RISIKOBASIERTE KONTROLLPLANUNG

Privacy Audits & Standards, GPR
Datenschutzbeirat, 2016

ERLEBEN, WAS VERBINDET.

AGENDA

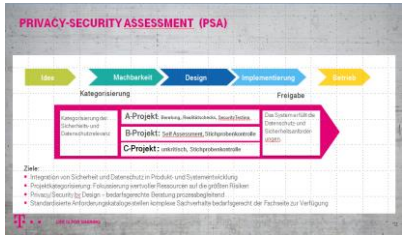
KONTROLL-PORTFOLIO VON GROUP PRIVACY

RISIKOBASIERTE KONTROLLEN SIND TEIL DES DATENSCHUTZ-COMPLIANCE-MANAGEMENT-SYSTEMS

JÄHRLICHER PLANUNGSPROZESS FÜR RISIKOBASIERTE KONTROLLEN

KONTROLL-PORTFOLIO VON GROUP PRIVACY

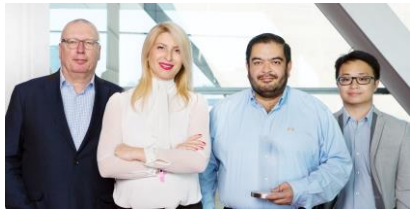
VORABKONTROLLEN IM PSA*-VERFAHREN



- Vorabkontrollen von Systemen und Organisationen

*Privacy-Security-Assessment

KONZERN-DATENSCHUTZZAUDIT



- Konzernweite Überprüfung des Datenschutz-Niveaus

ANLASS-KONTROLLEN

ad hoc!

- Bei Hinweisen auf potentielle Vorfälle

RISIKOBASIERTE KONTROLLEN

JAHRES-PLANUNG

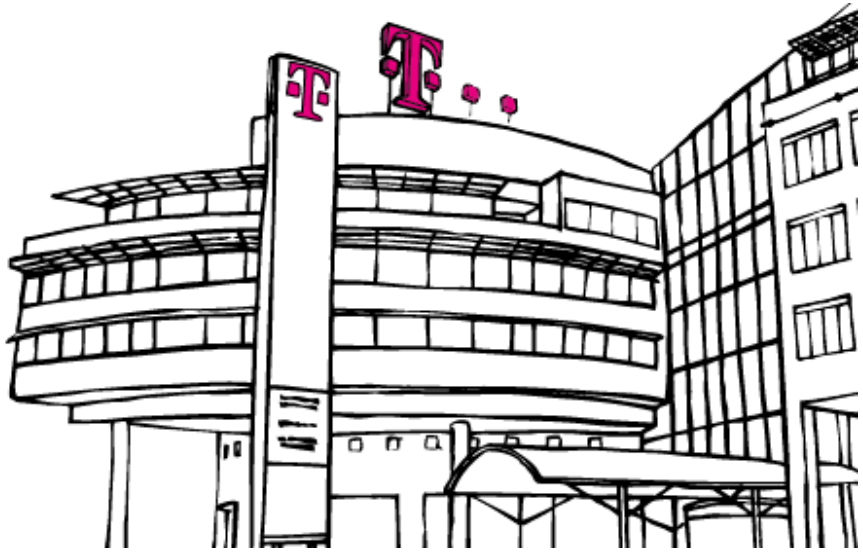
- Kontrollen von einzelnen Systemen und Organisationen

ZERTIFIZIERTE RISIKOKONTROLLPLANUNG

2013 hat Group Privacy das Telekom Datenschutz Compliance-Management-System entwickelt.

Wesentliche Elemente sind:

- Risikobasierte Kontrollplanung
- Durchführung von Kontrollen



2014 haben die Wirtschaftsprüfer von Deloitte & Touche die Wirksamkeit des Datenschutz-**Compliance-Management-Systems** der Telekom bestätigt und eine Zertifizierung mit Empfehlungen nach **IDW PS 980** erteilt.

Bericht

Deloitte.

