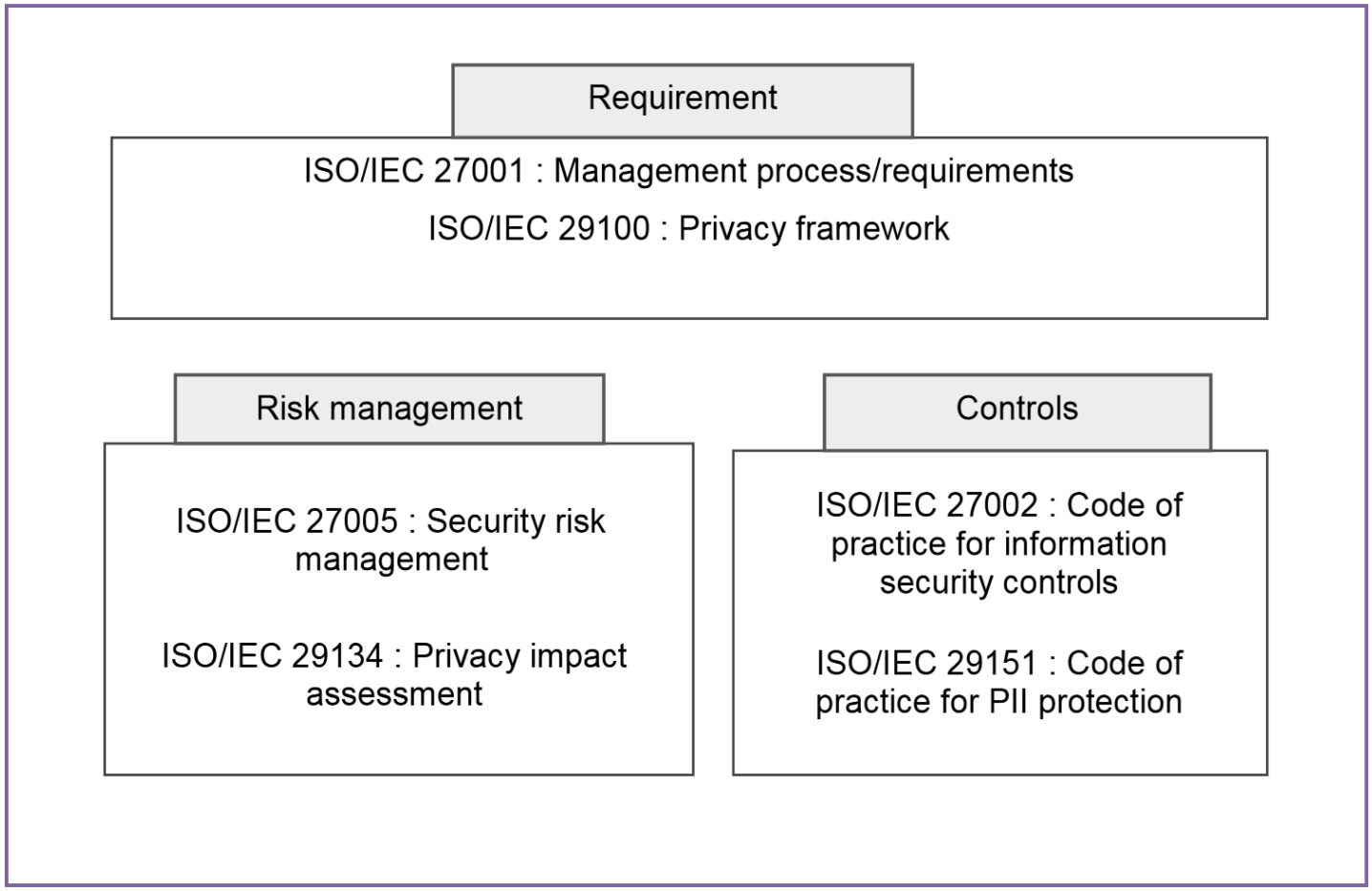
Durchführung einer Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO in Anlehnung an die ISO/IEC 29134

Musterbeispiel „Insight AG – Kfz-Telematik-Versicherungstarif“

Inhalt

Vorwort zur ISO/IEC 29134

Zusammenwirken von ISO-Standards



Quelle: ISO/IEC DIS 29151:2016(E) Seite xi

Aufbau der ISO 29134

FINAL DRAFT

INTERNATIONAL STANDARD

ISO/IEC FDIS 29134

ISO/IEC JTC **1**/SC **27**

Secretariat: DIN

Voting begins on:
2017-02-20

Voting terminates on:
2017-04-17

Information technology — Security techniques — Guidelines for privacy impact assessment

Technologies de l'information — Techniques de sécurité — Lignes directrices pour l'évaluation d'impacts sur la vie privée

Datenschutzfolgeabschätzung nach DS-GVO

Kurzpapier der DSK

DATENSCHUTZKONFERENZ

„Eine DSFA ist kein einmaliger Vorgang. Sollten sich z. B. neue Risiken ergeben, die Bewertung bereits erkannter Risiken ändern oder wesentliche Änderungen im Verfahren ergeben, die in der DSFA bisher nicht berücksichtigt wurden, so ist die DSFA zu überprüfen und ebenso anzupassen. Um dies zu garantieren, wird ein stetiger, iterativer Prozess der Überprüfung und Anpassung empfohlen."

