SH Schleswig-Holstein
Der echte Norden

IT-Planungsrat
Digitale Zukunft gestalten

7. Fachkongress des IT-Planungsrats am 12./13. März 2019 in Lübeck

Mit Datenschutzmanagement zu datenschutzkonformen Digitalisierungsprojekten

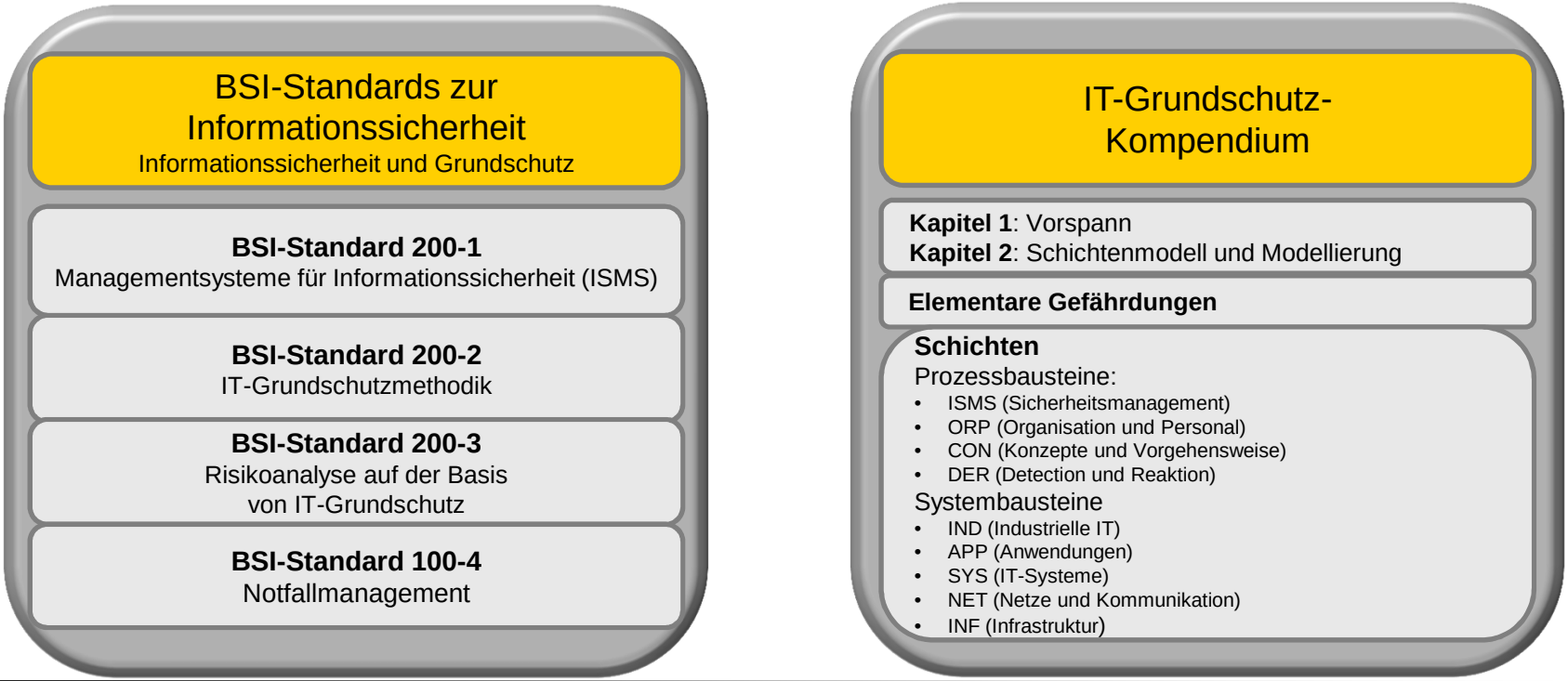
Gabriel Schulz
Stellvertreter des Landesbeauftragten für Datenschutz und Informationsfreiheit M-V

Grundlagen des Datenschutzmanagements

Art. 24 Abs.1: Verantwortung des für die Verarbeitung Verantwortlichen

Der Verantwortliche setzt unter Berücksichtigung der …Risiken für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen um, um sicherzustellen und den Nachweis dafür erbringen zu können, dass die Verarbeitung gemäß dieser Verordnung erfolgt. Diese Maßnahmen werden erforderlichenfalls überprüft und aktualisiert.