PLANUNGSPROZESS FÜR DATENSCHUTZKONTROLLEN

ECKPUNKTE

- Jährlich
- Risikobasiert
- Systematisch & Formalisiert

ZIEL

- Herausfiltern der kritischen IT-Systeme und Organisationen

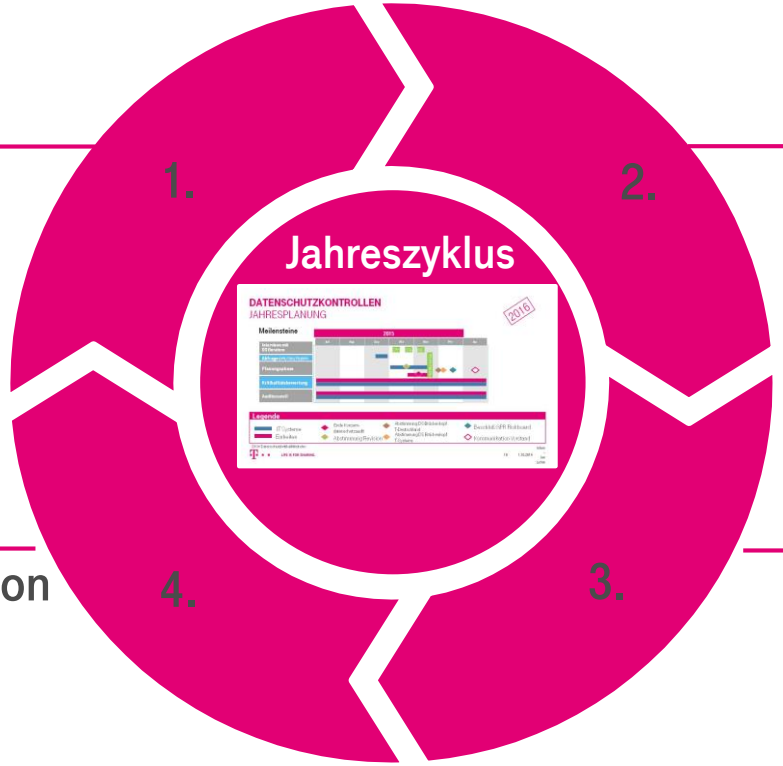
JÄHRLICHER PLANUNGSPROZESS
WESENTLICHE ELEMENTE

1. Informationserhebung und Erstbewertung (ganzjährig)

2. Sortierung und Validierung (September)

3. Einholung zusätzlicher Expertise (Oktober-November)

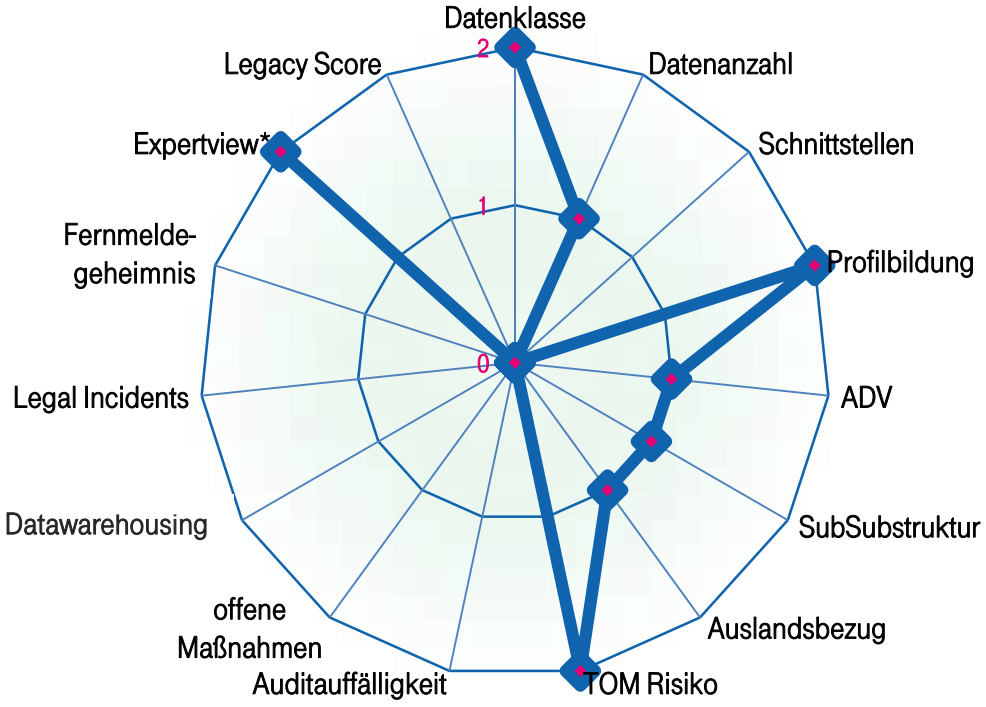
4. Beschluss und Kommunikation (Dezember-Januar)