Quelle: Abgestimmtes DSK Kurzpapier zur DSFA

Kurzpapier der DSK

DATENSCHUTZKONFERENZ

Kapitel in ISO 29134

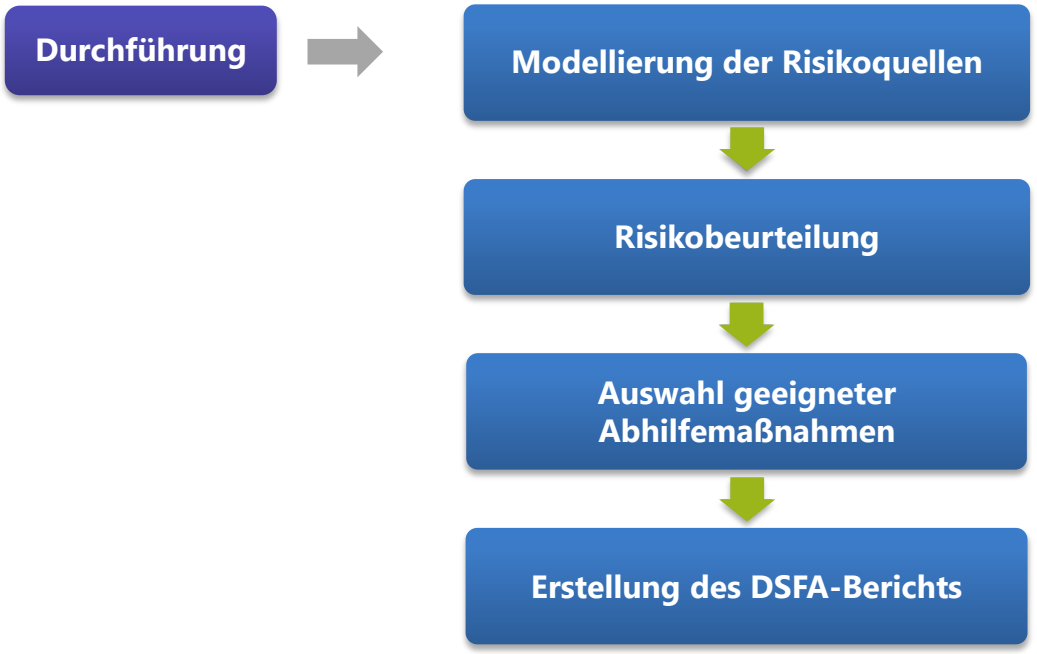
Vorbereitung

Zusammenstellung des DSFA-Teams	✓ 6.3.1
Prüfplanung	✓ 6.3.2
Festlegung des Beurteilungsumfangs (Scope)	✓ 6.3.3
Identifikation und Einbindung von Akteuren und betroffenen Personen	✓ 6.3.4
Bewertung der Notwendigkeit/ Verhältnismäßigkeit in Bezug auf Zweck	-
Identifikation der Rechtsgrundlagen	-

Quelle: Abgestimmtes DSK Kurzpapier zur DSFA

Kurzpapier der DSK

DATENSCHUTZKONFERENZ



Quelle: Abgestimmtes DSK Kurzpapier zur DSFA

Kapitel in ISO 29134

- ✓ 6.4.4
- ✓ 6.4.4
- ✓ 6.4.5
- ✓ 7

Kurzpapier der DSK

DATENSCHUTZKONFERENZ

Umsetzung →

- **Umsetzung der Abhilfemaßnahmen**
- **Test der Abhilfemaßnamen**
- **Dokumentation: Nachweis über die Einhaltung der DS-GVO**
- **Freigabe der Verarbeitungsvorgänge**

Kapitel in ISO 29134

✓	6.5.3
✓	6.5.4
✓	7
	-

Quelle: Abgestimmtes DSK Kurzpapier zur DSFA

Kurzpapier der DSK

DATENSCHUTZKONFERENZ

Kapitel in ISO 29134

Überprüfung → **Ggf. Überprüfung und Audit der DSFA** — **6.5.5**

↓

Fortschreibung — **6.5.5**

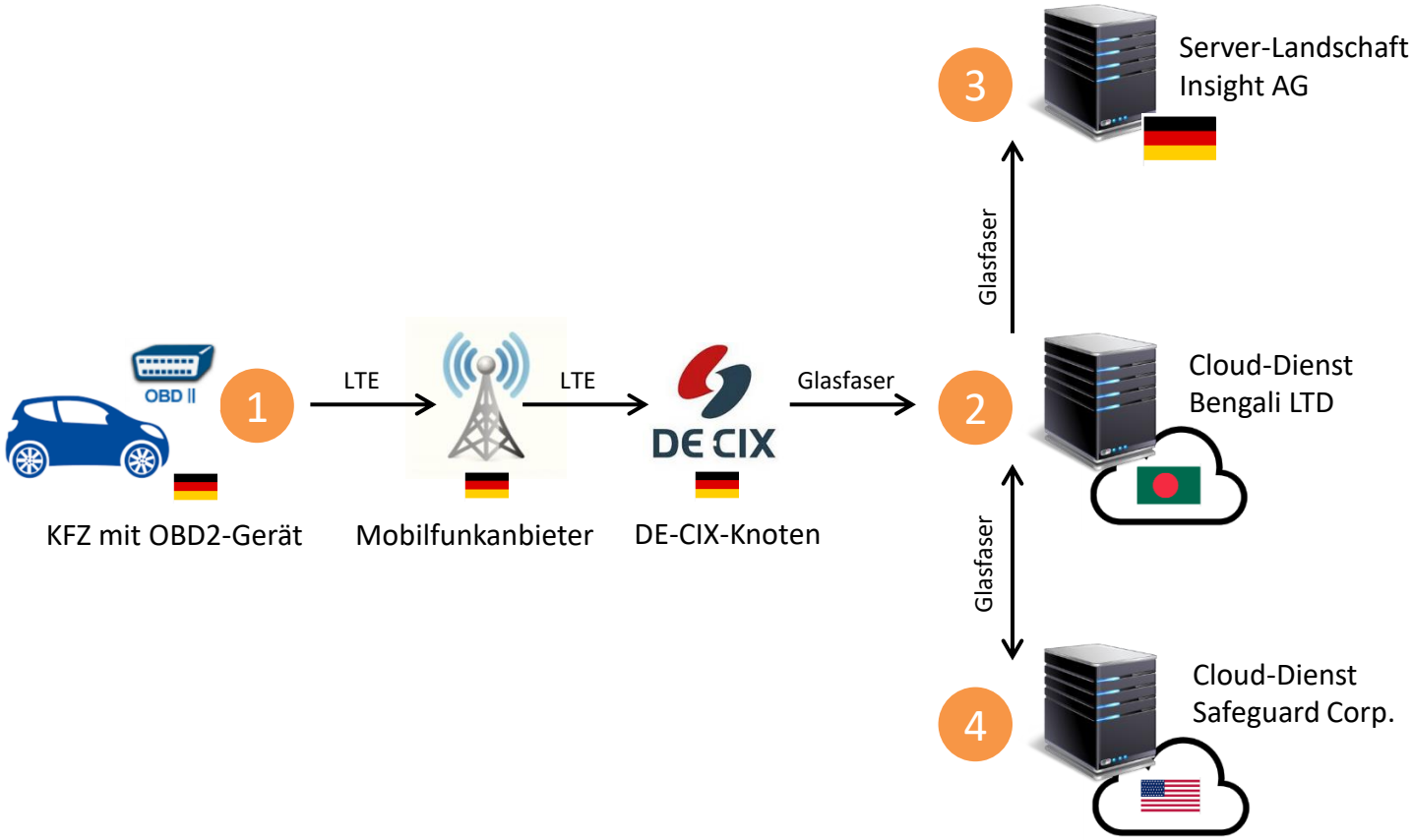
Quelle: Abgestimmtes DSK Kurzpapier zur DSFA