Modernisierter IT-Grundschutz des BSI



I

(Gesetzgebungsakte)

VERORDNUNGEN

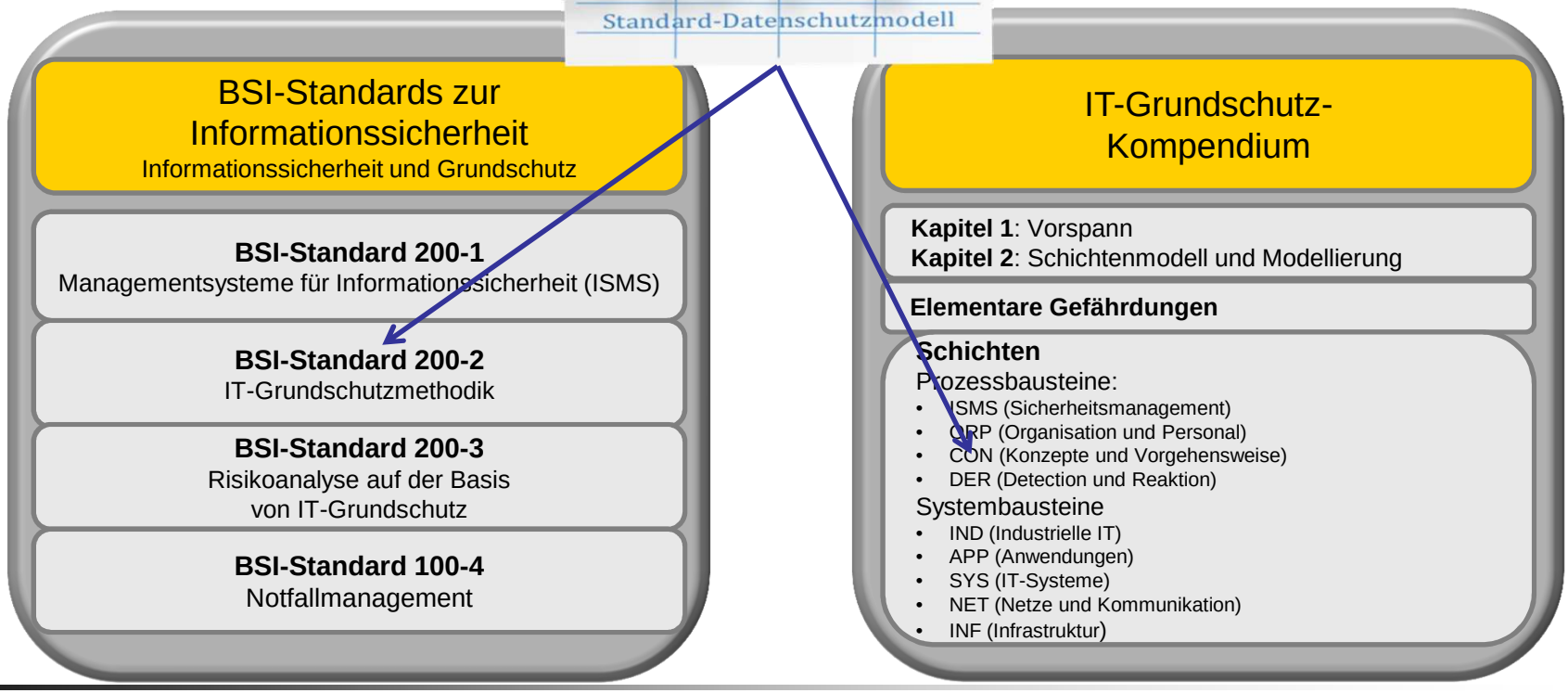
VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES

vom 27. April 2016

zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung)