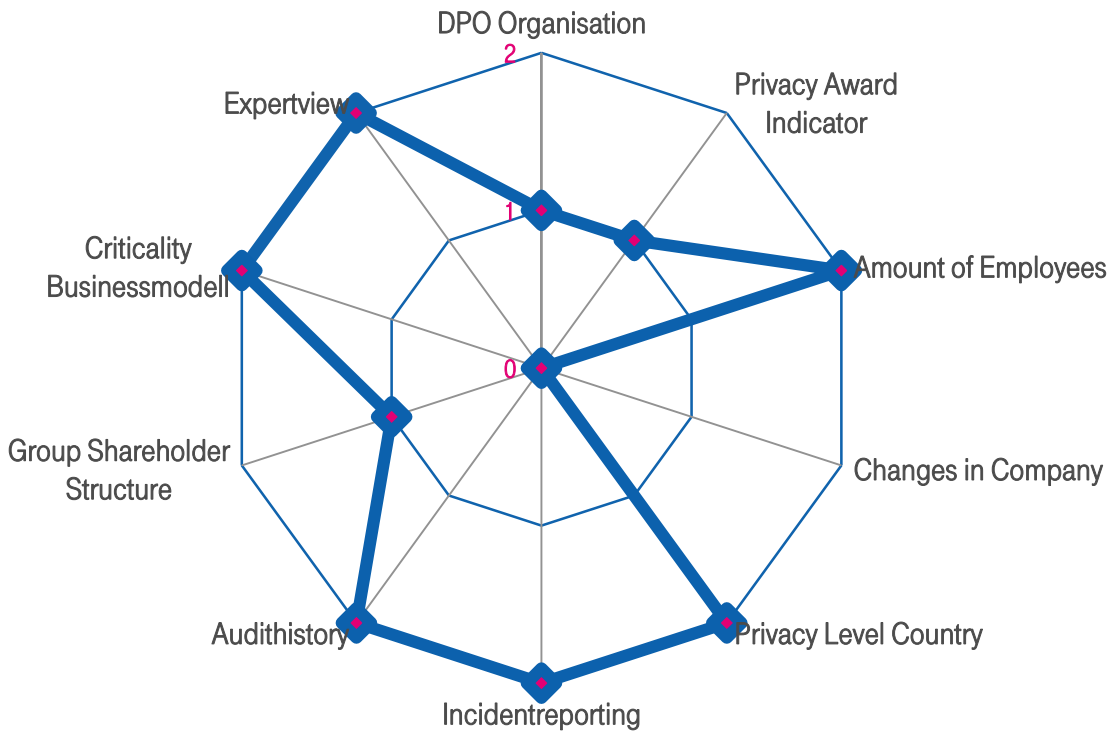
Jährlich | **Risikobasiert** | **Systematisch & Formalisiert**

DATENSCHUTZKRITIKALITÄTSINDEX (RISIKOBASIERT)
INFORMATIONSERHEBUNG

SYSTEME



ORGANISATIONEN



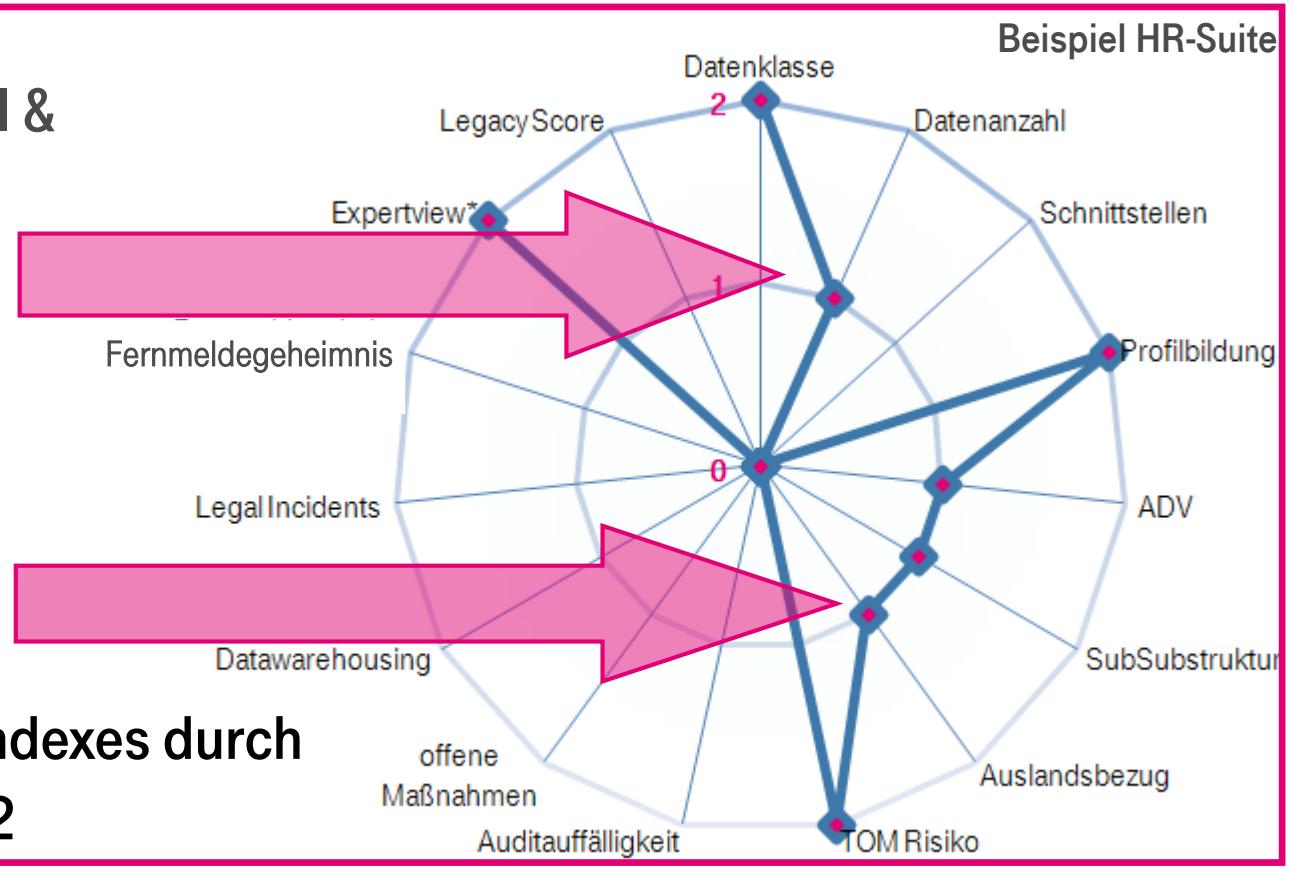
DATENSCHUTZKRITIKALITÄTSINDEX (RISIKOBASIERT)