Durchführung am Musterbeispiel „Insight AG“

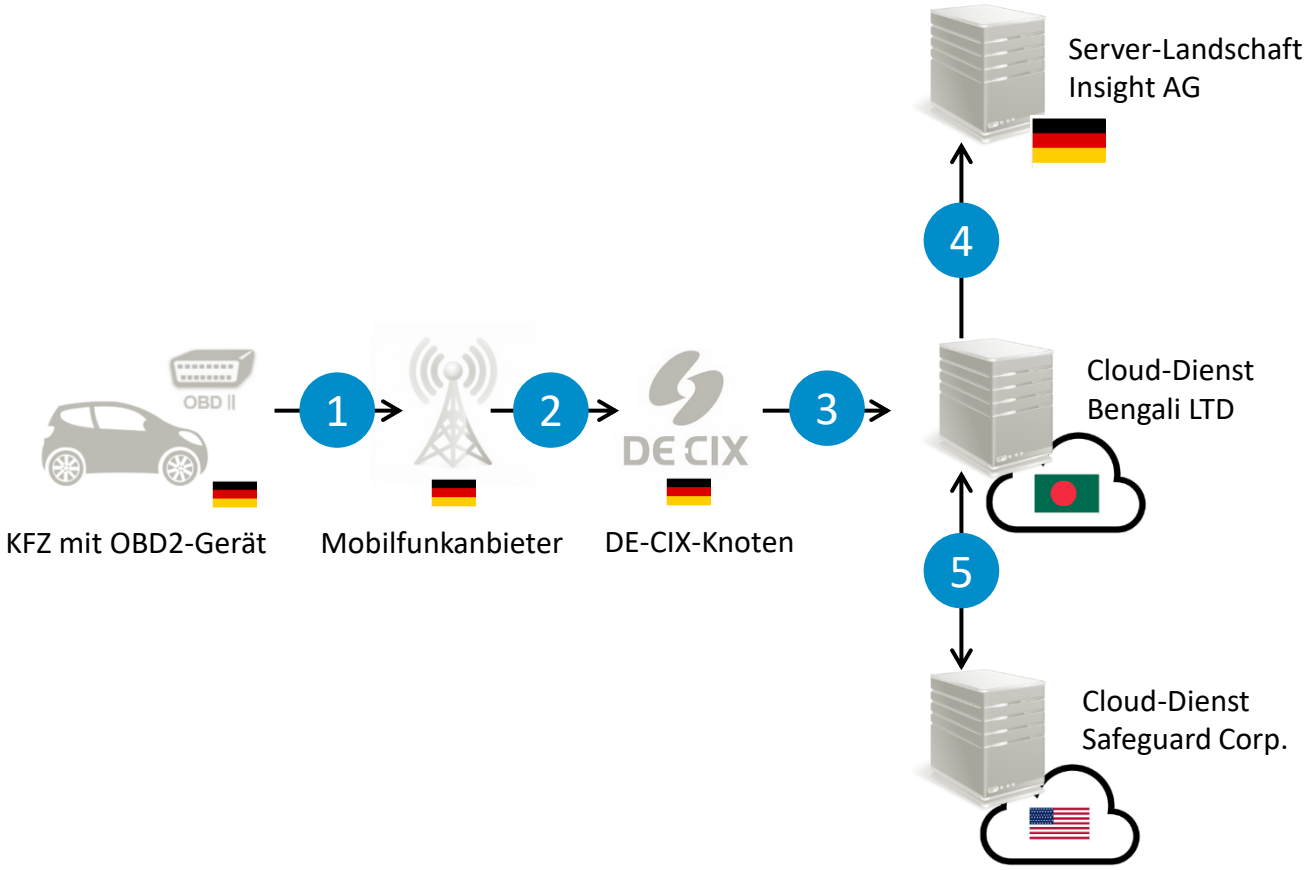
Zusammenstellung des DSFA Teams

Name	Position	Rolle
Herr Schröder	Geschäftsführer, Insight AG	Der Geschäftsführer Herr Schröder, der auch der Auftraggeber der DSFA ist, behält den Überblick über die Durchführung und übernimmt wichtige Lenkungs- und Entscheidungsfunktionen, insbesondere in kritischen oder unklaren Situationen.
Herr Stromberg	Prozessverantwortlicher (Process owner), Insight AG	Herr Stromberg leitet das DSFA-Projekt und hat die finanziellen, zeitlichen und personellen Aspekte im Blick. Er fügt alle Ergebnisse der Prozessschritte zusammen und berichtet direkt an Herrn Schröder.
Herr Schutz	Datenschutzbeauftragter, Insight AG	Der Datenschutzbeauftragter Herr Schutz übernimmt eine beratende Funktion, vor allem im Hinblick auf die Einhaltung des geltenden Datenschutzgesetzes. Er informiert über die notwendigen Informationen, die ein DSFA-Bericht enthalten muss und identifiziert die betroffenen Datenkategorien.
Frau Asci	IT-Leiterin, Insight AG	Die IT-Leiterin Frau Asci ist die Teilprojektleiterin des technischen Bereiches (Risikobeurteilung nach ISO-Norm, Systemarchitektur usw.).
Frau Recht	Juristin, Insight AG	Die Juristin Frau Recht ist die zweite Teilprojektleiterin und ist für die rechtliche Bewertung der DSFA-Durchführung und Dokumentation zuständig.
Herr Kutrapali	Geschäftsführer, Bengali LTD	Herr Kutrapali ist der Geschäftsführer des Cloud Dienstleisters „Bengali LTD“ und steht im engen Kontakt mit Frau Asci und Herrn Stromberg und beantwortet alle Fragestellungen z.B. zum Aufbau der IT-Infrastruktur des Unternehmens oder seinem US-Backup-Dienstleister.

