the definition of the **BCM strategy**

Digital operational resilience testing

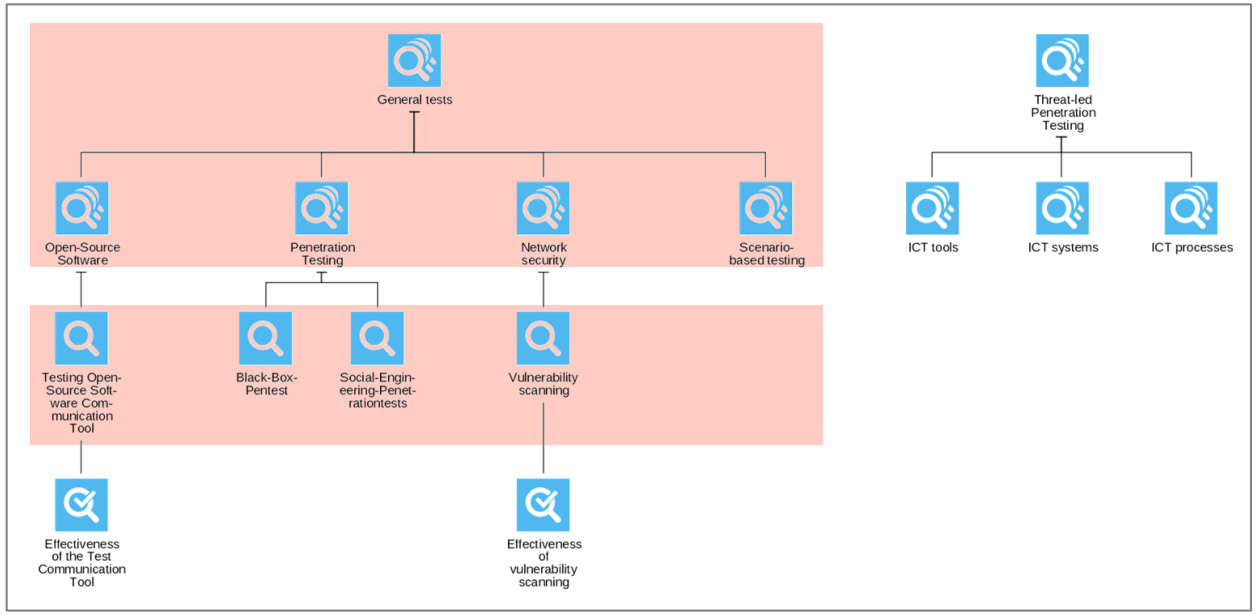
ADOGRC
Governance, Risk & Compliance
by boc-group.com