EINZELBEISPIELE INDIKATOREN

Beispiel für Indikatoren: Datenanzahl & Auslandsdatenverarbeitung

Wie hoch ist die Anzahl der verarbeiteten Datensätze?	
Es werden weniger als 100.000 Datensätze verarbeitet.	0
Es werden zwischen 100.000 und 1.000.000 Datensätze verarbeitet.	1
Es werden mehr als 1.000.000 Datensätze verarbeitet.	2

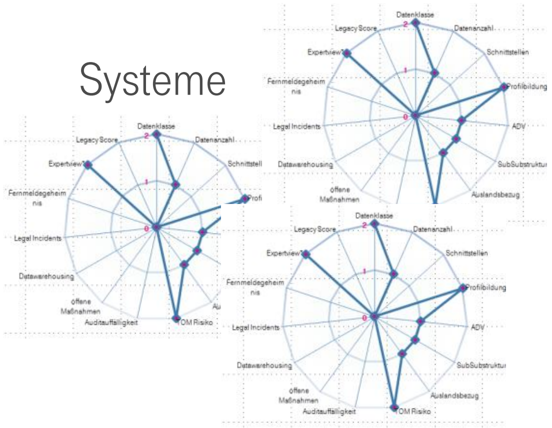
Findet eine Auslandsdatenverarbeitung statt?	
Es findet keine Auslandsdatenverarbeitung statt.	0
Die Daten werden im EWR (Nearshore) verarbeitet.	1
Die Datenverarbeitung findet außerhalb des EWR (Offshore) statt.	2



Bildung des Datenschutzkritikalitätsindexes durch die Addition von Risikofaktoren: ∑ 12

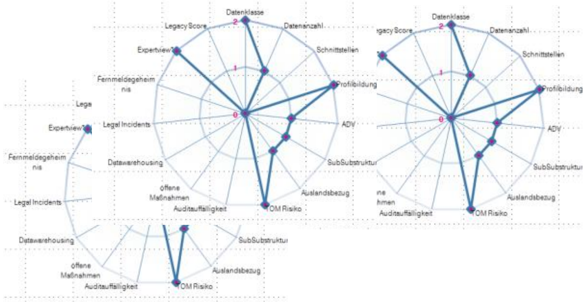
SORTIERUNG UND VALIDIERUNG EINZELBEWERTUNGEN

