Burda...

ISMS using the example of a media and technology group

1
Scoping

2
Organisation

3
History

4
Governance

5
Risk

6
Compliance

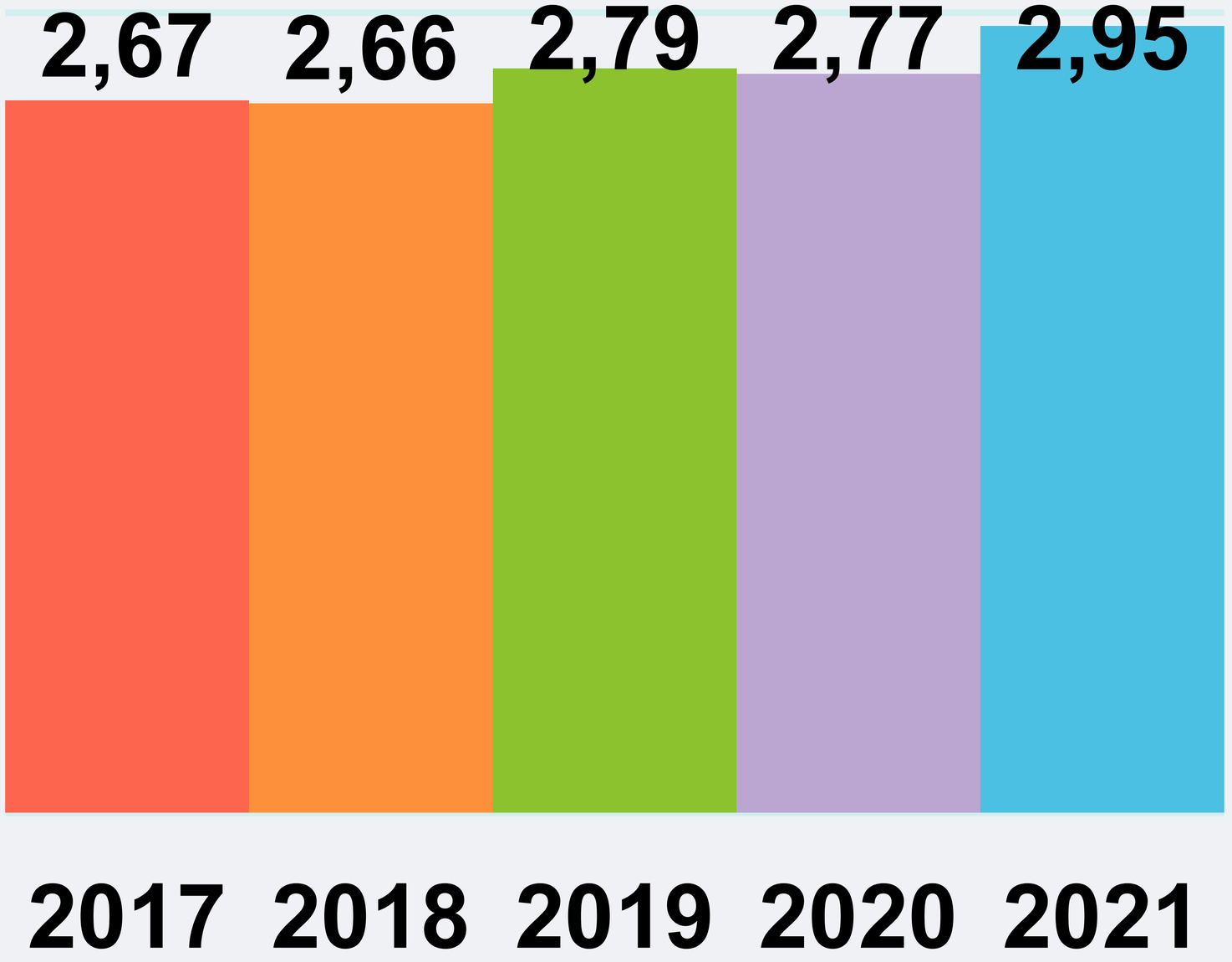
7
ISMS

8
ISMS tool

9
Outlook & Lesson Learned

1 Scoping

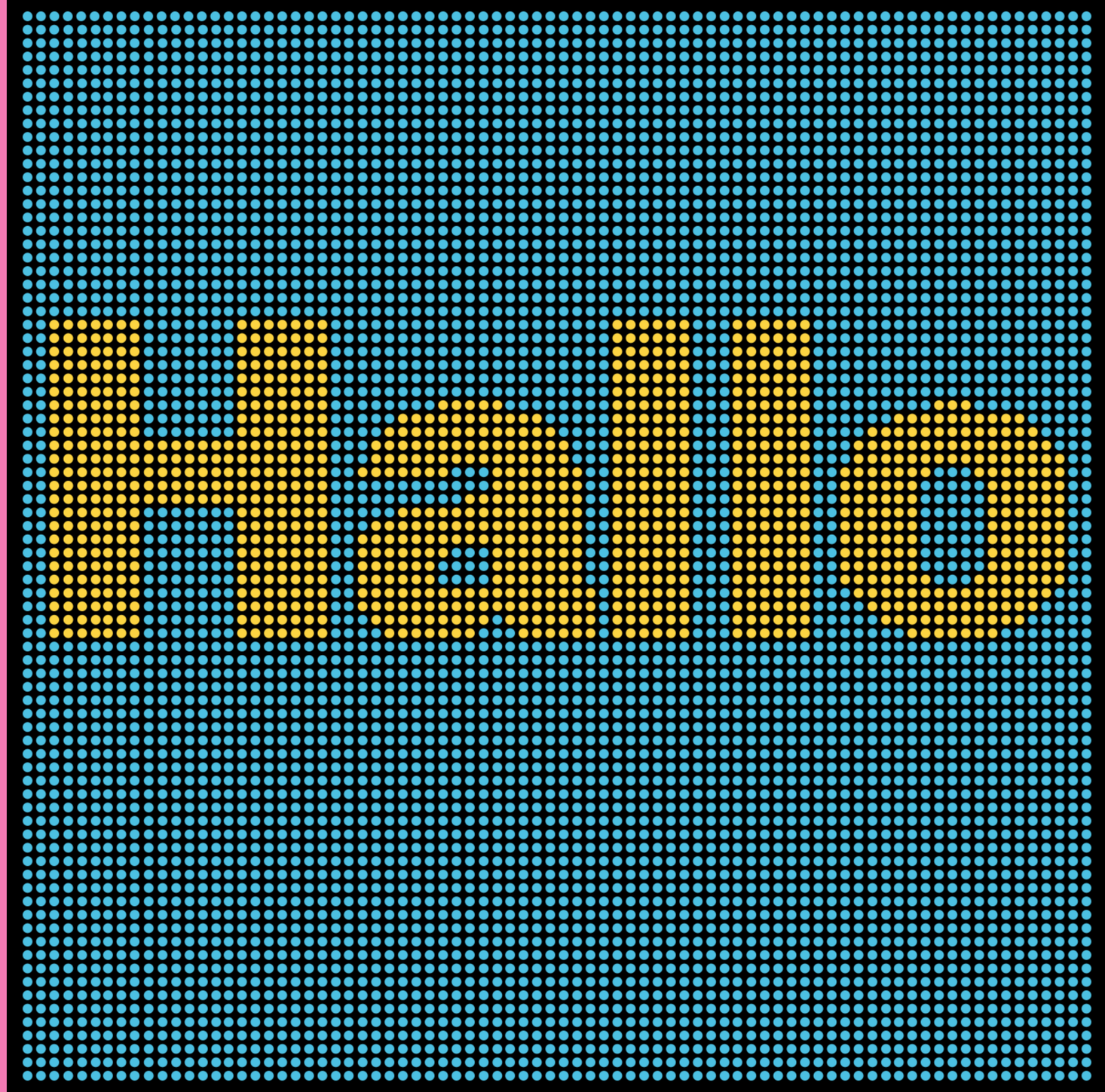
Turnover in EUR bn



Consolidated turnover

10.500 Employees

Year end 2021



Fashion & Beauty	burda style, freundin, Harper's BAZAAR, InStyle, SHOW ROOM, ELLE
Garden	mein schöner Garten, garten spaß, GARTEN Träume, LandEdition
Holiday trip	HolidayCheck.com, zoover, MietwagenCheck.de
News	FOCUS, FOCUS ONLINE, THE HUFFINGTON POST, The Weather Channel, Finanzen100
Occupation	XING, kununu, JOBBÖRSE·COM Ein Service von XING
Entertainment	BUNTE, cinema, FREIZEIT REVUE, Lisa, TV SPIELFILM
Food	meine Familie & ich, Das Kochrezept, Sweet Dreams, GUT EINKAUFEN MIT FREUDE KOCHEN das schmeckt!, Bon Gusto
Lifestyle	fit FOR FUN, PLAYBOY, Silkes Weinkeller
Consumer Tech	CHIP, cyberport, computeruniverse
Living	ELLE DECORATION, home & style, Das Haus, Wohnen & Garten
Health	FOCUS GESUNDHEIT, jameda, FOCUS DIABETES

