

IT Governance – aktuelle Chancen und Herausforderungen

Dornbirn, 25. Juni 2025

Ralf Kimpel

Vorstellung

Ralf Kimpel

- Von 1991 bis 2007 als **Wirtschaftsprüfer und Risikomanagement-Berater** bei KPMG und Deloitte tätig
- Seit 2008 als **Direktor** bei der **Hubert Burda Media-Gruppe** für den Governance-Bereich **Corporate Audit, Risk & Insurance** zuständig; bis 31.12.2024 verantwortlich für **Information Security**
- Vorsitzender des Beirats des Berufsverbandes der **RMA Risk Management & Rating Association e.V.** (2014 bis 2024 Vorsitzender des Vorstands)
- Mitglied im **Deutschen Institut für Interne Revision**
- **Certified Internal Auditor**
- **Certification in Risk Management Assurance**



Let's connect



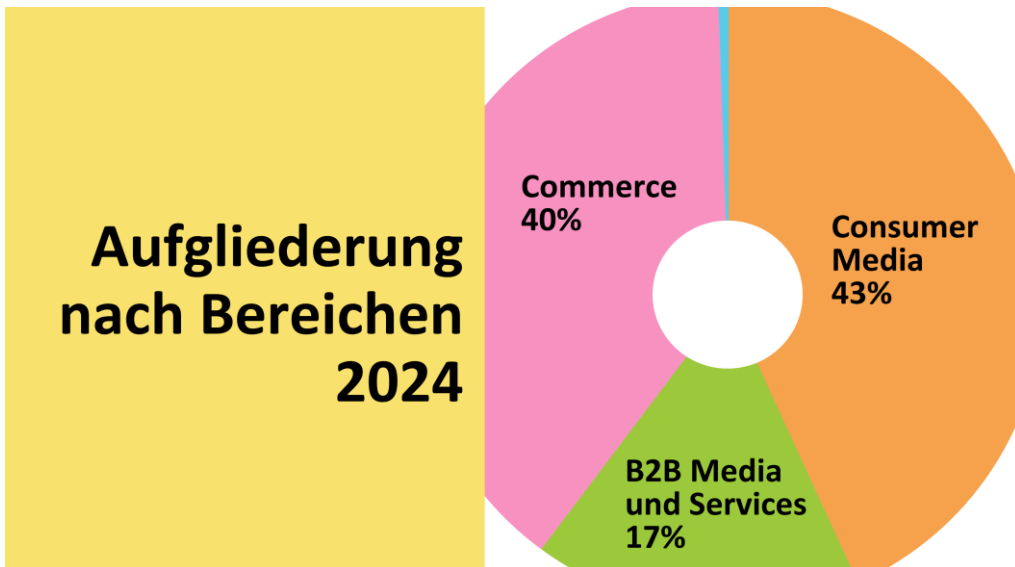
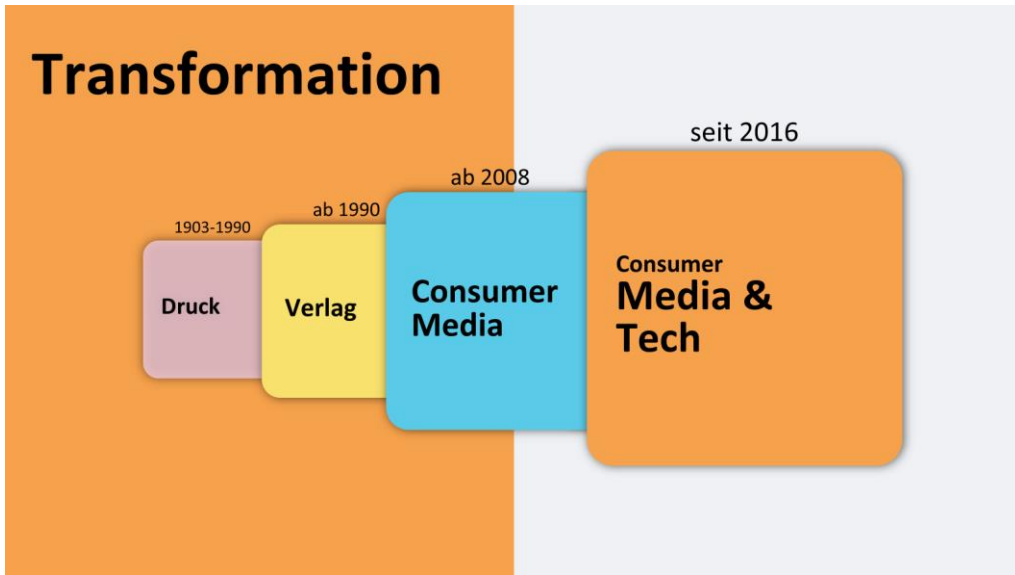
Agenda

1. Hubert Burda Media im Überblick

2. Anforderungen an die IT Governance in Unternehmen

3. Umsetzung in der Praxis von Hubert Burda Media

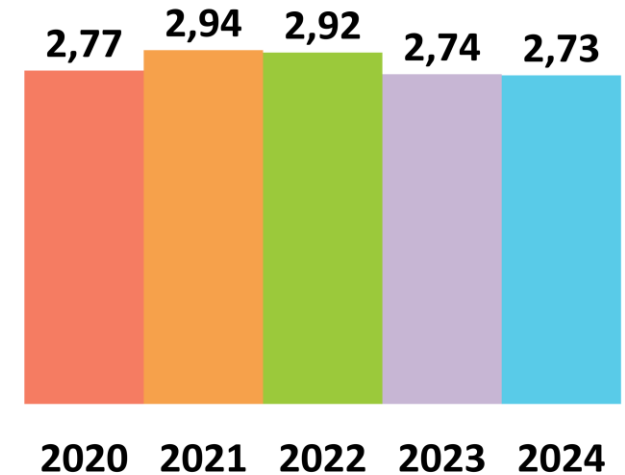
Hubert Burda Media ist...