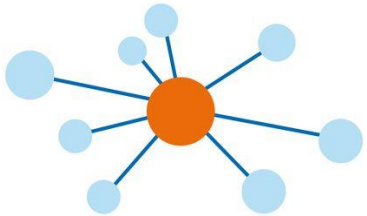
Systemarchitektur (Teil des Scope)



Datenflüsse (Teil des Scope)



Identifikation von Akteuren



- **Verantwortliche:** Insight AG
- **Auftragsverarbeiter**: Bengali LTD, Dienstleister Bangladesch
  Safeguard Corp., Dienstleister USA
  (Subunternehmer)
- **Betroffene**: Versicherte Privatpersonen
- **Weitere Betroffene**: z. B. anderweitige Fahrer des Kfz mit eingebautem Gerät

Risikobeurteilung: Ansatz nach ISO 31000

Risikobeurteilung

I. Risikoidentifikation

- Risikobeschreibung
- Risikoquelle
- Verarbeitungs-grundsatz nach Art. 5 DS-GVO

II. Risikoanalyse

- Möglicher Schaden
- Schadenskategorie (nach ErwGr. 75 DS-GVO)
- Eintrittswahrschein-lichkeit
- Schwere des Schadens

III. Risikobewertung

- Ergebnis

Möglicher Schaden? ErwGr. 75 DS-GVO

Erwägungsgrund 75:

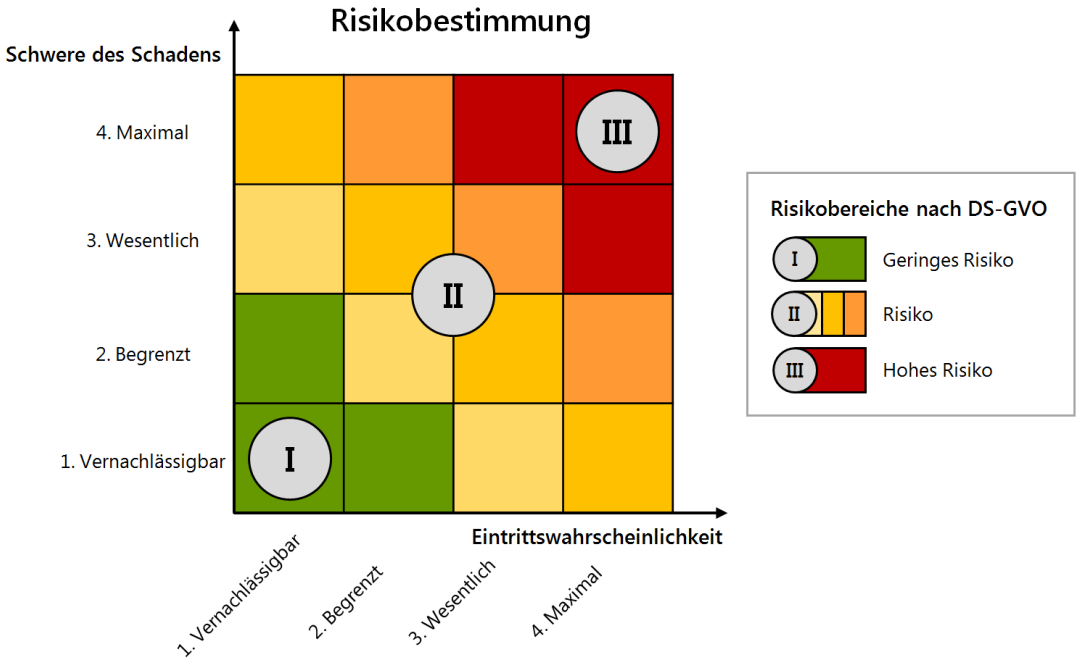
Die **Risiken** für die Rechte und Freiheiten natürlicher Personen – **mit unterschiedlicher Eintrittswahrscheinlichkeit und Schwere** – können aus einer Verarbeitung personenbezogener Daten hervorgehen, die zu einem physischen, materiellen oder immateriellen Schaden führen könnte, insbesondere wenn die Verarbeitung zu einer Diskriminierung, einem Identitätsdiebstahl oder -betrug, einem finanziellen Verlust, einer Rufschädigung, […]

Mögliche Schadenkategorien nach ErwGr. 75 DS-GVO	
Diskriminierung	
Identitätsdiebstahl	
Finanzieller Verlust	
Rufschädigung	
Verlust der Vertraulichkeit bei Berufsgeheimnis	
Unbefugten Aufhebung der Pseudonymisierung	
Andere wirtschaftliche oder gesellschaftliche Nachteile	
Hinderung der Kontrolle der Betroffenen über eigene Daten	
Verarbeitung von sensiblen Daten (Politik, Religion, Sexualleben, Gesundheit, etc.)	[…]

Risikobeurteilung: Ansatz

Erwägungsgrund 76:

Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten der betroffenen Person sollten in Bezug auf die Art, den Umfang, die Umstände und die Zwecke der Verarbeitung bestimmt werden. Das Risiko sollte anhand einer **objektiven Bewertung** beurteilt werden, bei der festgestellt wird, ob die Datenverarbeitung ein Risiko oder ein hohes Risiko birgt.



Schwere des Risikos

Vernachlässigbar	Kleine Unannehmlichkeiten
Begrenzt	Größere Unannehmlichkeiten
Wesentlich	Wesentliche Folgen
Maximal	Wesentliche und/oder irreversible Folgen

Eintrittswahrscheinlichkeit

Vernachlässigbar	Fast unmöglich / nicht vorstellbar
Begrenzt	Mit gewissem Aufwand machbar (schwierig)
Wesentlich	Mit geringem Aufwand machbar
Maximal	Einfach