BurdaDirect

BurdaDruck

BurdaForward

BurdaHome

BurdaInternational

BurdaLife

BurdaNews

BurdaPrincipal Investments

BurdaServices

BurdaStudios

BurdaStyle

BurdaTech

BCN.

C3

Blue Ocean

HolidayCheck GROUP

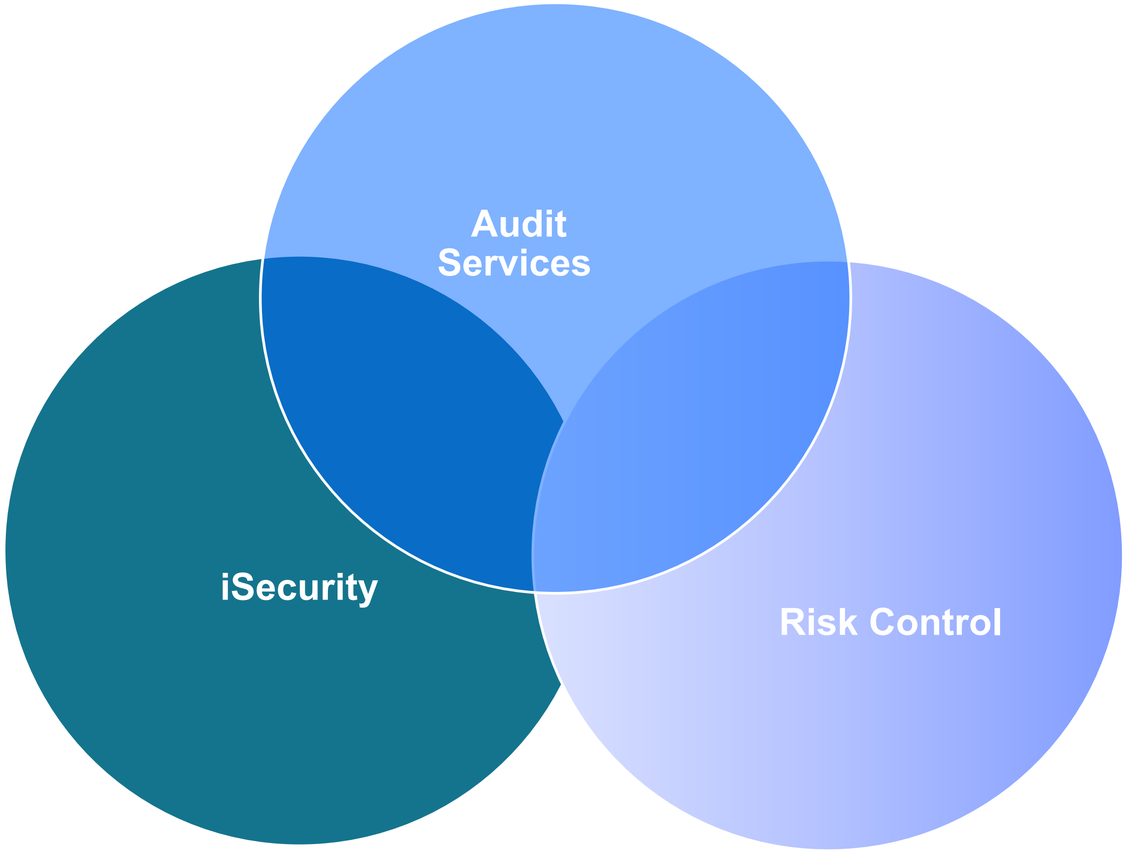
XING

International presence

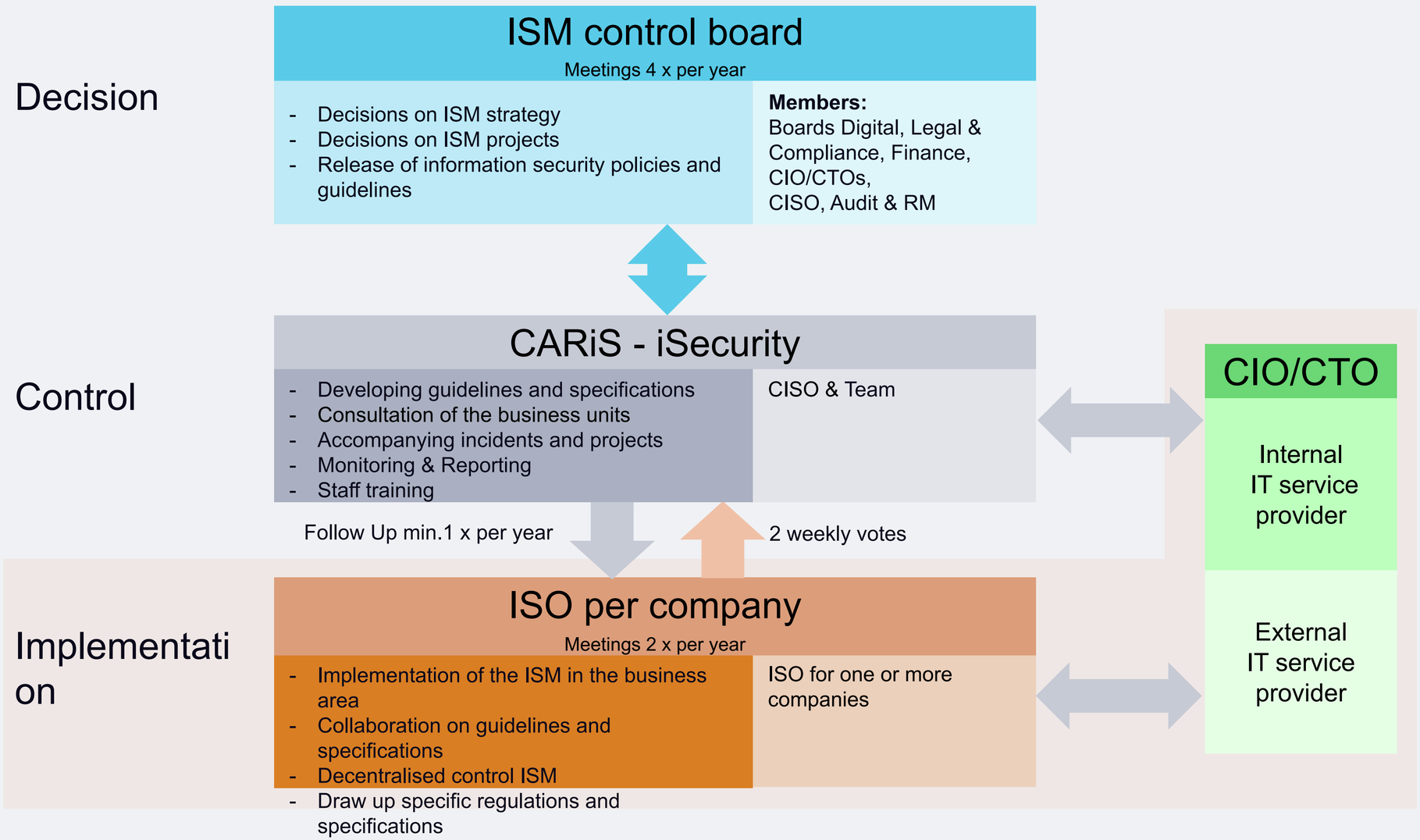
Germany
Africa
Brazil
France
Hong Kong
India
Kazakhstan
Malaysia
Poland
Portugal
Romania
Singapore
Spain
Taiwan
Thailand
Czech republic
Turkey
UK
USA