(Text von Bedeutung für den EWR)

Modernisierte SDM tz des BSI



BSI-Grundschutz und SDM

BSI-Standard 200-2 Abschnitt 8.2 (Schutzbedarfsfeststellung)

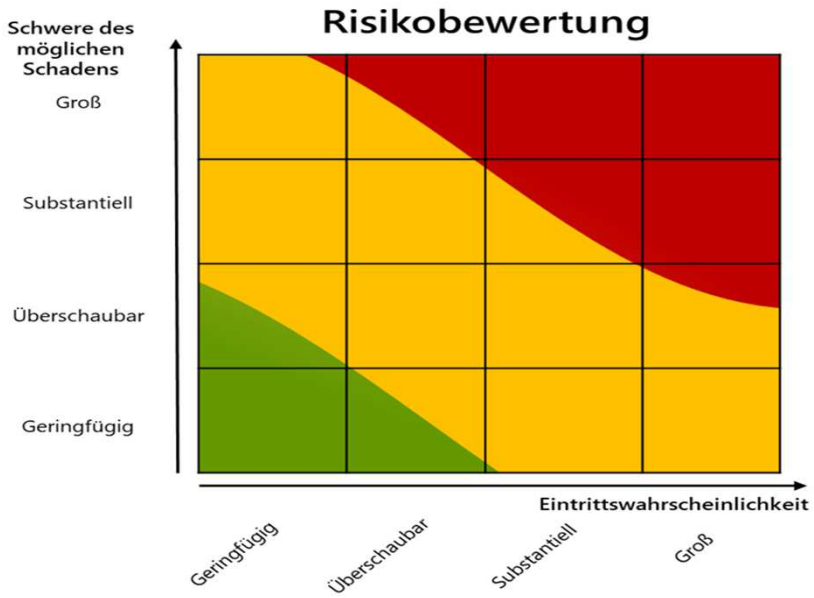
- „Auch im Datenschutz muss der Schutzbedarf festgelegt werden, um angemessen technische und organisatorische Schutzmaßnahmen bestimmen und konfigurieren zu können. Das Standard-Datenschutzmodell (SDM) bietet eine ganze Reihe an Kriterien, um das Risiko eines Grundrechtseingriffs, und daraus folgend des Schutzbedarfs, anhand von drei Stufen zu bestimmen.“

BSI-Kompendium, Baustein CON.2: Datenschutz

CON.2.A1 Umsetzung Standard-Datenschutzmodell

- Es MUSS geprüft werden, ob das SDM angewendet wird. Eine etwaige Nichtberücksichtigung des vollständigen Schutzzielekatalogs und eine Nichtanwendung der SDM-Methodik sowie der Referenzmaßnahmen MÜSSEN begründet werden.

Risiken für Betroffene (Grundrechtseingriff)