Hubert Burda Media

Umsatz in Mrd.EUR

Konsolidierte Umsatzerlöse



Fashion & Beauty	burda style	freundin	BAZAR	InStyle	ELLE
Garten	Garten	garten spitz	GARTEN	LandEdition	
Urlaubsreise	HolidayCheck	HolidayCheck Reisen		Mietwagen Check.de	
News	FOCUS	ONLINE FOCUS	The Weather Channel	Finanzen100	
Beruf	XING	kununu	Honeypot	InterNations	
Unterhaltung	BUNTE	cinema	FREIZEITREVUE	Lisa	TV SPIELFILM
Food	tdt	Das Kochrezept	my Sweet Plans	das schmeckt!	einfach backen
Lifestyle	fit	Esquire	InStyle	SILKES WEINKELLER	
Consumer Tech	CHIP		cyberport	computeruniverse	
Wohnen	ELLE DECORATION	DasHaus	Wohnen & Garten	WOHNEN	
Gesundheit	FOCUS GESUNDHEIT		NetDoktor	my life	

Werte & Verantwortung bei Burda – ein Familienunternehmen

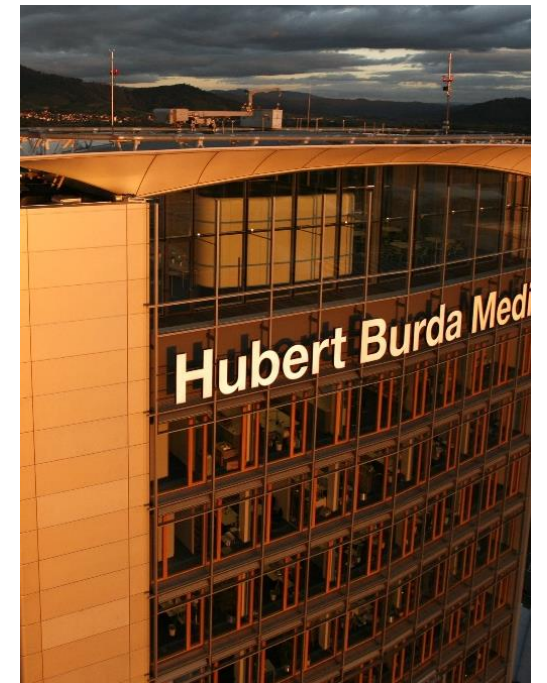


Burda in Unternehmenswerten („Purpose“)

1. Vielfalt
2. Unternehmertum
3. Verantwortung

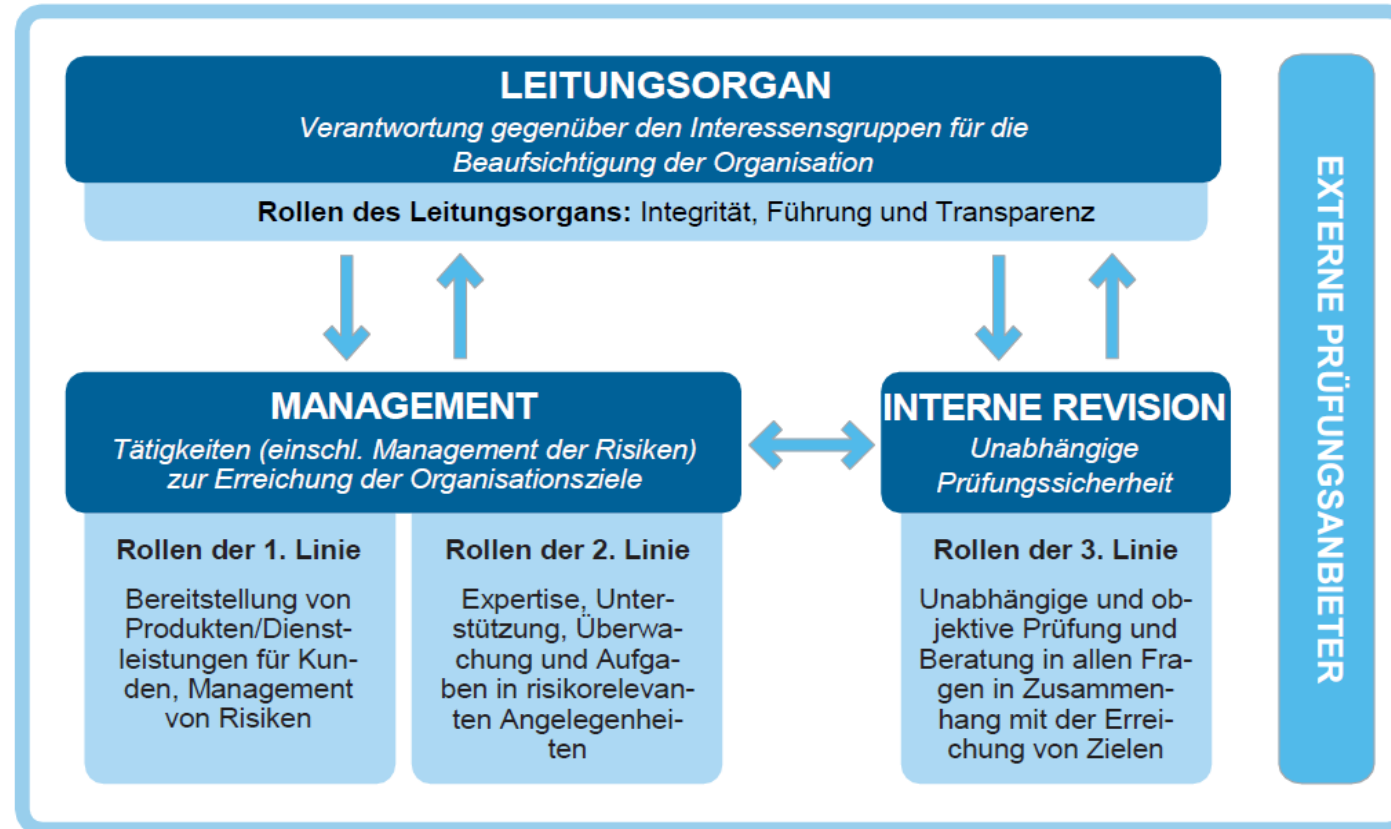
Burda in Zahlen (2024)

- Umsatz: 2,7 Mrd. €
- Mitarbeitende: > 9.500
- Länder: 12
- Reichweite: > 60 Mio.
- Brands: > 500