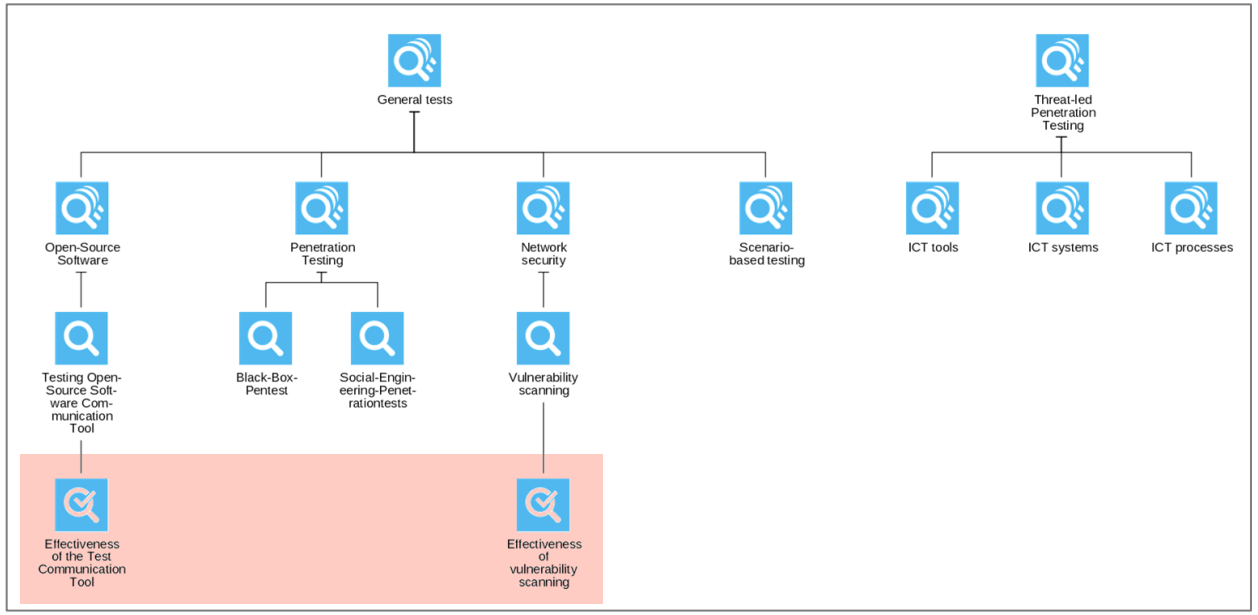
Test Strategy

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

1. **Control groups** and **controls** can be used to map the test concept

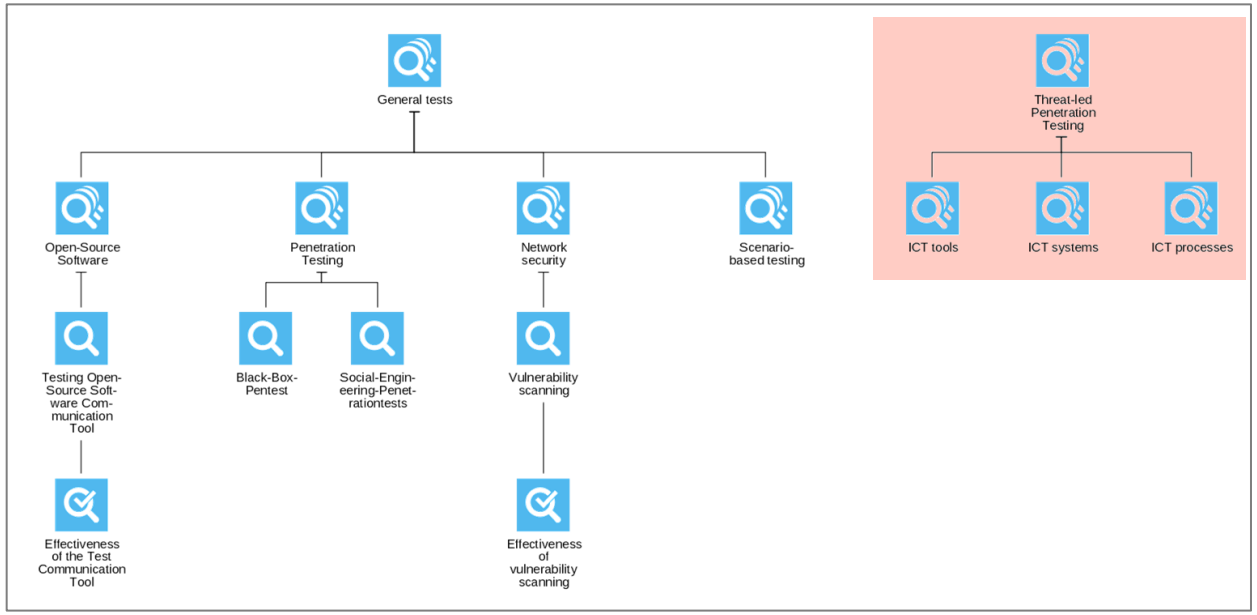


Effectiveness of the tests



2. The effectiveness of the test is checked and documented with the **control test**

Threat-led Penetration Testing



3. If necessary, the **TLPT** can be mapped and evaluated according to the same principle

DORA-Reporting

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

Available 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.