2 ISMS organisation

Corporate Audit, Risk & iSecurity (CARiS) supports and relieves management in its duty of corporate monitoring

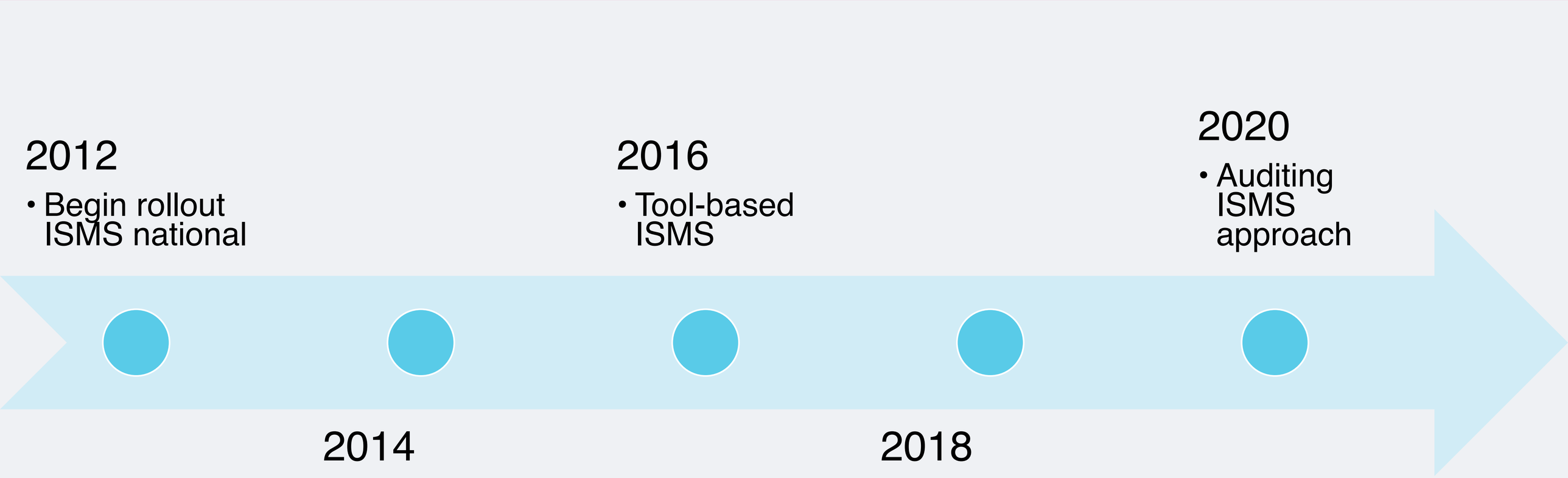


The ISMS is based on central control and decentralised responsibility in the business units



3 History

Baby steps

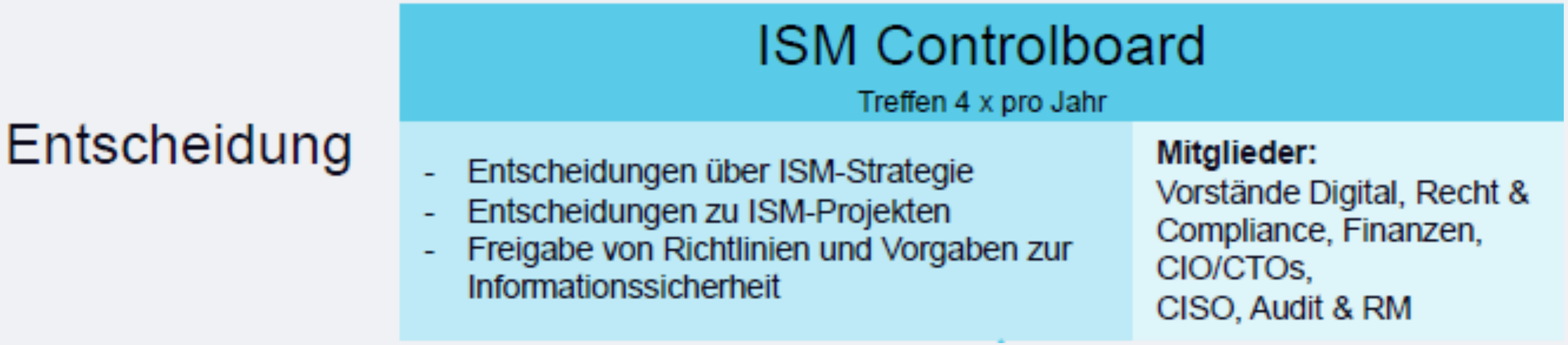

2012
• Begin rollout ISMS national
2014
• Reporting structure via Excel
2016
• Tool-based ISMS
2018
• Begin rollout ISMS internationally
2020
• Auditing ISMS approach

4

Governance

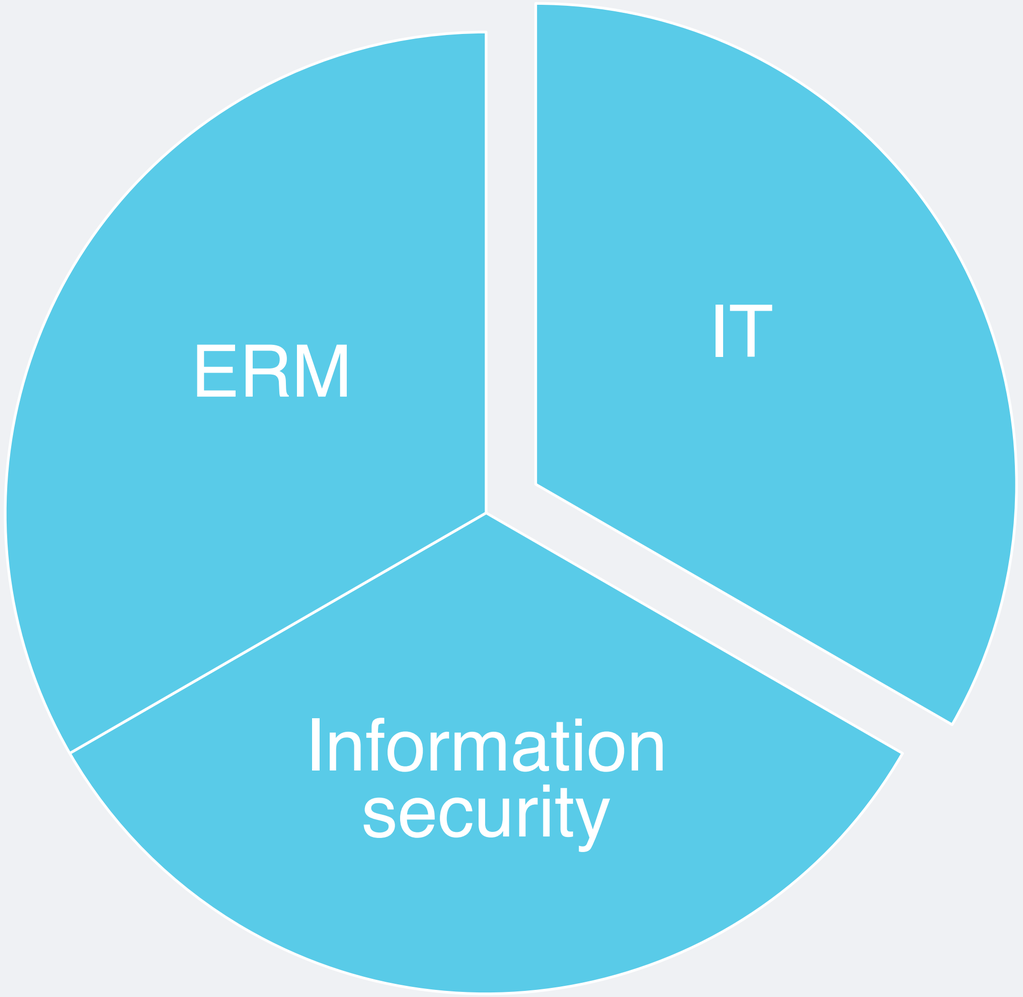
Implementation of the governance function at HBM