Risikobeurteilung: Tabellarische Umsetzung

	Risikobeurteilung (gemäß ISO 31000)							
	I. Risikoidentifikation			II. Risikoanalyse				III. Risikobewertung
Risiko ID	Verarbeitungsgrundsatz (nach Art. 5 DS-GVO)	Risikoquelle	Risikobeschreibung	Möglicher Schaden	Schadenskategorie (nach ErwGr. 75)	Eintrittswahrscheinlichkeit	Schwere des Schadens	Ergebnis
1	Verfügbarkeit	Externer Mitarbeiter - USA	Löschung der Backups der Rohdaten in den USA be	Einschränkungen beim Auskun	Hinderung der Kontrolle der Betroffe	Begrenzt (2)	Begrenzt (2)	Risiko (4)
2	Verfügbarkeit	Cyberkrimineller (Hacker/Schadsoftv	Löschung der Backups der Rohdaten in den USA be	Einschränkungen beim Auskun	Hinderung der Kontrolle der Betroffe	Wesentlich (3)	Begrenzt (2)	Risiko (5)
3	Verfügbarkeit	Softwarefehler	Löschung der Backups der Rohdaten in den USA be	Einschränkungen beim Auskun	Hinderung der Kontrolle der Betroffe	Begrenzt (2)	Begrenzt (2)	Risiko (4)
4	Verfügbarkeit	Hardwaredefekt (physikalisch)	Löschung der Backups der Rohdaten in den USA be	Einschränkungen beim Auskun	Hinderung der Kontrolle der Betroffe	Vernachlässigbar (1)	Begrenzt (2)	geringes Risiko (2-3)
5	Verfügbarkeit	Umwelteinflüsse (Naturgewalt)	Löschung der Backups der Rohdaten in den USA be	Einschränkungen beim Auskun	Hinderung der Kontrolle der Betroffe	Vernachlässigbar (1)	Begrenzt (2)	geringes Risiko (2-3)
6	Verfügbarkeit	Externer Mitarbeiter - Bangladesch	Löschung der Rohdaten in Bangladesch bei Bengali	Einschränkungen beim Auskun	Hinderung der Kontrolle der Betroffe	Wesentlich (3)	Begrenzt (2)	Risiko (5)
7	Verfügbarkeit	Cyberkrimineller (Hacker/Schadsoftv	Löschung der Rohdaten in Bangladesch bei Bengali	Einschränkungen beim Auskun	Hinderung der Kontrolle der Betroffe	Wesentlich (3)	Begrenzt (2)	Risiko (5)
8	Verfügbarkeit	Umwelteinflüsse (Naturgewalt)	Löschung der Rohdaten in Bangladesch bei Bengali	Einschränkungen beim Auskun	Hinderung der Kontrolle der Betroffe	Vernachlässigbar (1)	Begrenzt (2)	geringes Risiko (2-3)
9	Verfügbarkeit	Softwarefehler	Löschung der Rohdaten in Bangladesch bei Bengali	Einschränkungen beim Auskun	Hinderung der Kontrolle der Betroffe	Begrenzt (2)	Begrenzt (2)	geringes Risiko (2-3)
10	Verfügbarkeit	Hardwaredefekt (physikalisch)	Löschung der Rohdaten in Bangladesch bei Bengali	Einschränkungen beim Auskun	Hinderung der Kontrolle der Betroffe	Vernachlässigbar (1)	Begrenzt (2)	geringes Risiko (2-3)
11	Verfügbarkeit	Versicherter (Kfz-Fahrer)	Löschung der Rohdaten in Bangladesch bei Bengali	Einschränkungen beim Auskun	Hinderung der Kontrolle der Betroffe	Vernachlässigbar (1)	Begrenzt (2)	geringes Risiko (2-3)
12	Verfügbarkeit	Dritter (anderer Kfz-Fahrer)	Löschung der Rohdaten in Bangladesch bei Bengali	Einschränkungen beim Auskun	Hinderung der Kontrolle der Betroffe	Vernachlässigbar (1)	Begrenzt (2)	geringes Risiko (2-3)
13	Integrität und Vertraulichkeit	Externer Mitarbeiter - Bangladesch	Unbefugte Entwendung der Rohdaten vom Fahrzeu	Rufschädigung, Disikriminierur	Rufschädigung	Wesentlich (3)	Maximal (4)	hohes Risiko (7-8)
14	Integrität und Vertraulichkeit	Versicherter (Kfz-Fahrer)	Unbefugte Entwendung der Rohdaten vom Fahrzeu	Rufschädigung, Disikriminierur	Rufschädigung	Begrenzt (2)	Begrenzt (2)	Risiko (4)
15	Integrität und Vertraulichkeit	Dritter (anderer Kfz-Fahrer)	Unbefugte Entwendung der Rohdaten vom Fahrzeu	Rufschädigung, Disikriminierur	Rufschädigung	Begrenzt (2)	Wesentlich (3)	Risiko (5)
16	Integrität und Vertraulichkeit	Cyberkrimineller (Hacker/Schadsoftv	Unbefugte Entwendung der Rohdaten vom Fahrzeu	Rufschädigung, Disikriminierur	Rufschädigung	Wesentlich (3)	Maximal (4)	hohes Risiko (7-8)
17	Integrität und Vertraulichkeit	Interner Mitarbeiter - Insight AG	Unbefugte Entwendung der Rohdaten vom Fahrzeu	Rufschädigung, Disikriminierur	Rufschädigung	Wesentlich (3)	Maximal (4)	hohes Risiko (7-8)
18	Integrität und Vertraulichkeit	Externer Mitarbeiter - USA	Unbefugte Entwendung der Rohdaten vom Fahrzeu	Rufschädigung, Disikriminierur	Rufschädigung	Begrenzt (2)	Maximal (4)	Risiko (6)
19	Verfügbarkeit	Softwarefehler	Datenpaketverlust zwischen Fahrzeug und DE-CIX-K	Einschränkungen beim Auskun	Finanzieller Verlust	Begrenzt (2)	Begrenzt (2)	Risiko (4)
20	Verfügbarkeit	Hardwaredefekt (physikalisch)	Datenpaketverlust zwischen Fahrzeug und DE-CIX-K	Einschränkungen beim Auskun	Finanzieller Verlust	Wesentlich (3)	Begrenzt (2)	Risiko (5)
21	Verfügbarkeit	Cyberkrimineller (Hacker/Schadsoftv	Datenpaketverlust zwischen Fahrzeug und DE-CIX-K	Einschränkungen beim Auskun	Finanzieller Verlust	Wesentlich (3)	Begrenzt (2)	Risiko (5)
22	Integrität und Vertraulichkeit	Versicherter (Kfz-Fahrer)	Manipulation der Rohdaten im Fahrzeug	"Falsche" Bewertung bei Unfall	Andere wirtschaftliche oder gesellsch	Vernachlässigbar (1)	Wesentlich (3)	Risiko (4)
23	Integrität und Vertraulichkeit	Dritter (anderer Kfz-Fahrer)	Manipulation der Rohdaten im Fahrzeug	"Falsche" Bewertung bei Unfall	Andere wirtschaftliche oder gesellsch	Vernachlässigbar (1)	Wesentlich (3)	Risiko (4)
24	Integrität und Vertraulichkeit	Sonstiger Dritte (Mitarbeiter Kfz-We	Manipulation der Rohdaten im Fahrzeug	"Falsche" Bewertung bei Unfall	Andere wirtschaftliche oder gesellsch	Begrenzt (2)	Wesentlich (3)	Risiko (5)
25	Integrität und Vertraulichkeit	Softwarefehler	Manipulation der Rohdaten im Fahrzeug	"Falsche" Bewertung bei Unfall	Andere wirtschaftliche oder gesellsch	Begrenzt (2)	Wesentlich (3)	Risiko (5)
26	Integrität und Vertraulichkeit	Hardwaredefekt (physikalisch)	Manipulation der Rohdaten im Fahrzeug	"Falsche" Bewertung bei Unfall	Andere wirtschaftliche oder gesellsch	Begrenzt (2)	Wesentlich (3)	Risiko (5)
27	Integrität und Vertraulichkeit	Cyberkrimineller (Hacker/Schadsoftv	Manipulation der Rohdaten im Fahrzeug	"Falsche" Bewertung bei Unfall	Andere wirtschaftliche oder gesellsch	Wesentlich (3)	Maximal (4)	hohes Risiko (7-8)
28	Integrität und Vertraulichkeit	Interner Mitarbeiter - Insight AG	Manipulation der Mapping-Daten in den Systemen	Falsche Profile, finanzieller Ver	Profilbildung durch Bewertung persö	Begrenzt (2)	Begrenzt (2)	Risiko (4)
29	Integrität und Vertraulichkeit	Externer Mitarbeiter - Bangladesch	Manipulation der Mapping-Daten in den Systemen	Falsche Profile, finanzieller Ver	Profilbildung durch Bewertung persö	Vernachlässigbar (1)	Begrenzt (2)	geringes Risiko (2-3)
30	Integrität und Vertraulichkeit	Cyberkrimineller (Hacker/Schadsoftv	Manipulation der Mapping-Daten in den Systemen	Falsche Profile, finanzieller Ver	Profilbildung durch Bewertung persö	Begrenzt (2)	Begrenzt (2)	Risiko (4)
31	Integrität und Vertraulichkeit	Hardwaredefekt (physikalisch)	Manipulation der Mapping-Daten in den Systemen	Falsche Profile, finanzieller Ver	Profilbildung durch Bewertung persö	Vernachlässigbar (1)	Begrenzt (2)	geringes Risiko (2-3)
32	Integrität und Vertraulichkeit	Softwarefehler	Manipulation der Mapping-Daten in den Systemen	Falsche Profile, finanzieller Ver	Profilbildung durch Bewertung persö	Begrenzt (2)	Begrenzt (2)	Risiko (4)
33	Integrität und Vertraulichkeit	Interner Mitarbeiter - Insight AG	Manipulation der Score-Wert-Daten in den Systeme	Finanzieller Verlust (verfälschte	Finanzieller Verlust	Wesentlich (3)	Begrenzt (2)	Risiko (5)
34	Integrität und Vertraulichkeit	Externer Mitarbeiter - Bangladesch	Manipulation der Score-Wert-Daten in den Systeme	Finanzieller Verlust (verfälschte	Finanzieller Verlust	Begrenzt (2)	Begrenzt (2)	Risiko (4)
35	Integrität und Vertraulichkeit	Softwarefehler	Manipulation der Score-Wert-Daten in den Systeme	Finanzieller Verlust (verfälschte	Finanzieller Verlust	Begrenzt (2)	Begrenzt (2)	Risiko (4)
36	Integrität und Vertraulichkeit	Hardwaredefekt (physikalisch)	Manipulation der Score-Wert-Daten in den Systeme	Finanzieller Verlust (verfälschte	Finanzieller Verlust	Vernachlässigbar (1)	Begrenzt (2)	geringes Risiko (2-3)
37	Integrität und Vertraulichkeit	Cyberkrimineller (Hacker/Schadsoftv	Manipulation der Score-Wert-Daten in den Systeme	Finanzieller Verlust (verfälschte	Finanzieller Verlust	Vernachlässigbar (1)	Begrenzt (2)	geringes Risiko (2-3)
38	Richtigkeit	Versicherter (Kfz-Fahrer)	Fehlerhafte Datenübermittlung durch Box aus Kfz	Daten werden nicht oder nicht	Andere wirtschaftliche oder gesellsch	Vernachlässigbar (1)	Begrenzt (2)	geringes Risiko (2-3)