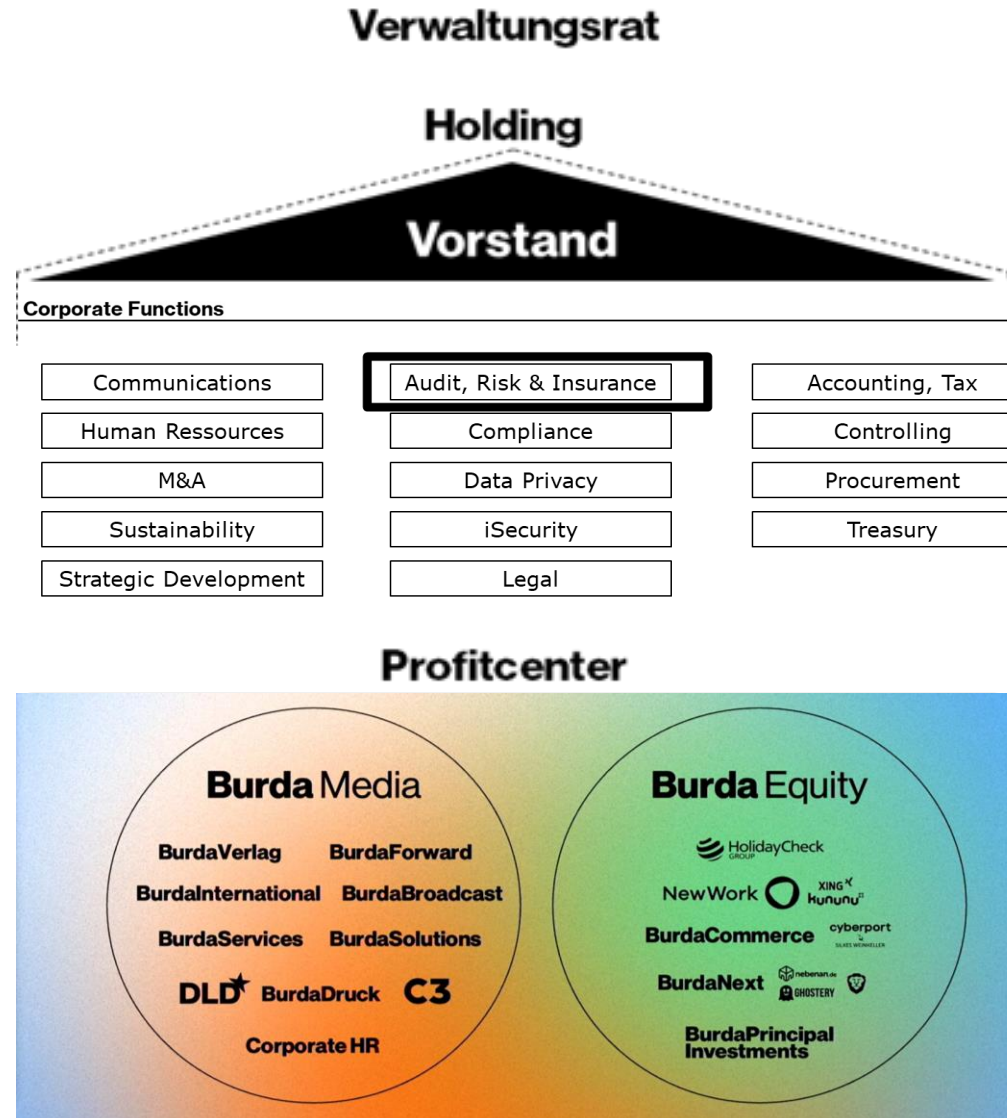
Das 3-Linien-Modell des DIIR/IIA bildet die Grundlage für unser Governance-Modell

Das IIA Drei- Linien-Modell



LEGENDE: ↑ Verantwortung, Berichterstattung | ↓ Delegation, Leitung, Ressourcen, Beaufsichtigung | ↔ Ausrichtung, Kommunikation, Koordination, Zusammenarbeit

Risikomanagement als zentraler Baustein der Unternehmenssteuerung



Agenda

1. Hubert Burda Media im Überblick

2. Anforderungen an die IT Governance in Unternehmen

3. Umsetzung in der Praxis von Hubert Burda Media

Definition von IT Governance (Gabler-Wirtschaftslexikon)

„IT Governance bezeichnet den rechtlichen und faktischen **Ordnungsrahmen für die Leitung**, Organisation (prozessual wie aufbauorganisatorisch) **und Überwachung der IT eines Unternehmens**.

Mit der IT Governance soll sichergestellt werden, dass die **Unternehmensziele durch den IT-Einsatz unterstützt und vorangetrieben** werden.

Es umfasst **Richtlinien, Standards und Verfahren**, die die Nutzung und Verwaltung von IT-Ressourcen im Unternehmen regulieren.“

Herausforderungen für eine angemessene IT Governance

- Die zunehmende **Komplexität und Vielfalt der IT-Systeme** erfordert eine flexible und anpassungsfähige IT Governance!
- Die **Bedrohung durch Cyberangriffe** wächst stetig, Sicherheitsstrategien müssen kontinuierlich angepasst werden (durch KI noch gefährlicher)!
- Die **Verwaltung großer Datenmengen – vor allem pbD - und die Sicherstellung ihrer Vertraulichkeit, Integrität und Verfügbarkeit** stellt eine erhebliche Herausforderung dar!
- Die **Einhaltung ständig wachsender gesetzlicher Vorgaben** kann komplex und ressourcenintensiv sein!

BITKOM-Analyse zeigt Konfliktzonen und Wege zur Kohärenz in der Digitalgesetzgebung auf