- The **governance function** at HBM is performed by the ISM Control Board, which consists of the highest governance body within the IS organisation. The ISM Control Board:
  - sets out the general direction of information security at HBM;
  - decides on the implementation of essential information security projects;
  - decides on the content, scope and implementation of the Group-wide information security guidelines;
  - decides on contentious issues of information security;
  - represents the interests of information security on the Board of Directors.



5 Risk

Risk management at HBM



6 Compliance

External and internal information security requirements at HBM

- **Contractual requirements**

- **External compliance**
  - EU General Data Protection Regulation (EU-DSGVO)
  - NIS Directive (Digital Service Providers: Search Engines, Cloud Services and Marketplaces)
  - Telemedia Act (TMG) and Telecommunications Act (TKG, in particular §§ 88 ff)
  - Unfair Competition Act (UWG, in particular §17 Betrayal of Business and Trade Secrets)
  - Processing of credit card data (PCI)

- **Internal compliance (Group guidelines)**
  - Information security management
  - Information security for IT services
  - Use of IT and communication systems

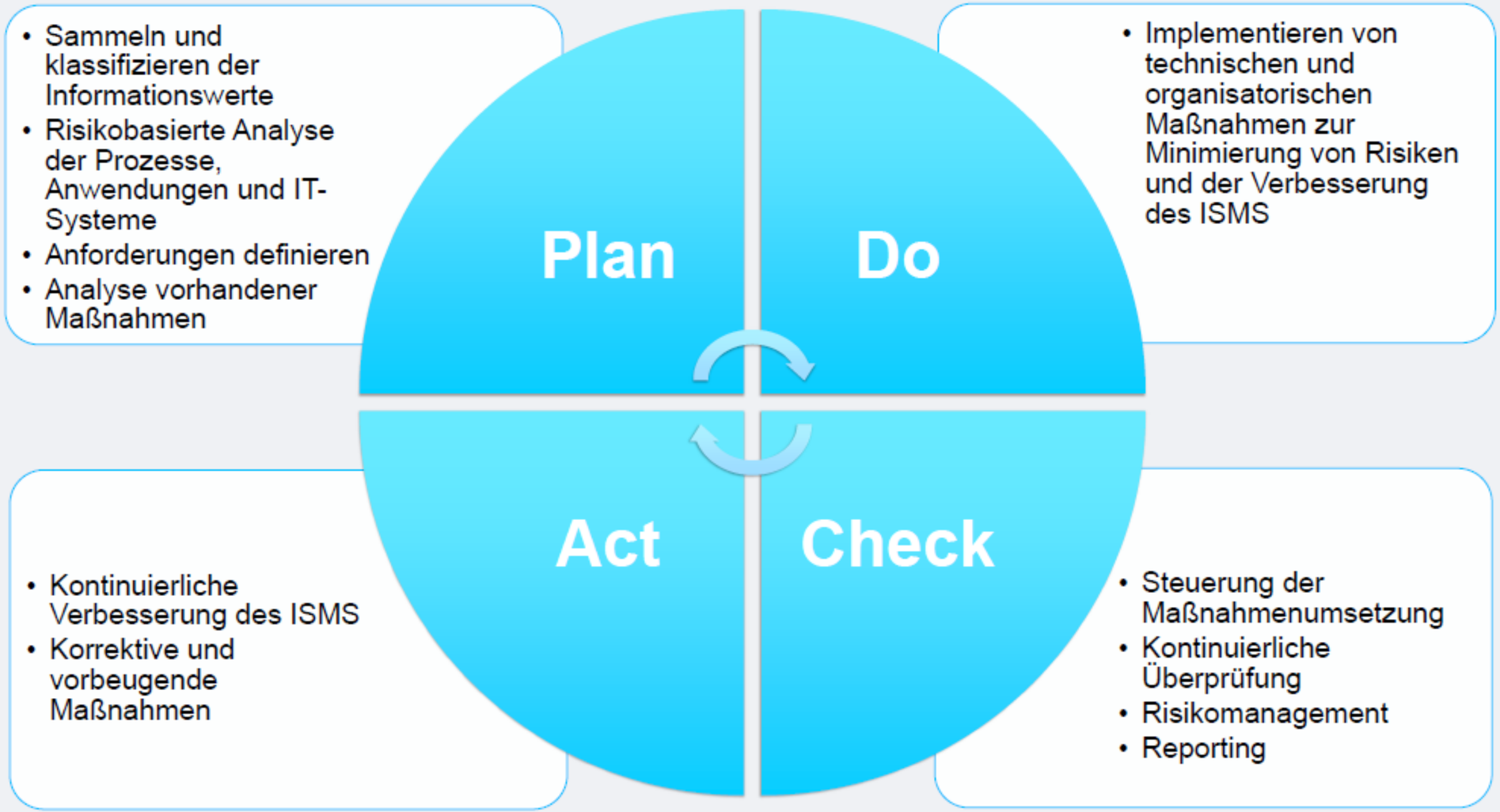
- **Relevant standards with regard to information security**
  - **ISO 27001** (requirements for the introduction, operation, monitoring, maintenance and improvement of a documented ISMS, taking into account the ISec risks within HBM).
  - **BSI** (especially the catalogues of measures for technical infrastructure)
  - **COBIT** (mapping IT processes, maturity model) & **ITIL** (for general mapping of IT service processes)