Risikobeispiel: Integrität und Vertraulichkeit

Risiko ID 16

	Risikobeurteilung (gemäß ISO 31000)							
	I. Risikoidentifikation			II. Risikoanalyse				III. Risikobewertung
Risiko ID	Verarbeitungsgrundsatz (nach Art. 5 DS-GVO)	Risikoquelle	Risikobeschreibung	Möglicher Schaden	Schadenskategorie (nach ErwGr. 75)	Eintrittswahrscheinlichkeit	Schwere des Schadens	Ergebnis
16	Integrität und Vertraulichkeit	Cyberkrimineller (Hacker/Schadsoftware)	Unbefugte Entwendung der Rohdaten vom Fahrzeug/Versicherten werden aus der Datenbank in Bangladesch entwendet.	Rufschädigung, Disikriminierung, andere wirtschaftliche Schäden	Rufschädigung	Wesentlich (3)	Maximal (4)	hohes Risiko (7-8)

Risikoquelle: Cyberkrimineller (Hacker/Schadsoftware)

Risikobeschreibung: Unbefugte Entwendung der Rohdaten vom Fahrzeug/Versicherten werden aus der Datenbank in Bangladesch entwendet.

Verarbeitungsgrundsatz: Integrität und Vertraulichkeit

Möglicher Schaden: Rufschädigung durch unbefugte Verwendung der Daten, Diskriminierung wegen unbefugter Auswertung von Fahrtrouten, andere wirtschaftliche Schäden (z. B. durch Erpressung)

Schadenskategorie: Rufschädigung, Diskriminierung, andere wirtschaftliche Schäden

Eintrittswahrscheinlichkeit: Wesentlich (3)

Schwere des Schadens: Maximal (4)