Systeme



Nr.	Systeme	Datenklasse	Auslandsbezug	Datenanzahl	Schnitt-stellen	Profil-bildung	ADV	SubSubstruktur	Auditauffälligkeit	TOM Risiko	offene Maßnahmen	Dataware-housing	Legal Incidents	Fernmelde-geheimnis	Expertview	Legacy Score	Score
1	System 1	1	2	2	2	1	0	0	2	1	0	0	0	2	4	0	17
2	System 2	1	1	2	2	1	0	1	1	1	2	0	0	2	3	0	17
3	System 3	2	1	2	1	1	2		0	2	0	0	0	2	3	0	16
4	System 4	2	0	0	0	2	0	2	0	2	0	0	0	2	5	0	15
8	System 5	1	1	2	2	1	0	1	1	0	1	2	0	0	3	0	15

Organisationen



	Organisationen	O Organisation	vacy Award Indicator	ount of Employees	anges in Company	vacy Level Country	identreporting	udithistory	oup Shareholder Structure	icality Businessmo	pertview	
1	Organisation 1	1	1	2	0	2	2	2	1	2	10	23
2	Organisation 2	0	0	2	2	0	2	0	2	2	10	20
3	Organisation 3	0	0	2	2	2	0	0	1	2	10	19
4	Organisation 4	1	1	2	0	2	1	4	0	2		13
5	Organisation 5	1	2	2	0	1	0	2	2	2		12

EINHOLUNG ZUSÄTZLICHER EXPERTISE

Abfrage von weiteren Systemen/Organisationen sowie aktuellen Risikoeinschätzungen:

- Abfrage bei den Datenschutz-Brückenköpfen
- Vorstands-Quartalsgespräche von L GPR
- Abfrage bei den Data Privacy Officers der internationalen Einheiten
- Interviews mit ausgewählten Managern

→ Ergänzung und Anpassung der Kontroll-Liste

ERGEBNIS

Zwei konsolidierte Kontroll-Listen für IT Systeme und Organisationen sortiert nach Kritikalität

BESCHLUSS UND KOMMUNIKATION

- **Finale Abstimmung** im Audit-Council mit den anderen kontrollierenden Abteilungen (Vermeidung von Doppelkontrollen, wenn möglich Vereinbarung von Joint-Kontrollen)
- **Finaler Beschluss** der Kontrollplanung durch L GPR und V-DRC

ENDERGEBNIS

Abschluss Jahreskontrollplanung und Start der Umsetzung

1. **Terminierung** der Kontrollen und Auditorenbenennung
2. **Bekanntgabe** des Jahresprogramms
3. **Quartalsweises Review** der Jahreskontrollplanung und ggf. Planungsanpassung

GLOSSAR

ADV	Auftragsdatenverarbeitung
CMS	Compliance Management System
DKI	Datenschutzkritikalitätsindix
GPR	Group Privacy
ICS	Internal Control System
TOM	Technische und Organisatorische Maßnahmen
PAS	Privacy Audits & Standards
PSA	Privacy Security Assessment
IDW	Institut der Wirtschaftsprüfer in Deutschland e.V.
PS	Prüfungsstandard
V-DRC	Vorstand Datenschutz, Recht und Compliance

VIELEN DANK!

www.telekom.com/datenschutz
www.telekom.com/privacy

DATENSCHUTZ AUDIT UNIVERSUM DES KONZERNS

DATENSCHUTZKONTROLLSYSTEM IM ÜBERBLICK

Konzerndatenschutzaudit

Jährlich flächendeckende Überprüfung:

- Systematische Qualitätssicherung im Bereich Datenschutz
- Generierung von Datenschutz KPI
- Awareness

PSA

Privacy & Security Assessment (PSA) für alle Projekte und IT-Systeme:

- Integration von Datenschutz und Sicherheit bereits in d. Entwicklung
- Beratung, Prüfung, Dokumentation und Freigabe
- PSA verbindlich ausgerollt

Stichproben PSA

Überprüfung folgender Elemente:

- Kategorisierung
- Prozesskonformität
- Dokumentation

Fokusaudits

Fokussierte Realitätsschecks am System:

- Beratungsergänzend
- Nach Wirkbetriebsaufnahme
- Autonom

Kontrollplan

Risikobasierte Datenschutzkontrollen:

- Systemkontrollen
- Organisationskontrollen
- National und international

Anlasskontrollen

Anlassbezogene Ad-hoc Kontrollen aufgrund potentieller Vorfälle

Audit-Council

Abstimmungsgremium aller kontrollierenden Bereiche:

- Austausch, Zusammenarbeit, Effizienzsteigerung
- Kontroll-Map
- Joint-Kontrollen
- Themenmitnahme

Internes Control System

Das interne Kontrollsystem (ICS) der Telekom beinhaltet datenschutzrechtliche Anforderungen, die regelmäßig intern wie extern geprüft und bestätigt werden.

RISIKOBASIERTE KONTROLLPLANUNG FÜR 2016