Digitalgesetzgebung der EU: Konfliktzonen und Wege zur Kohärenz

Version 1.0 – April 2025

Digitalgesetzgebung der EU: Konfliktzonen und Wege zur Kohärenz

2 Zwischen DS-GVO und ...

Rechtsakt	Problem	Mögliche Lösung
Data Act	<p>Datenzugriffsrechte im Data Act vs. Betroffenenrechte der DS-GVO:</p> <p>Die im Data Act verankerten Zugriffsrechte (Art. 3-5 DA) stehen potenziell in Konflikt mit den Betroffenenrechten der DS-GVO, wie dem Recht auf Berichtigung, Löschung und Einschränkung der Verarbeitung personenbezogener Daten (Art. 16 ff. DS-GVO). Dies kann dazu führen, dass bei der Offenlegung von Daten im Rahmen des Data Act unbeabsichtigt Persönlichkeitsrechte beeinträchtigt werden.</p>	<p>Durch den Einsatz von Pseudonymisierungs- oder Anonymisierungsverfahren kann gewährleistet werden, dass bei der Datenweitergabe keine direkt identifizierbaren personenbezogenen Informationen offengelegt werden.</p> <p>Jedoch ist zu beachten, dass der Einsatz pseudonymer Daten beim DA nicht hilft. Vorschlag daher: gemischte Datensätze werden nicht wie pb-Daten behandelt, wenn die pb-Daten nach anerkannten Standards pseudonymisiert sind und eine Repersonalisierung durch unbefugte Dritte ausgeschlossen ist.</p> <p>Solche Maßnahmen erlauben den Zugang zu den für den Data Act relevanten Daten, ohne die DS-GVO-Bestimmungen zu verletzen.</p> <p>In Fällen, in denen beide Rechtsakte anwendbar sind, sollte geprüft werden, ob die spezifischeren Regelungen des Data Act Vorrang haben – sofern dies mit dem Schutz der Betroffenenrechte vereinbar ist.</p>
Data Act	<p>Rechtsgrundlage der DS-GVO bei divergierenden Rollen von Nutzern und Betroffenen im Data Act:</p> <p>Auf welche Rechtsgrundlage der DS-GVO greift man zurück, wenn Nutzer nach Data Act und Betroffener nach DS-GVO auseinanderfallen?</p>	<p>Siehe grds. Erwägungsgründe 7 und 34 DA. Die Lösung könnte eine Klarstellung im Verordnungstext selbst statt in den Erwägungsgründen sein.</p>
Data Act	<p>Sieht der Data Act die Möglichkeit der Auftragsverarbeitung im Sinne der DS-GVO auch für einen Datenempfänger vor, oder müssen diese die Daten stets selbst verarbeiten: Kann ein Datenempfänger Daten im Sinne einer Shared Data Economy bei Einwilligung des Nutzers durch einen Auftragsverarbeiter verarbeiten lassen?</p>	<p>Der Gesetzgeber sollte explizit bestimmen, unter welchen Umständen die DS-GVO-Grundlagen herangezogen werden und wie im Falle divergierender Definitionen vorzugehen ist. Eine systematische Abgrenzung – etwa über spezifische Anwendungsfälle oder Datenkategorien – kann hier als Leitfaden dienen.</p>
Data Act	<p>Risikopotenzial durch Datenklassifizierung im Data Act:</p> <p>Die Pflicht zur Differenzierung zwischen personenbezogenen und nicht-personenbezogenen Daten und Geschäftsgeheimnissen birgt für Dateninhaber ein erhebliches Risikopotenzial. Unklare oder fehlerhafte</p>	<p>Die Einführung standardisierter, technischer Verfahren zur automatisierten Klassifikation von Daten unterstützt Dateninhaber dabei, ihre Daten korrekt zu kategorisieren.</p>

4

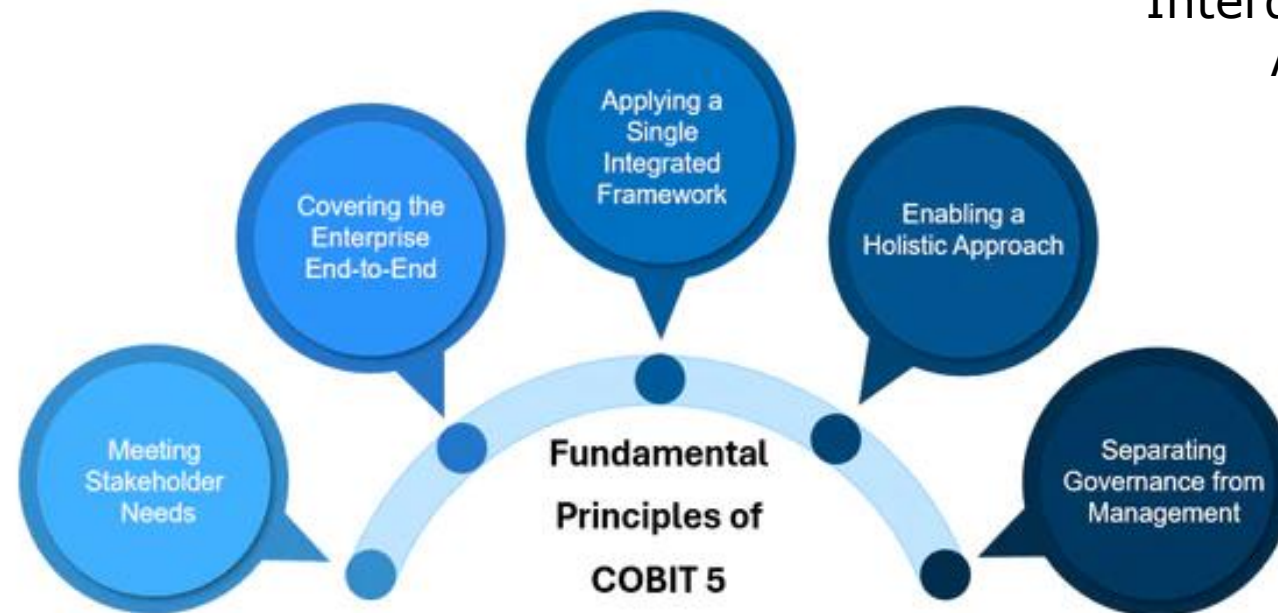
IT Governance Modelle können bei der Etablierung einer guten IT Governance helfen