7 ISMS

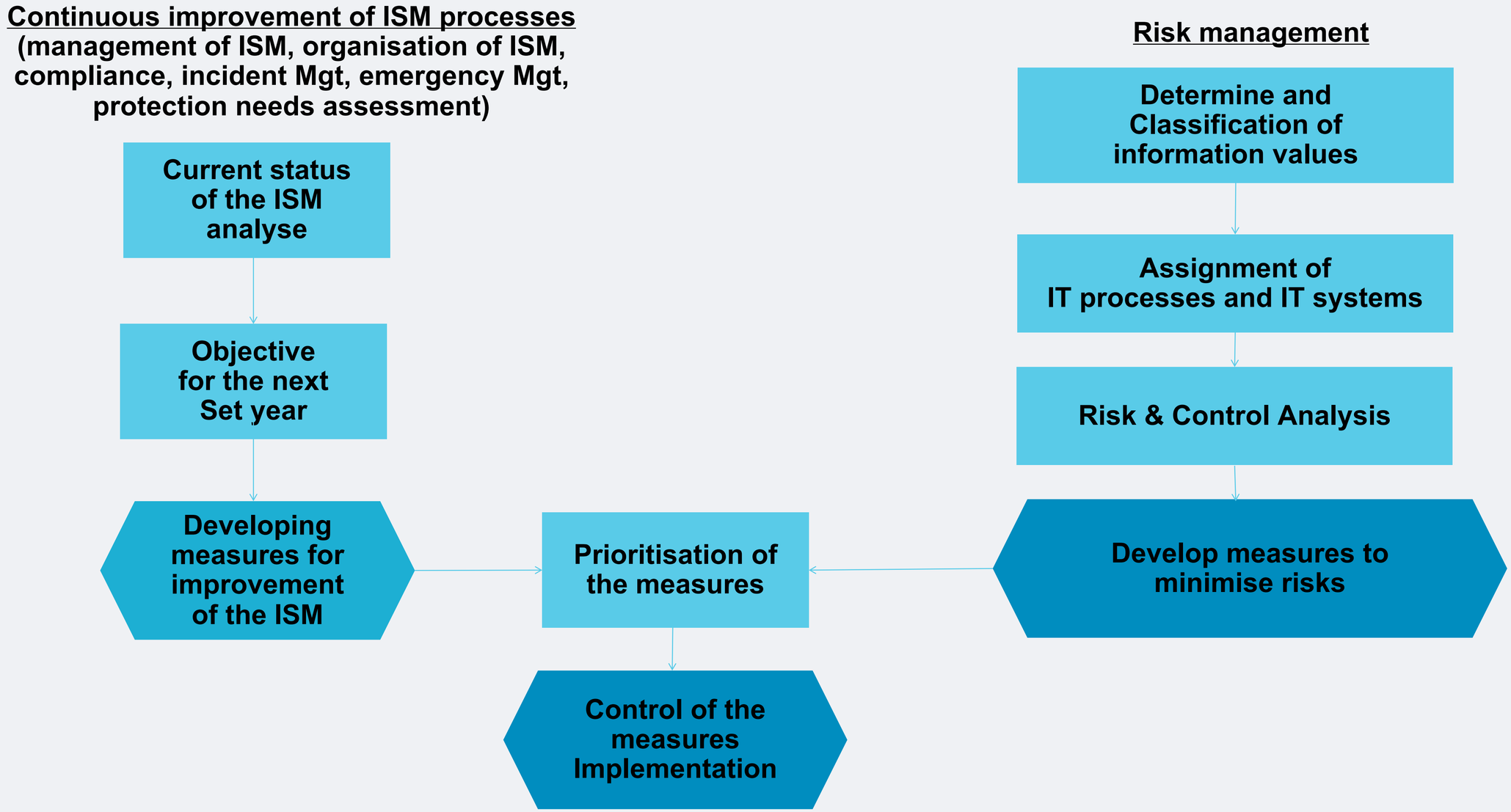
ISMS implementation planning

Phase	Business division
1	Digital Brands National
2	Media Brands National and Burda printing
3	Digital and Media Brands International