Ergebnis Risikobewertung: **hohes Risiko (7-8)**

Risikobeispiel: Zweckbindung

Risiko ID 45

	Risikobeurteilung (gemäß ISO 31000)							
	I. Risikoidentifikation			II. Risikoanalyse				III. Risikobewertung
Risiko ID	Verarbeitungsgrundsatz (nach Art. 5 DS-GVO)	Risikoquelle	Risikobeschreibung	Möglicher Schaden	Schadenskategorie (nach ErwGr. 75)	Eintrittswahrscheinlichkeit	Schwere des Schadens	Ergebnis
45	Zweckbindung	Interner Mitarbeiter - Insight AG	Gespeicherte Daten werden für weitere Zwecke (Profilbildung, etc.) verwendet	Diskriminierung, finanzieller Schaden, Rufschädigung, Identitätsdiebstahl oder Betrug	Profilbildung durch Bewertung persönlicher Aspekte (Vorlieben, Interessen, Aufenthaltsort, Ortswechsel, etc.)	Wesentlich (3)	Wesentlich (3)	Risiko (6)

Risikoquelle: Interner Mitarbeiter – Insight AG

Risikobeschreibung: Gespeicherte Daten werden für weitere Zwecke (Profilbildung, etc.) verwendet

Verarbeitungsgrundsatz: Zweckbindung

Möglicher Schaden: Diskriminierung, finanzieller Schaden, Rufschädigung, Identitätsdiebstahl oder Betrug, heimliche Profilbildung

Schadenskategorie: Profilbildung durch Bewertung persönlicher Aspekte (Vorlieben, Interessen, Aufenthaltsort, Ortswechsel, etc.)

Eintrittswahrscheinlichkeit: Wesentlich (3)

Schwere des Schadens: Wesentlich (3)

Ergebnis Risikobewertung: **Risiko (6)**

Risikobeispiel: Transparenz

Risiko ID 62

	Risikobeurteilung (gemäß ISO 31000)							
	I. Risikoidentifikation			II. Risikoanalyse				III. Risikobewertung
Risiko ID	Verarbeitungsgrundsatz (nach Art. 5 DS-GVO)	Risikoquelle	Risikobeschreibung	Möglicher Schaden	Schadenskategorie (nach ErwGr. 75)	Eintrittswahrscheinlichkeit	Schwere des Schadens	Ergebnis
62	Transparenz	Geschäftsführung	Fahrer (ungleich Halter) weiß nichts von der Verarbeitung	Profilbildung durch Bewertung persönlicher Aspekte	Profilbildung durch Bewertung persönlicher Aspekte (Vorlieben, Interessen, Aufenthaltsort, Ortswechsel, etc.)	Maximal (4)	Wesentlich (3)	hohes Risiko (7-8)

Risikoquelle: Geschäftsführung – Insight AG
Risikobeschreibung: Fahrer des Kfz (ungleich Halter/Versicherter) weiß nichts von der Verarbeitung
Verarbeitungsgrundsatz: Transparenz
Möglicher Schaden: Profilbildung durch Bewertung persönlicher Aspekte
Schadenskategorie: Profilbildung durch Bewertung persönlicher Aspekte (Vorlieben, Interessen, Aufenthaltsort, Ortswechsel, etc.)
Eintrittswahrscheinlichkeit: Maximal (4)
Schwere des Schadens: Wesentlich (3)
Ergebnis Risikobewertung: **hohes Risiko (7-8)**