- ITIL
- ISO/IEC 38500
- ISO/IEC 27000
- COBIT

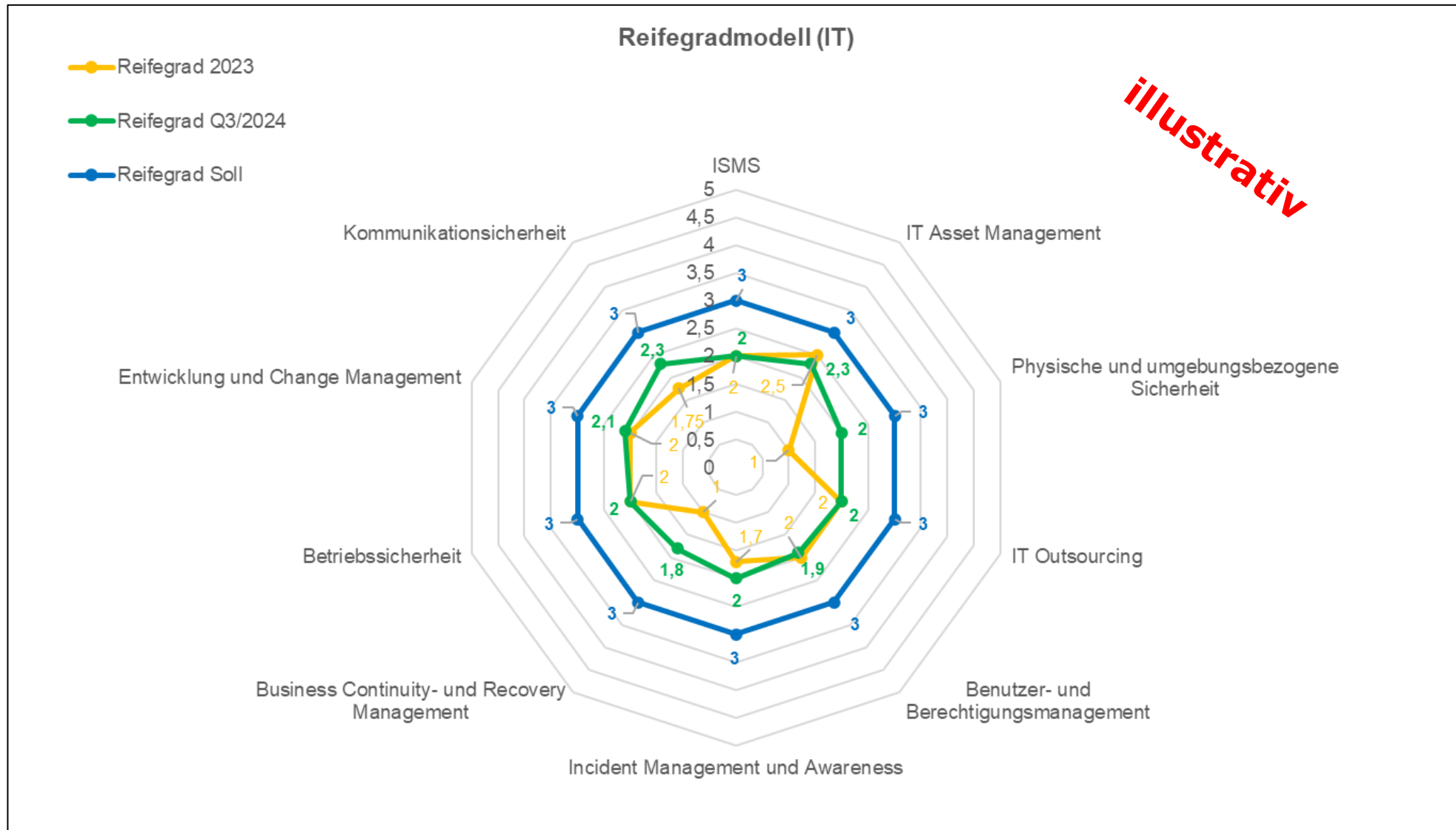
Managementsystem
(PDCA);
Reifegradmodell

Interdisziplinärer
Ansatz

Schutzbedarfsanalysen +
Business Impact Analysis



Mit einem Reifegradmodell kann der Status aufgezeigt und die Weiterentwicklung visualisiert werden



Der RMA-Arbeitskreis Information Risk Management erarbeitet gemeinsam mit der ISACA Best Practice Lösungen

- **IT-Risikomanagement** – leicht gemacht mit Cobit
- Liste der **Top 11 IT-Risiken**
- **Anwendung der ISO 31000 in der IT** (derzeit in Überarbeitung)
- IRM-Leitfadens zur **Risikoidentifikation in der Praxis** (in Arbeit)