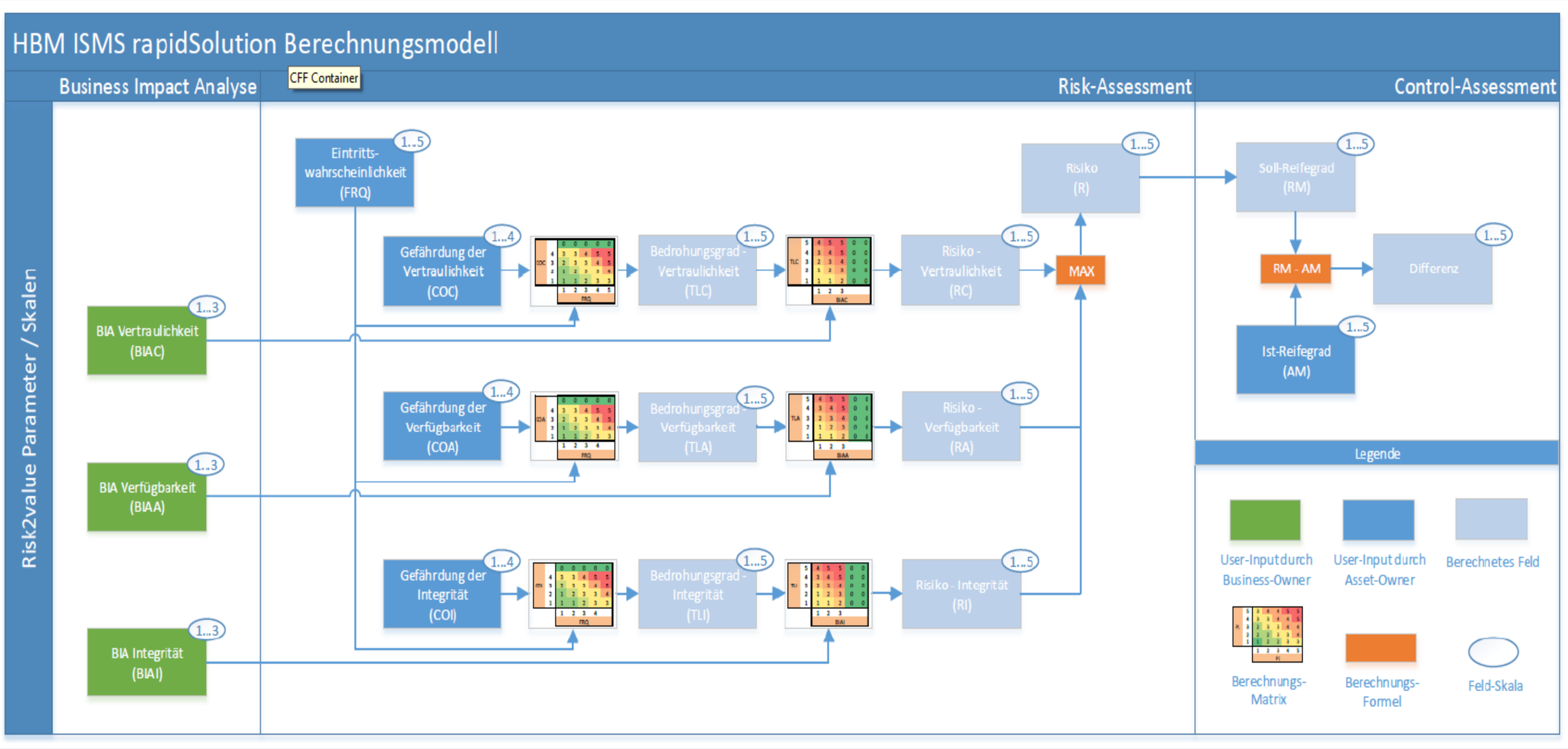
Implementation of the ISMS at HBM 1/3



Implementation of the ISMS at HBM 2/3



Implementation of the ISMS at HBM 3/3



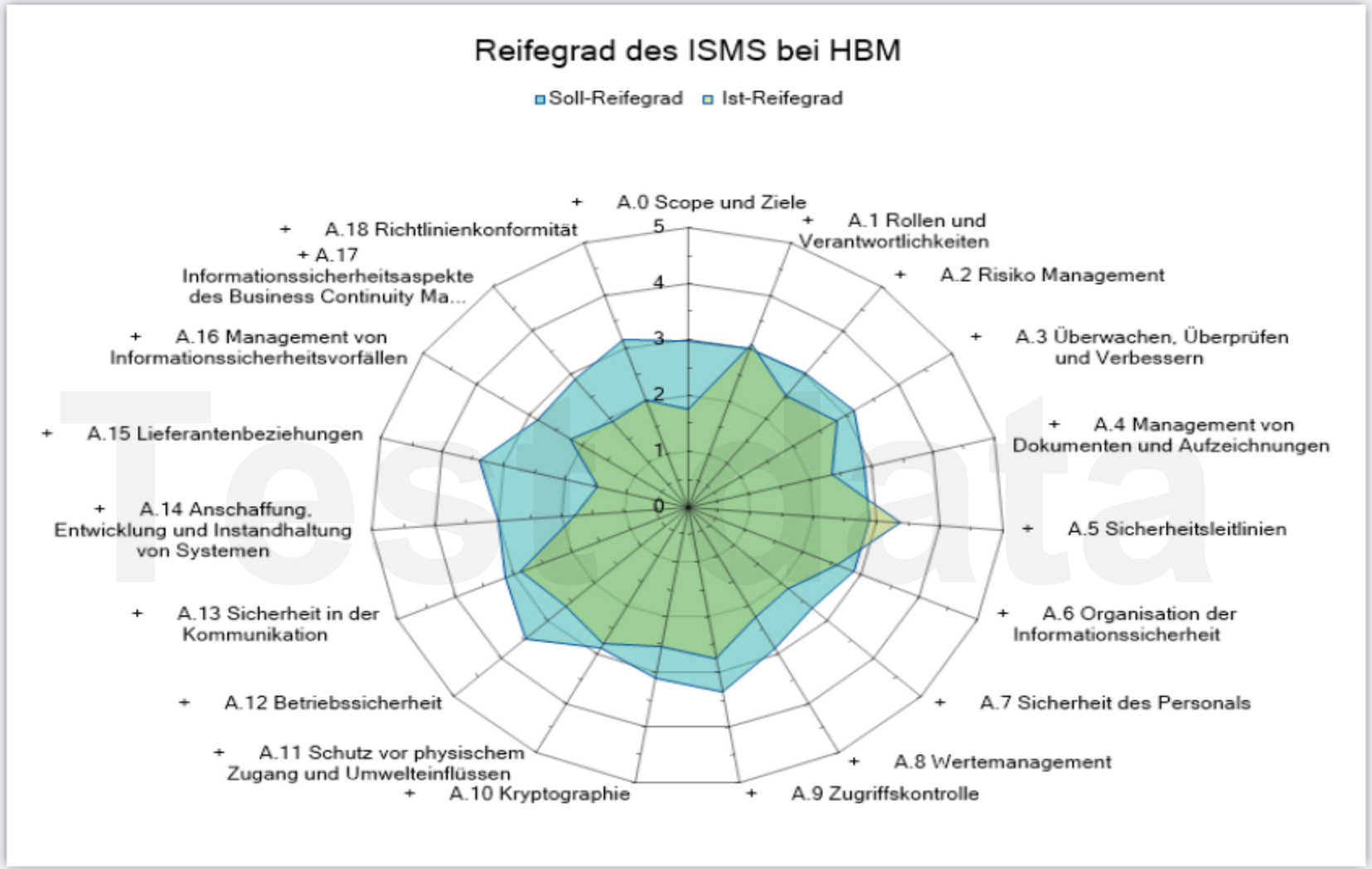
Evaluation of the ISMS at HBM 1/2

COBIT maturity level	
0	Not available
1	Initial
2	Repeatable, but intuitive
3	Defines
4	Controlled and measurable
5	Optimised

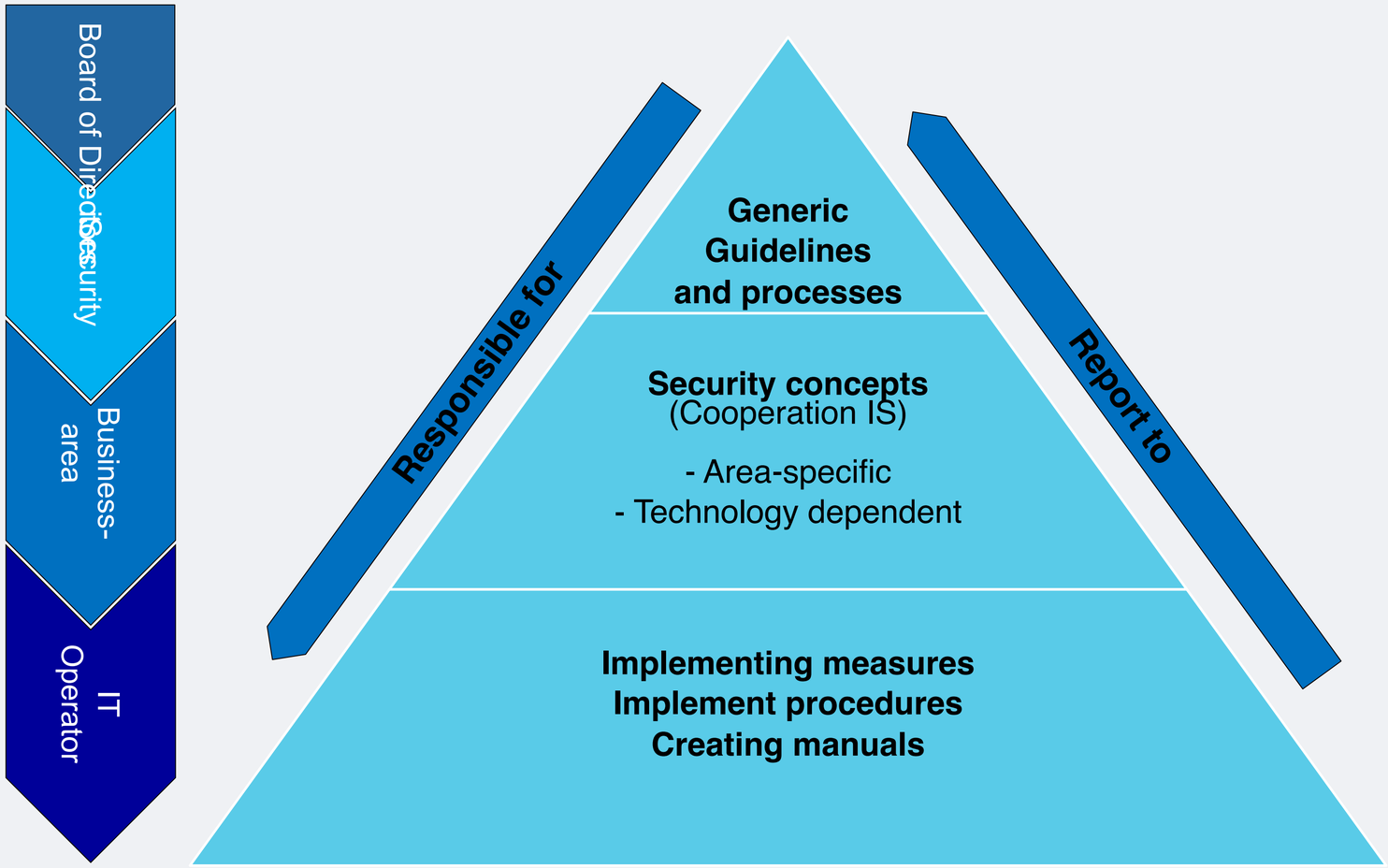
Evaluation of the ISMS at HBM 2/2

Ergebnis der ISM-Bewertung:

sowie des Reifegrads der Kontrollen und Maßnahmen zur Beherrschung der IT-Risiken des Unternehmen in risk2value



Control of the ISMS



ISM Full vs. ISM Lite

- **Two control catalogues are drawn up on the basis of defined criteria**
  - ISM Full: a fully comprehensive implementation of ISM large companies
  - ISM Lite: minimal approach to the implementation of an ISM reduced exposure of the company with regard to information security

Gesellschaft			
Kriterien			
Name der Gesellschaft			
Jahresumsatz in TEUR	<100 € ☐	>100€/<500€ ☐	>500 € ☐
Anzahl MA	Klein<50MA ☐	Mittel>50MA<100MA ☐	Groß>100MA ☐
Marktsituation Hauptmärkte	national ☐	international ☐	EU ☐ außerhalb EU ☐
Datenklassen	Personenbezogene Daten ☐ Kundendaten/Kontakt ☐ besonders schützenswerte Daten ☐		
Visibilität	innerhalb HBM B2C ☐ Branche bzw. B2B ☐		
Abhängigkeit IT	Gering ☐	Mittel ☐	Hoch ☐
Beteiligungsverhältnisse HBM (K.O.Prinzip)	< 50 % K.O. ☐	> 50 % ☐	
Unternehmensreife	Startup 1-3 Jahre ☐	switch < 5 Jahre bzw. 1 jährige Betriebszugehörigkeit ☐	Etabliert>5Jahre ☐ Um-strukturierung ☐
Standorte	national ☐	international ☐	EU ☐ außerhalb EU ☐
Unternehmensaktivität verstehen	**Details (optional)**		
Business			
Kunden			
Compliance-Anforderung			
Markt			
Stake-Holder			
IT-Mitarbeiter Anzahl			
Admins/Programmierer Anzahl			
Aufnahme			
Infowerte (BIA)			
IT - Landschaft (grob)			
Ergebnis	Lite ☐	Full ☐	
Begründung			
Name:		Datum:	

8 ISMS tool

Excel questionnaire

- On the basis of a standardised hazard catalogue, the IT systems recorded are evaluated with regard to possible hazards, the effects of the hazards on the protection goals (confidentiality, integrity, availability) and the probability of occurrence.