Geringes Risiko

Risiko

Hohes Risiko

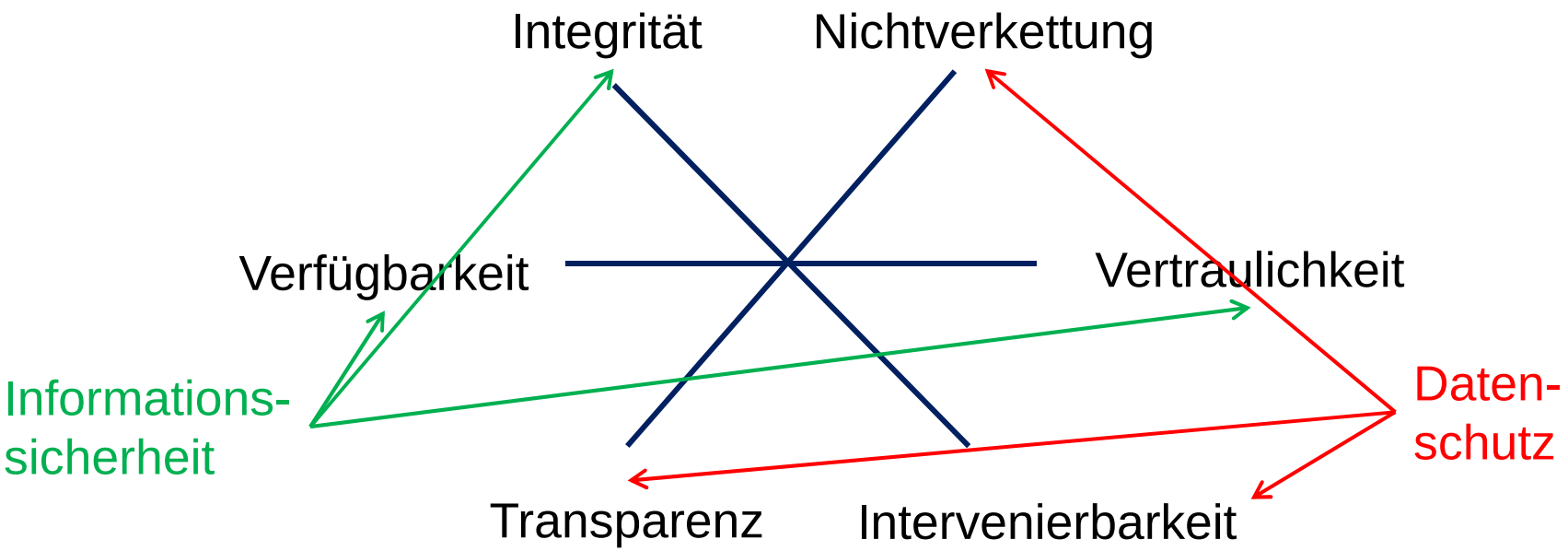
Das Standard-Datenschutzmodell

Eine Methode zur Datenschutzberatung und -prüfung auf der Basis einheitlicher Gewährleistungsziele

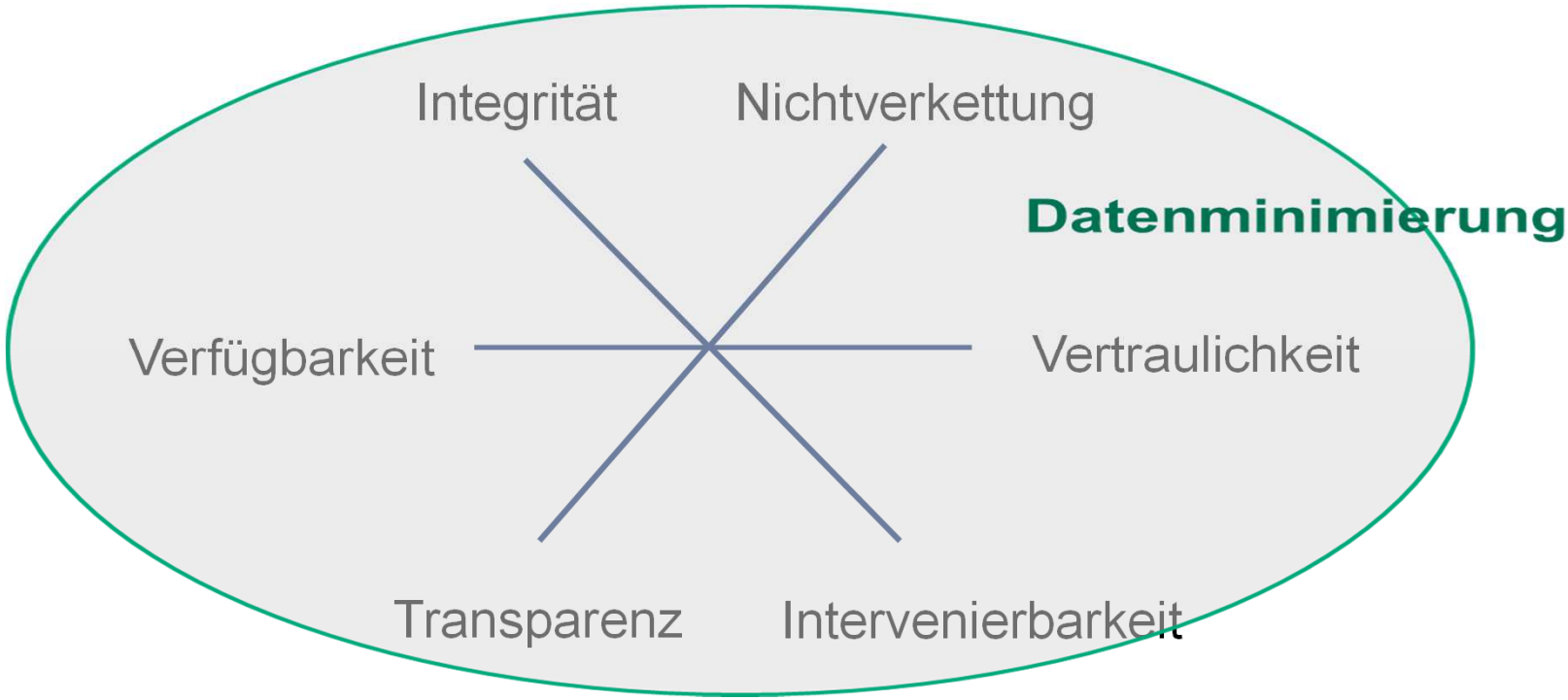
Gewährleistungsziele – wofür?