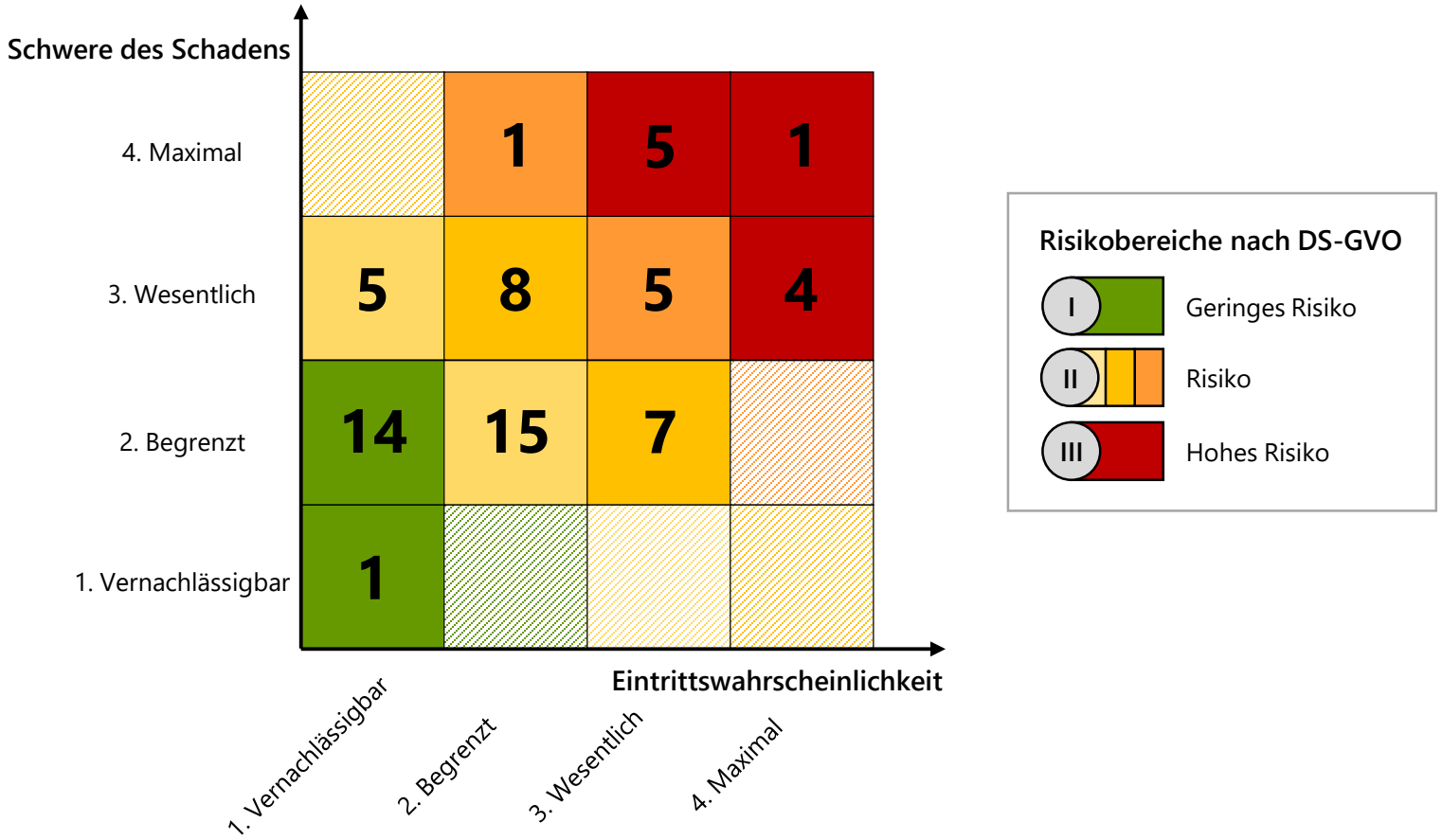
Risikobeispiel: Datenminimierung

Risiko ID 58

	Risikobeurteilung (gemäß ISO 31000)							
	I. Risikoidentifikation			II. Risikoanalyse				III. Risikobewertung
Risiko ID	Verarbeitungsgrundsatz (nach Art. 5 DS-GVO)	Risikoquelle	Risikobeschreibung	Möglicher Schaden	Schadenskategorie (nach ErwGr. 75)	Eintrittswahrscheinlichkeit	Schwere des Schadens	Ergebnis
58	Datenminimierung	Interner Mitarbeiter - Insight AG	Datenerhebung/verarbeitung ohne Erforderlichkeit (Folgedatenberechnung wie z.B. genaue Uhrzeit, Anzahl der Kneipenbesuche)	Diskriminierung, dem Zweck nicht angemessen	Diskriminierung	Maximal (4)	Wesentlich (3)	hohes Risiko (7-8)

Risikoquelle: Interner Mitarbeiter – Insight AG
Risikobeschreibung: Gespeicherte Daten werden für weitere Zwecke (Profilbildung, etc.) verwendet
Verarbeitungsgrundsatz: Zweckbindung
Möglicher Schaden: Diskriminierung, finanzieller Schaden, Rufschädigung, Identitätsdiebstahl oder Betrug, heimliche Profilbildung
Schadenskategorie: Profilbildung durch Bewertung persönlicher Aspekte (Vorlieben, Interessen, Aufenthaltsort, Ortswechsel, etc.)
Eintrittswahrscheinlichkeit: Maximal (4)
Schwere des Schadens: Wesentlich (3)
Ergebnis Risikobewertung: **hohes Risiko (7-8)**

Ergebnis der Risikobewertung



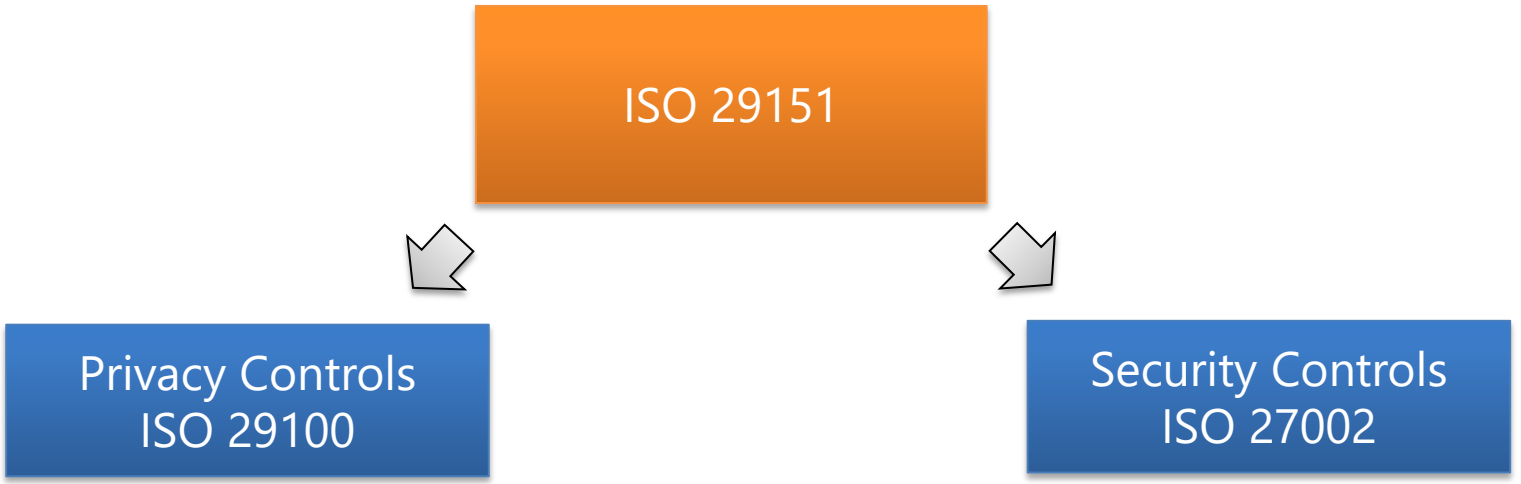
Abhilfemaßnahmen nach ISO 29134

6.4.5.2 Determine controls

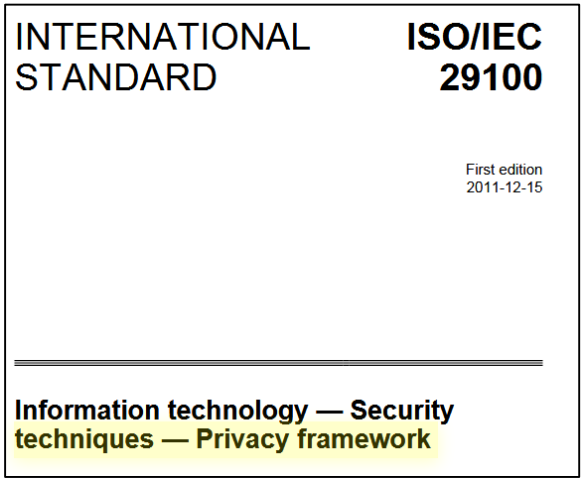
The assessor should compare the existing and determined controls to reference lists of controls and
verify that no necessary controls have been omitted:

- controls in ISO/IEC 27001:2013, Annex A;
- controls in ISO/IEC 29151;
- controls in any relevant privacy sets of controls, including national standards;
- controls from external factors;
- controls from internal factors.

Abhilfemaßnahmen nach ISO 29151



Abhilfemaßnahmen nach ISO 29100


INTERNATIONAL STANDARD

ISO/IEC 29100

First edition
2011-12-15

Information technology — Security techniques — Privacy framework

ISO 29100

- Rechtmäßigkeit
- Transparenz
- Faire Verarbeitung
- Zweckbindung
- Datenminimierung
- Richtigkeit
- Speicherbegrenzung
- Security
- Rechenschaftspflicht

Ergebnis der Restrisikobewertung