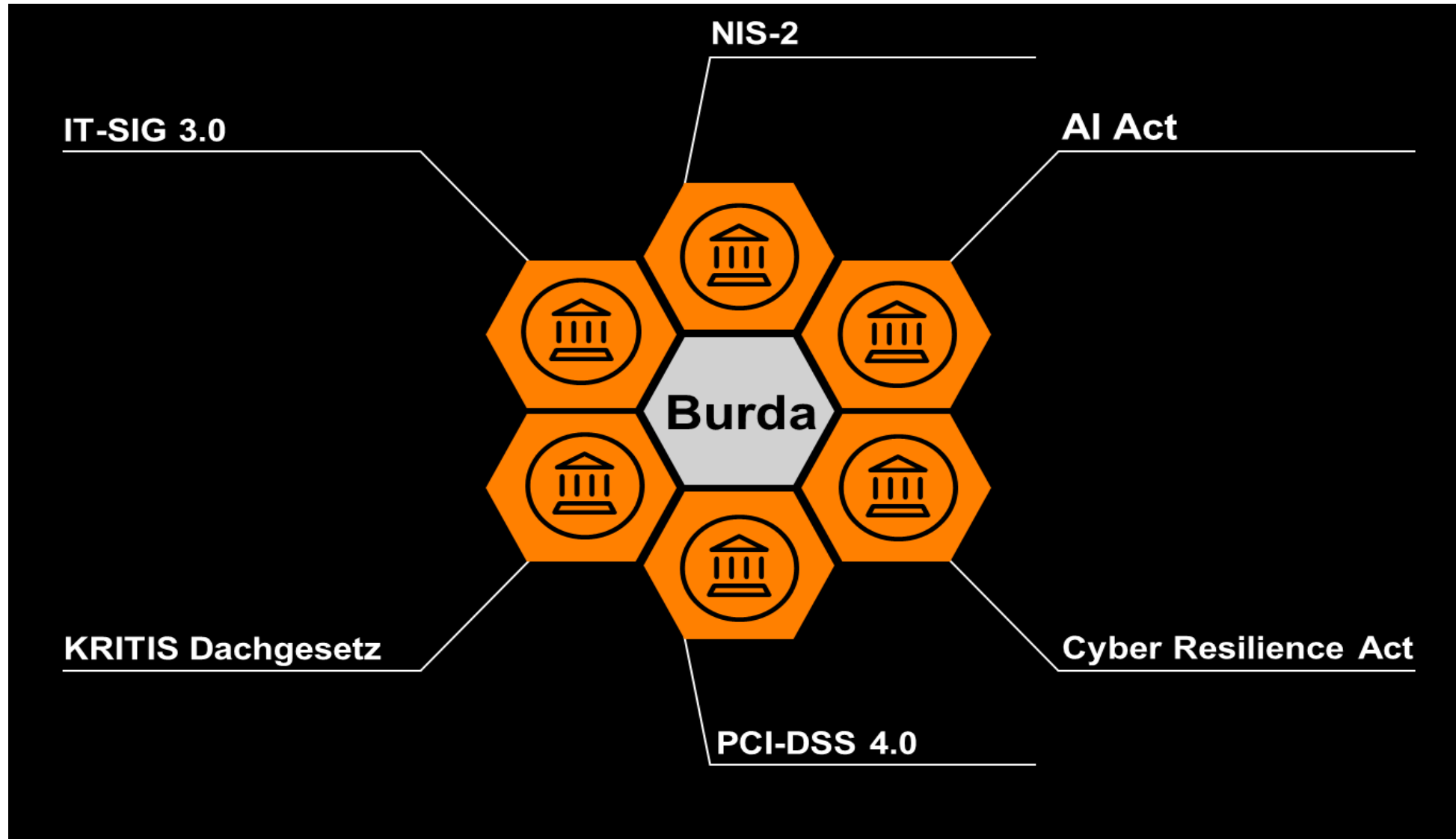
Agenda

1. Hubert Burda Media im Überblick

2. Anforderungen an die IT Governance in Unternehmen

3. Umsetzung in der Praxis von Hubert Burda Media

Regulatorische Anforderungen an die IT Governance bei Burda

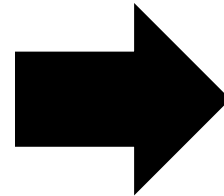


Die (IT) Governance-Organisation bei Burda

Regelwerk

- **Konzernrichtlinien:**
Compliance Board -> Vorstand

- **IT-Konzernrichtlinien:**
Data Governance Board
-> Compliance Board -> Vorstand
- **IT-Prozessvorgaben:**
CISO -> Data Governance Board



Data Governance Board

Team work (mit Vetorecht):

Datenschutz +
Informationssicherheit + IT
Revision + HR + Legal

- **IT-Detailanweisungen:**
CISO (in Abstimmung mit ISOs)

Die Konzern-Richtlinien zur IT bei Burda

Konzernrichtlinien	Adressaten
Informationssicherheit (Leitlinie)	Alle Mitarbeitenden
Nutzung von IT- und Kommunikationssystemen	Alle Mitarbeitenden
Informationssicherheit für IT-Services	Interne IT
Informationssicherheit & externe Dienstleister	Management, das externe Dienstleister einsetzt
<i>Richtlinie für externe Dienstleister</i>	<i>Externe Dienstleister</i>

Dezentrale Erfassung geschäftskritischer Anwendungen

- Dezentrale Systeme zur **Erfassung und Risikobewertung digitaler Assets** (z.B. über MS Forms) durch die User im jeweiligen Geschäftsbereich
- **Ausgenommen: Standard-Software-Produkte**, die von der zentralen IT bereitgestellt werden (z.B. MS O365)
- **Schnittstellen** wie Datenschutz, Informationssicherheit oder Betriebsrat werden **automatisch informiert**

5. Art des Assets *

Webanwendung / Software-as-a-Service ist die richtige Auswahl, wenn die Software über Web oder App bereitgestellt wird und die primäre Funktionalität und/oder die Inhalte vollständig in der Cloud liegen. Beispiele: Salesforce, Elaine, Trello, Canva, JIRA.

Anwendung ist die richtige Auswahl, wenn die Software auf deinem Gerät installiert wird und Cloud-Funktionen entweder nicht vorhanden sind oder keine primäre Funktionen der Anwendung darstellen. Beispiele: JetBrains IDEs, Schnittprogramme, Browser

Platform-as-a-Service (PaaS) ist die richtige Auswahl, wenn dein Team selbst Anwendungen in der Cloud bereitstellt und dabei vom Anbieter verwaltete Infrastruktur nutzt. Beispiele: Heroku, AWS Elastic Beanstalk, Google App Engine.

Infrastructure-as-a-Service (IaaS) ist die richtige Auswahl, wenn dein Team auf selbst verwalteter Cloud-Infrastruktur, Services und Anwendungen bereitstellt. Beispiele: AWS, Google Cloud, Microsoft Azure.

Serversystem ist die richtige Antwort wenn es sich um klassische Server-Anwendungen handelt, die im Rechenzentrum der BurdaSolutions oder bei externen Hosting-Anbietern laufen. Beispiele: Datenbanken, Mailserver.

Sonstiges: wenn du dir nicht sicher bist oder sich die Art des Cloud-Services nicht eindeutig bestimmen lässt, ist Sonstiges die richtige Auswahl.

Ihre Antwort auswählen

6. Hosting / Betrieb *

Wo wird das Asset gehostet / betrieben?

Ihre Antwort auswählen

7. Geschäftsrelevant *

Ist das Asset für die primären Geschäftsprozesse der Gesellschaft unabdingbar?

Ja

Nein

8. Personenbezogene Daten *

Werden mit dem Asset personenbezogene Daten verarbeitet?