- Wie kann der Jurist sichergehen, dass rechtliche Anforderungen tatsächlich technisch umgesetzt werden?
- Normen lassen sich nicht ohne Weiteres technisch operationalisieren, d. h. in technische Funktionen umsetzen.
- Juristen und Techniker müssen ihre Anforderungen transformieren können!

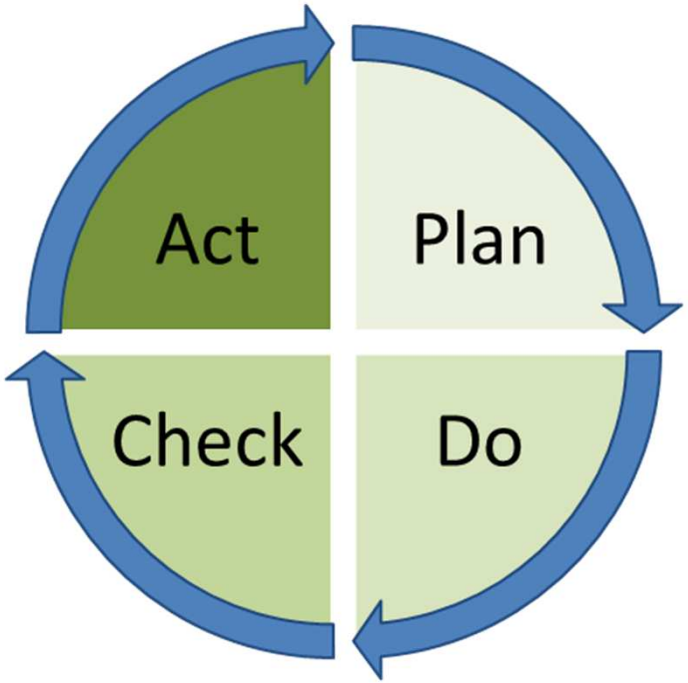
Systematisierung der Schutzziele



Systematisierung der Schutzziele



PDCA-Zyklus



PDCA-Zyklus nach dem SDM

Plan	⟹	Planen / Spezifizieren
Do	⟹	Implementieren
Check	⟹	Kontrollieren / Prüfen / Beurteilen
Act	⟹	Verbessern

Datenschutzmanagement

Gesetze, Verträge und (funktionale) Bearbeitungsbeschreibung

1. Planen / Spezifizieren
Welche Daten, IT-Systeme und Prozesse sind einzubeziehen, um eine Verarbeitung beurtei-len und prüfen zu können?
(relevant/nicht-relevant?)