Quick Assessment Informationssicherheit

Nr.	Thema	Frage	Antwort	Feststellung	Risiko/Bewertung	ISO 27001 Referer	Bewertung						
							0	1	2	3	4	5	Gesamt
							nicht existent	Initial	wiederholbar, aber intuitiv	definiert	gesteuert und messbar	optimiert	
A	Management der Informationssicherheit												0,00
A.1	Scope und Ziele												0,00
A.1.1		Sind der Scope und die Ziele des Unternehmens hinsichtlich Informationssicherheit durch das Top Management klar formuliert?				5.1; A.6.1.1							---
A.1.2		Werden dedizierte Ressourcen für Informationssicherheit in Form von Mitarbeitern, Zeit und Budgets bereitgestellt?				5.2							---
A.2	Rollen und Verantwortlichkeiten												0,00
A.2.1		Sind Aufgaben, Verantwortlichkeiten und Kompetenzen hinsichtlich Informationssicherheit durch das Top Management eindeutigen Rollen zugewiesen?				5.1							---

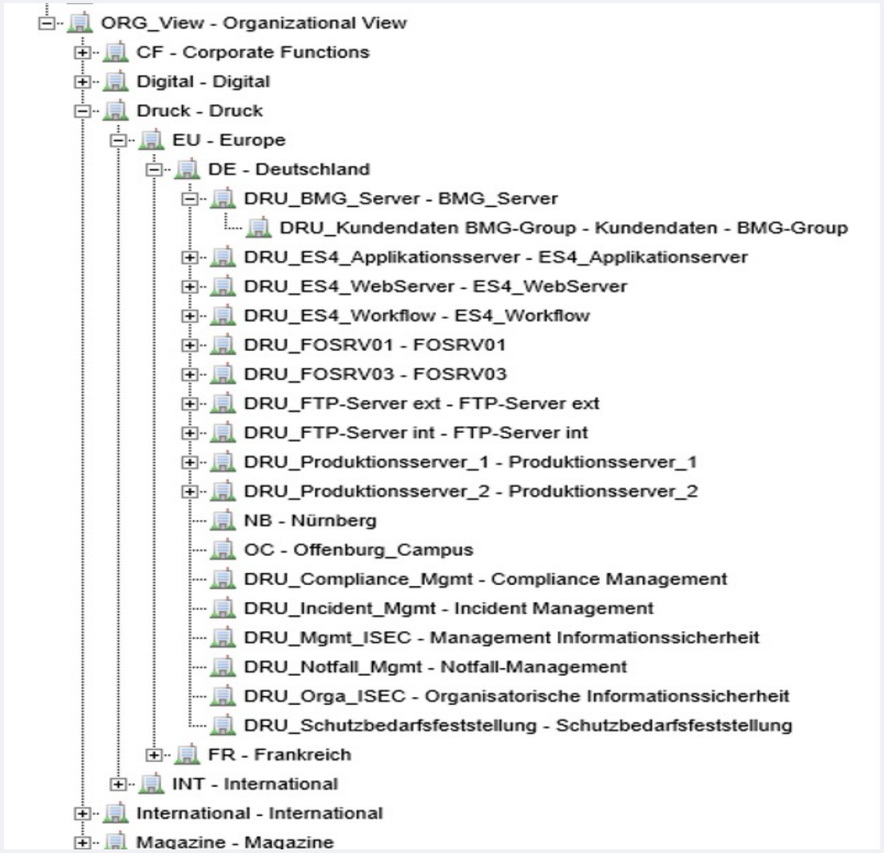
GRC tool

- **Definition**
  - GRC is the integrated collection of functions that enable an organisation to reliably achieve goals, eliminate uncertainty and act with integrity.

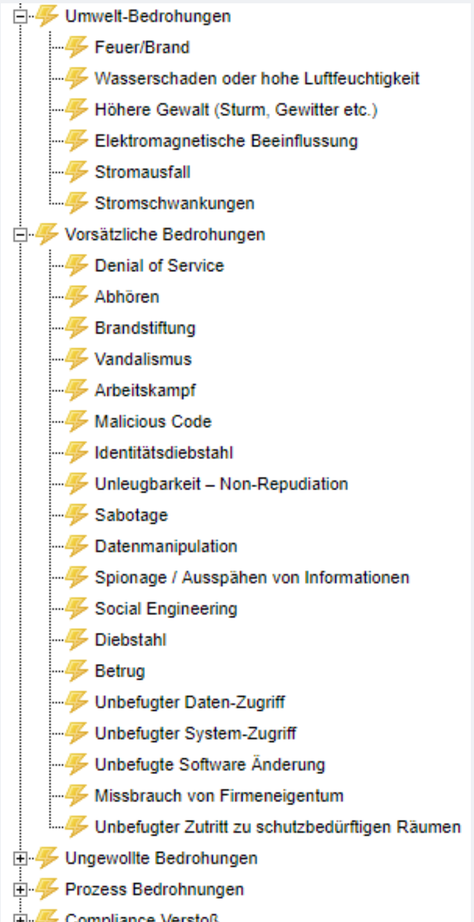
Tool: risk2value

- The implementation of the measures is currently controlled with the help of the company's own ISM application (**risk2value** by avedos business solutions GmbH).

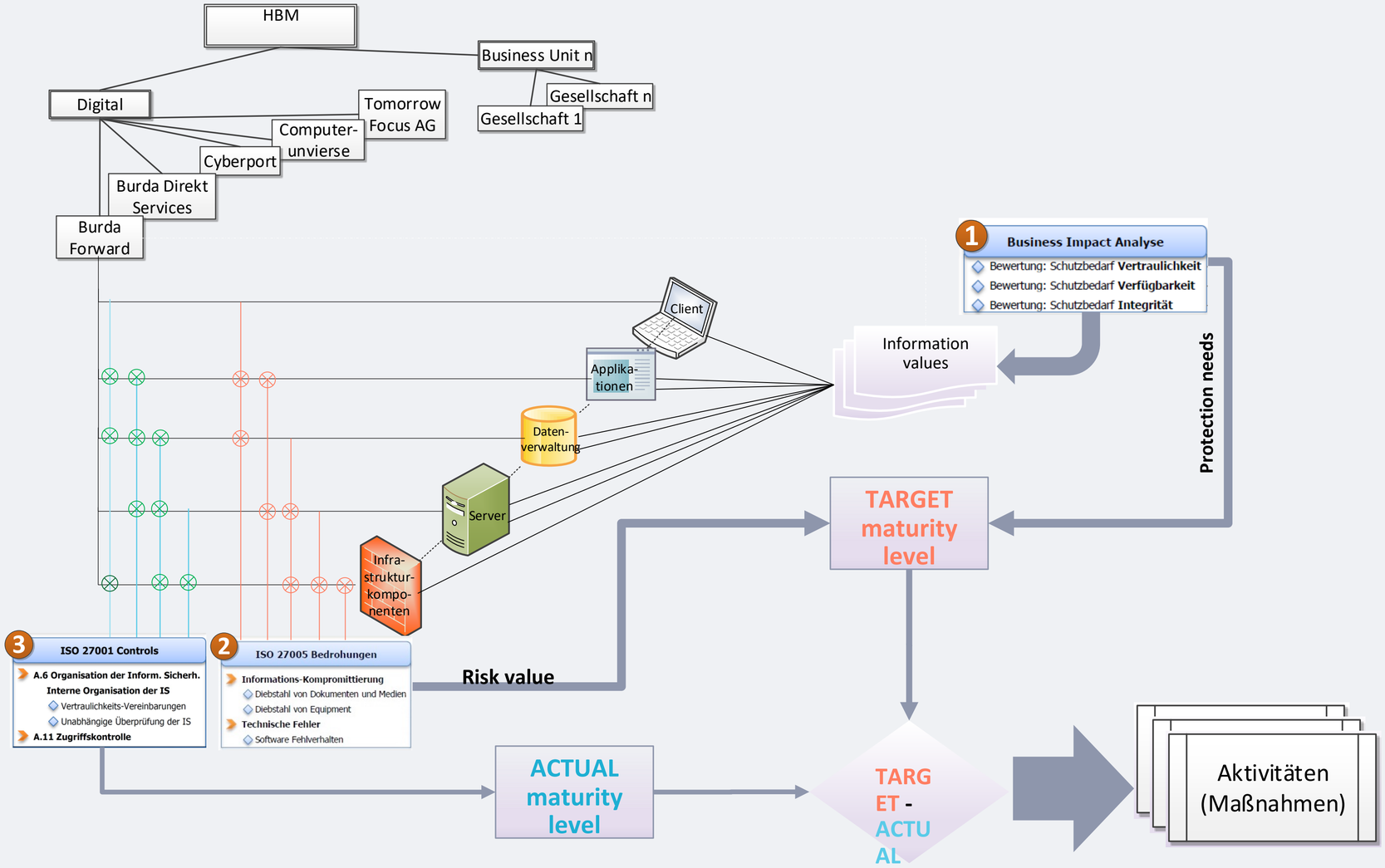
Overview and documentation of information assets and IT systems