Ja

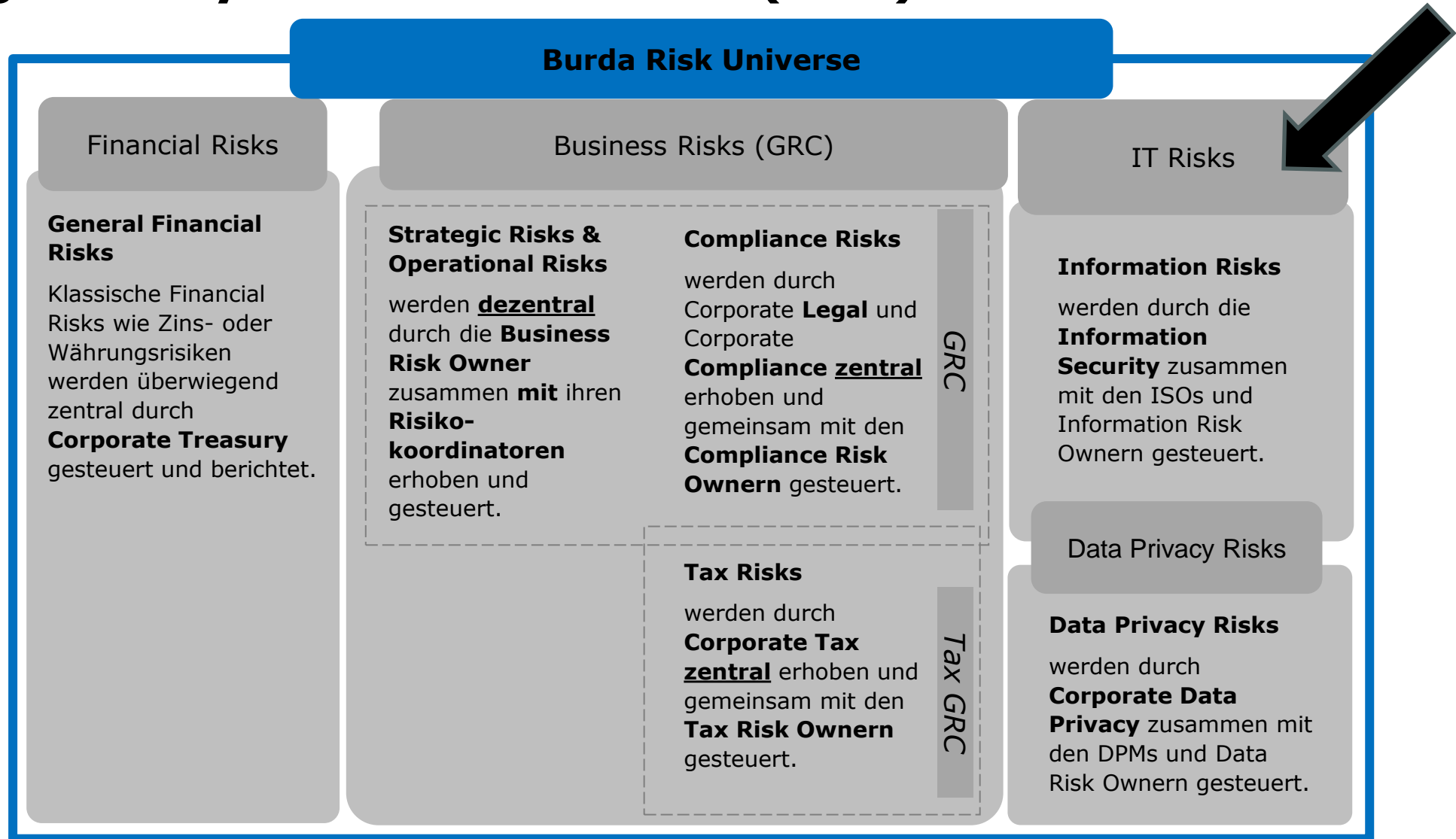
Zentrales Monitoring digitaler Assets aus Konzernsicht

Zentrales System der Informationssicherheit zur **Übernahme** (manuell oder per Schnittstelle) und **Monitoring der digitalen Assets**, die **aus Konzernsicht** geschäftskritisch sind:

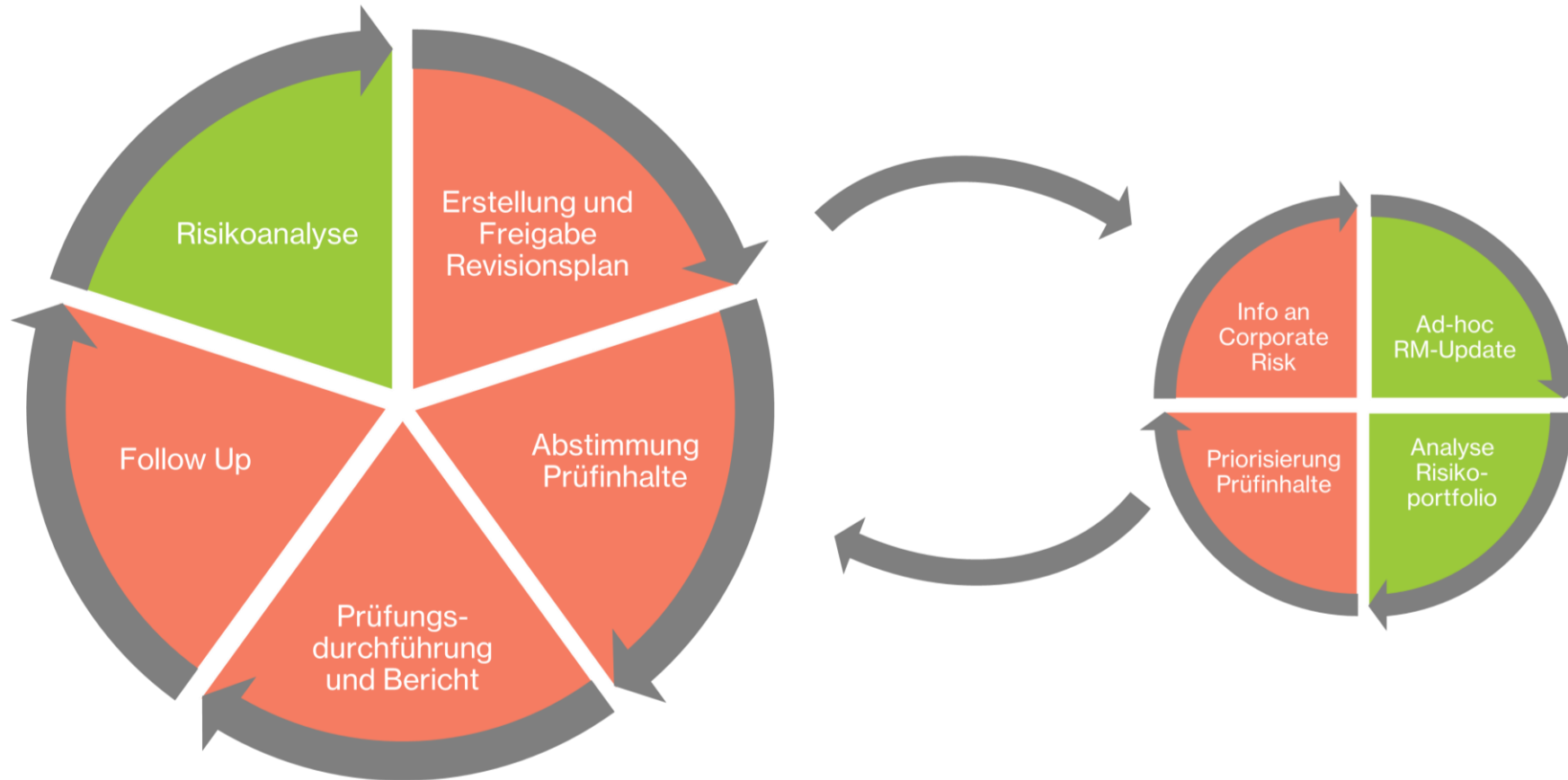
The screenshot displays the iSec RADAS interface. The top navigation bar includes 'FAQ', 'Asset', 'Assessments', 'Incidents', 'Freelancer/Lizenzgeber', 'Dienstleister', 'Fragen', 'Bedrohungen', 'Maßnahmen', and 'Admin'. The main content area shows a table with 611 entries. The table columns are: ID, Asset, Name, Klassifikation, Fragebogenkatalog, Brutto-Schutzbedarf, Netto-Schutzbedarf, Firma, Verantwortlicher, Workflow Abgeschlossen, and Aktionen. The table lists various assets such as 'openvpn connect IOS', 'Software Zlast (TOTP Generator für Windows)', 'Microsoft Office 365', 'CyberDuck', 'Lucid Link', 'Kalendersynchronisierung O365-Google Verwaltungsrat', 'Sentinel One', 'Mimecast', 'Thunderbird Mail Software', and 'Atlassian Confluence'. Each row includes a status icon, a classification (e.g., 'Öffentlich', 'Interne Daten', 'Vertraulich'), and a score for 'Brutto-Schutzbedarf' and 'Netto-Schutzbedarf'. The 'Verantwortlicher' column lists names and contact information for various companies like C3 Creative Code and Burda Digital Systems GmbH.