Spezifikation und Dokumentation
(Soll-Werte)

2. Implementieren
der Verarbeitungsfunktionen und der technischen und organisatorischen Maßnahmen inkl. der Herstellung der Prüfbarkeit

Dokumentation des laufenden Betriebs
(Ist-Werte)

3a. Kontrollieren / Prüfen
Welche Informationen sind erforderlich, um zu prüfen?
(Soll-Ist-Vergleich)

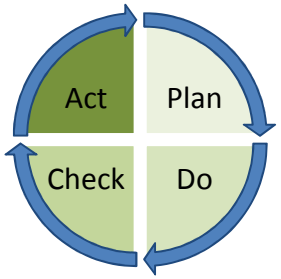
Prüfergebnisse

3b. Beurteilen
Sind die rechtlichen Vorgaben erfüllt und sich die Maßnahmen ausreichend und wirksam?
(rechtskonform/nicht-rechtskonform?)

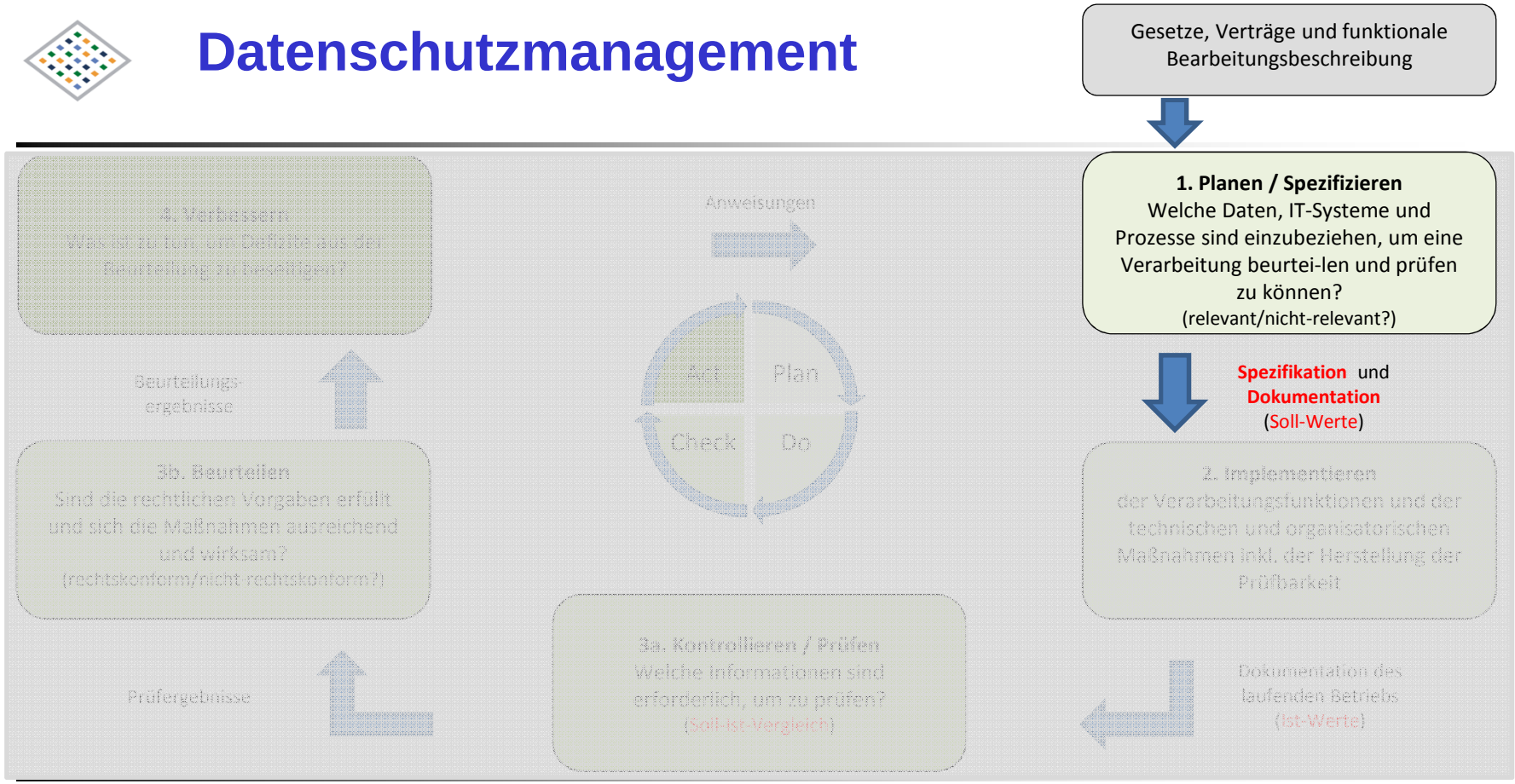
Beurteilungs-ergebnisse

4. Verbessern
Was ist zu tun, um Defizite aus der Beurteilung zu beseitigen?

Anweisungen



Datenschutzmanagement



1) Planen / Spezifizieren

Art. 4 Satz 1 Nr. 4 DS-GVO: Verantwortlicher

Der Verantwortliche ist derjenige, der … über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.

Art. 25 Abs. 1 DS-GVO: Datenschutz durch Technikgestaltung

Der Verantwortliche trifft zum Zeitpunkt der Festlegung der Mittel geeignete technische und organisatorische Maßnahmen

Art. 35 Abs. 1 DS-GVO: Datenschutz-Folgenabschätzung