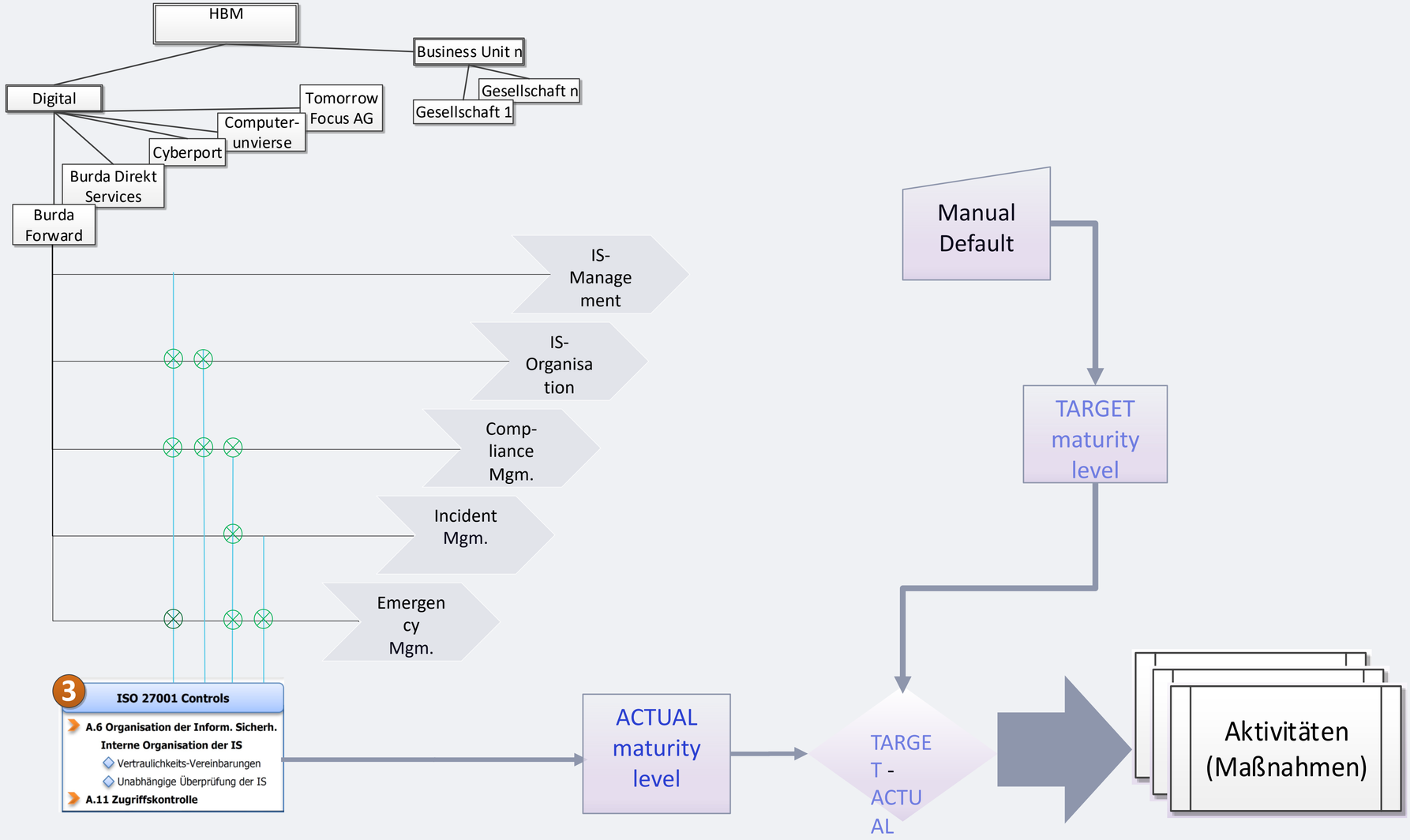
Overview and documentation of IT risks



ISec risk management is mapped in risk2value
Valuation of the assets



Evaluation of the ISM processes



9

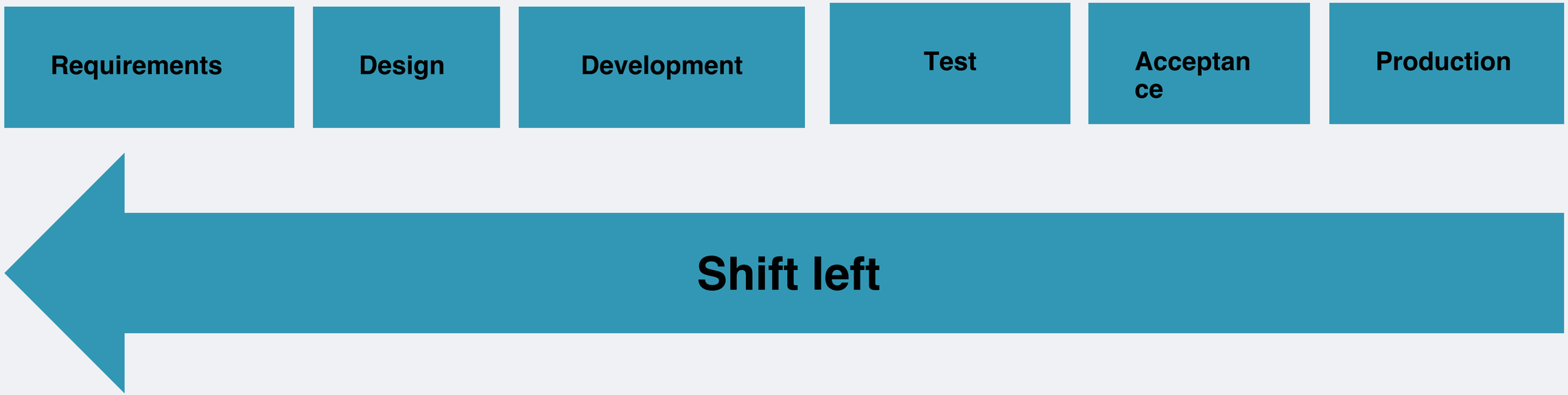
Outlook & Lesson Learned

Outlook

- Auditing approach
- CERT/SOC
- Build up staff

How do we get involved earlier in IT projects with ISM relevance?

Shift left


Requirements
Design
Development
Test
Acceptan
ce
Production
Shift left

Burda...