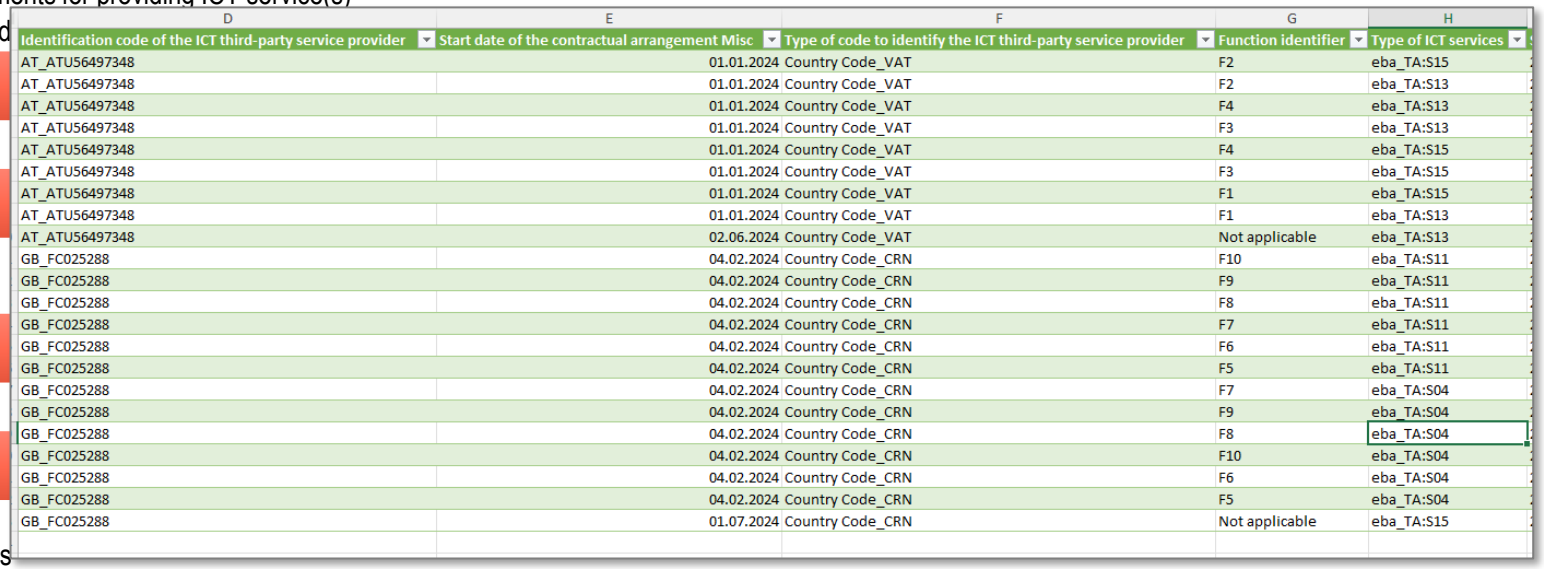
- RT.05.01: ICT third-party service provider
- RT.05.02: ICT service supply chains