Hat die Verarbeitung ein hohes Risiko für Betroffene, führt der Verantwortliche vorab eine Abschätzung der Folgen der Verarbeitung für den Schutz personenbezogener Daten durch.

1) Planen

Welche Aspekte beinhaltet die Planung?

a. Beschreibung der Datenverarbeitung
b. Identifikation und Dokumentation aller beteiligten „Akteure“
c. Identifikation und Dokumentation der Rechtsgrundlagen
d. Durchspielen von Use-Cases, um Risikoquellen erkennen zu können („Angreifermodells“)
e. Bestimmung des Risikos für die Rechte und Freiheiten Betroffener
f. Erarbeitung einer Dokumentation mit funktionalen Anforderungen
g. Bestimmung technischer und organisatorischer Maßnahmen
h. Erstellung und förmliche Abnahme des Lastenheftes
i. Erstellung von Test- und Pilotierungskonzepten
j. Erarbeitung der Freigabeprozedur / des Freigabeprozesses

1) Spezifizieren

Folgende Ebenen sind zu betrachten und darzustellen:

a. die Gestaltung der Prozesse („Fachlichkeit“) die den fachrechtlichen und datenschutzrechtlichen Anforderungen genügen müssen,
b. die Nutzung einer Fachapplikation durch die Sachbearbeitung,
c. die Technik der Datenverarbeitung, der Prozesse, IT-Systeme und IT-Infrastrukturen,
d. die Schnittstellen von Prozessen und IT-Systemen sowie
e. die jeweilige Administration der vorgenannten Ebenen