ID	Asset	Name	Klassifikation	Fragebogenkatalog	Brutto-Schutzbedarf	Netto-Schutzbedarf	Firma	Verantwortlicher	Workflow Abgeschlossen	Aktionen
978	openvpn connect IOS	openvpn-connect	Öffentlich	Fragebogenkatalog v2	1.00	1.00	C3 Creative Code and Content GmbH	Frank Schöne frank.schoene@c3.co 0171 766605	2025-05-27 13:40:50	
977	Software Zlast (TOTP Generator für Windows)	Software Zlast (TOTP Generator für Windows)	Interne Daten	Fragebogenkatalog v2	1.50	1.38	Burda Digital Systems GmbH	Armin Keller armin.keller@burda.com 0781 84 2368		
976	Microsoft Office 365	BMP Office 365	Vertraulich	Fragebogenkatalog v2	2.46	2.46	Burda Media Polska Sp. z o.o.	Marcin Karaś marcin.karas@burdamedia.pl +48601288916		
975	CyberDuck	CyberDuck	Öffentlich	Fragebogenkatalog v2	1.00	1.00	C3 Creative Code and Content GmbH	Frank Schöne frank.schoene@c3.co 0171 766605	2025-05-22 11:45:12	
974	Lucid Link	Lucid Link	Interne Daten	Fragebogenkatalog v2	1.98	1.00	Immediate Media Company Limited	Julian Adams julian.adams@immediate.co.uk +44 207 150 5186		
973	Kalendersynchronisierung O365-Google Verwaltungsrat	Kalendersynchronisierung Microsoft-Google Verwaltungsrat	Vertraulich	Fragebogenkatalog v2	2.35	1.69	Burda Digital Systems GmbH	Hermann Huber hermann.huber@burda.com +4915118067714	2025-05-23 08:24:40	
972	Kalendersynchronisierung O365-Google Verwaltungsrat			Fragebogenkatalog v2	n/a	n/a	n/a			
971	Sentinel One	Sentinel One	Interne Daten	Fragebogenkatalog v2	1.50	1.29	Immediate Media Company Limited	Simon Forey simon.forey@immediate.co.uk +44 207 150 5183		
970	Sentinel One			Fragebogenkatalog v2	n/a	n/a	n/a			
969	Mimecast	Mimecast	Interne Daten	Fragebogenkatalog v2	1.96	1.96	Immediate Media Company London Limited	Simon Forey simon.forey@immediate.co.uk +44 207 150 5183		
968	Thunderbird Mail Software	Thunderbird Mail Software	Vertraulich	Fragebogenkatalog v2	2.00	2.00	Hubert Burda Media Holding Kommanditgesellschaft	Bernhard Klein bernhard.klein@burda.com +49 (89) 9250 1262	2025-05-21 08:14:48	
967	Cloud Services StackIT	Cloud Services STACKIT	Interne Daten	Fragebogenkatalog v2	1.63	1.46	Burda Digital Systems GmbH	Markus Hoeschen und Thomas Hummel markus.hoeschen@burda.com 0781 84 2876		
966	Atlassian Confluence	Confluence für Ciscom	Interne Daten	Fragebogenkatalog v2	1.79	1.00	Burda Ciscom GmbH	Stephan Vollmer stephan.vollmer@burda.com	2025-05-20 12:57:16	

Wesentliche IT-Risiken werden in das unternehmensweite Risikomanagementsystem übernommen (GRC)



Einheiten, Prozesse und Systeme, die wesentliche Unternehmensrisiken steuern, werden regelmäßig geprüft



Chancen durch gute IT Governance

- Optimierte IT-Prozesse und eine gut definierte IT-Strategie können die **Effizienz der IT erhöhen und Kosteneinsparungen** ermöglichen sowie **Synergiepotenziale** heben!
- Eine wirksame IT Governance stellt die **Einhaltung von gesetzlichen Vorschriften** und Standards sicher!
- Durch eine gezielte IT Governance können **Innovationspotenziale** erschlossen und **Wettbewerbsvorteile** erzielt werden!
- Durch eine robuste IT Governance können **Sicherheitsmaßnahmen gestärkt und IT-Risiken gemindert** werden!