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

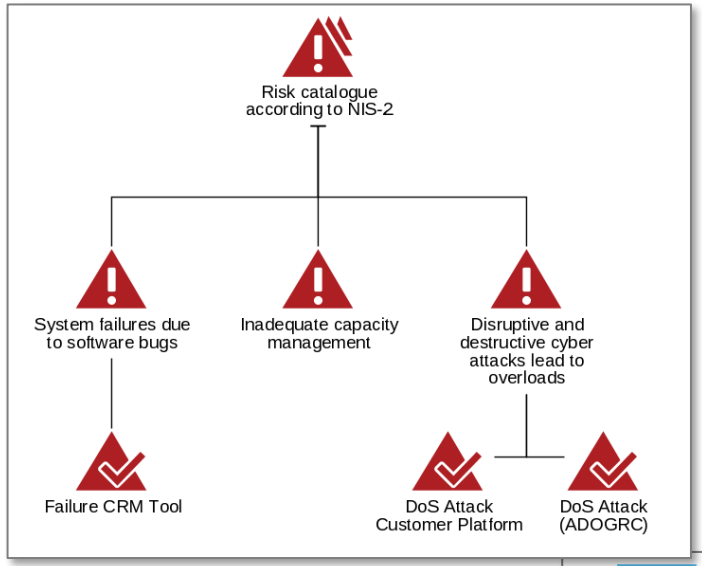
Prospects for NIS-2

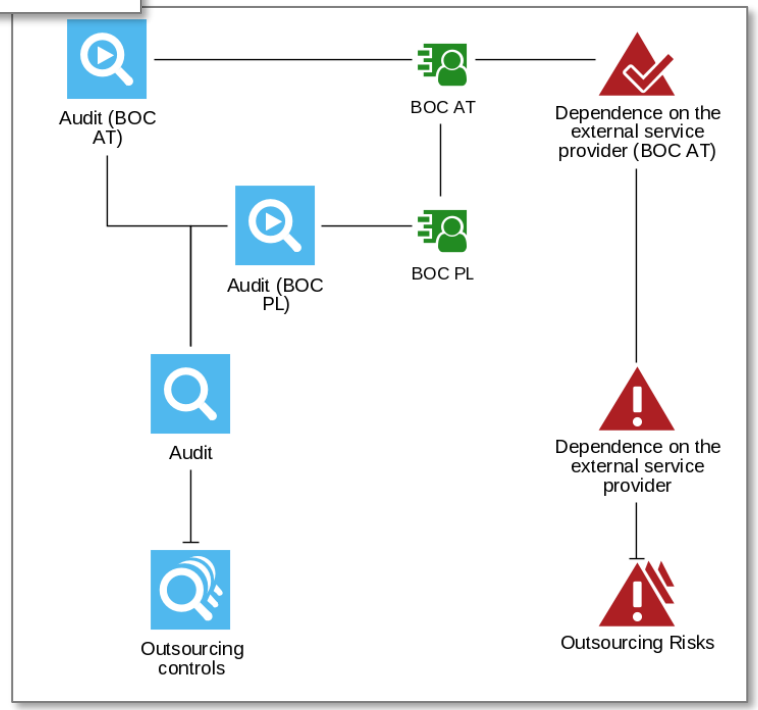
ADOGRC
Governance, Risk & Compliance

NIS2 Directive

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

- Risk analysis and concept for information system security
- Management of security incidents
- Supply chain security
- Business Continuity and Crisis Management
- Security measures for acquisition/ development/ maintenance of ICT applications
- Policies for cyber hygiene, access control and cryptography

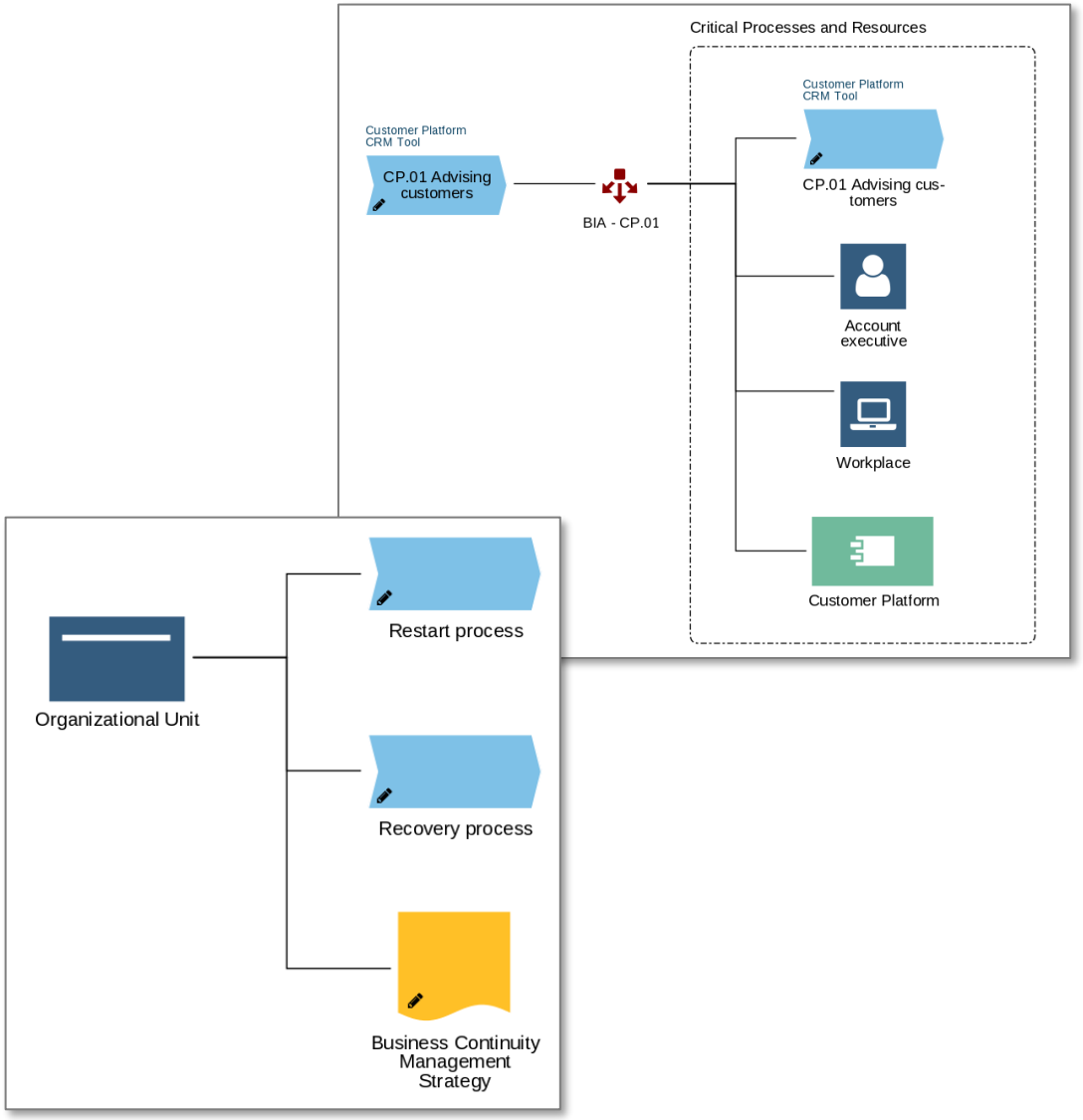




NIS2 Directive

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

- Risk analysis and concept for information system security
- Management of security incidents
- Supply chain security
- **Business Continuity and Crisis Management**
- Security measures for acquisition/ development/ maintenance of ICT applications
- Policies for cyber hygiene, access control and cryptography



Summary

ADOGRC
Governance, Risk & Compliance

ADOGRC supports you with

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

DORA

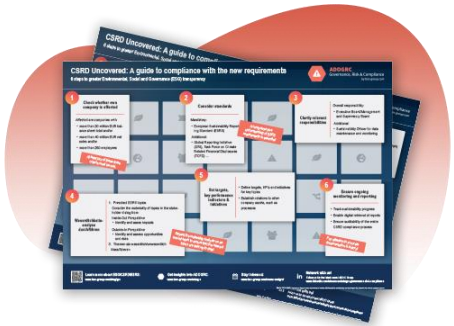
- ICT Risk Management (incl BCM)
- Managing ICT risks originating from third-party providers (incl RoI)
- Testing digital operational resilience
- Management of ICT-related incidents
- Agreements on information sharing
- Oversight of critical third-party providers

NIS 2

- Risk analysis and concept for information system security
- Business Continuity and Crisis Management
- Supply chain security
- Management of security incidents
- Security measures for acquisition/ development/ maintenance of ICT applications
- Policies for cyber hygiene, access control and cryptography

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!