1) Dokumentieren

Ziel der Dokumentation ist die Sicherung der Transparenz

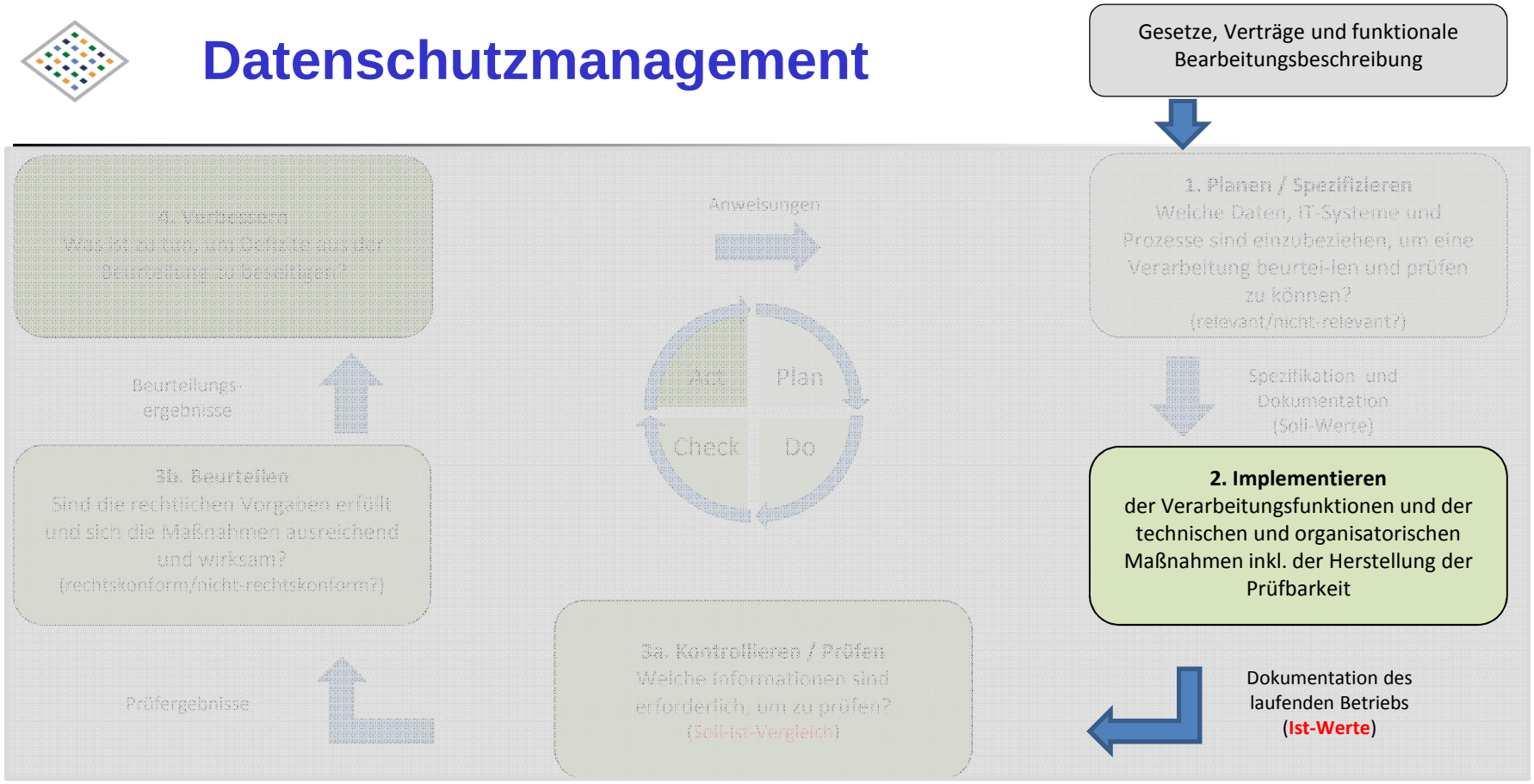
- von Datenbeständen,
- von Transformationen zwischen Daten,
- der benutzten Systemkomponenten, deren Funktionen und Schnittstellen,
- der Prozesse innerhalb von IT-Systemen und Organisationen und über IT-Systemgrenzen und Organisationsgrenzen hinweg und
- der Nachvollziehbarkeit von Entscheidungen und Verarbeitungshandeln.

1) Dokumentieren

Formale Anforderungen an die Dokumentation:

a. Strukturierung der Gesamtdokumentation
b. Dokumentation darüber, welcher Teil der Dokumentation der Verarbeitung als Papierausdruck und welcher Teil elektronisch vorliegt
c. Angemessenheit
d. Vollständigkeit
e. Revisionsfestigkeit
f. Aktualität
g. Fortschreibung

Datenschutzmanagement



2) Implementieren

Welche Aspekte beinhaltet die Implementierung?

a. Softwareentwicklung
b. Hardwareauswahl- und Bereitstellung
c. Umsetzung der technischen und organisatorischen Maßnahmen
d. Starten aller Protokollierungsfunktionen

→ Start des Test-, Pilot- oder Wirkbetriebs der Verarbeitungstätigkeit

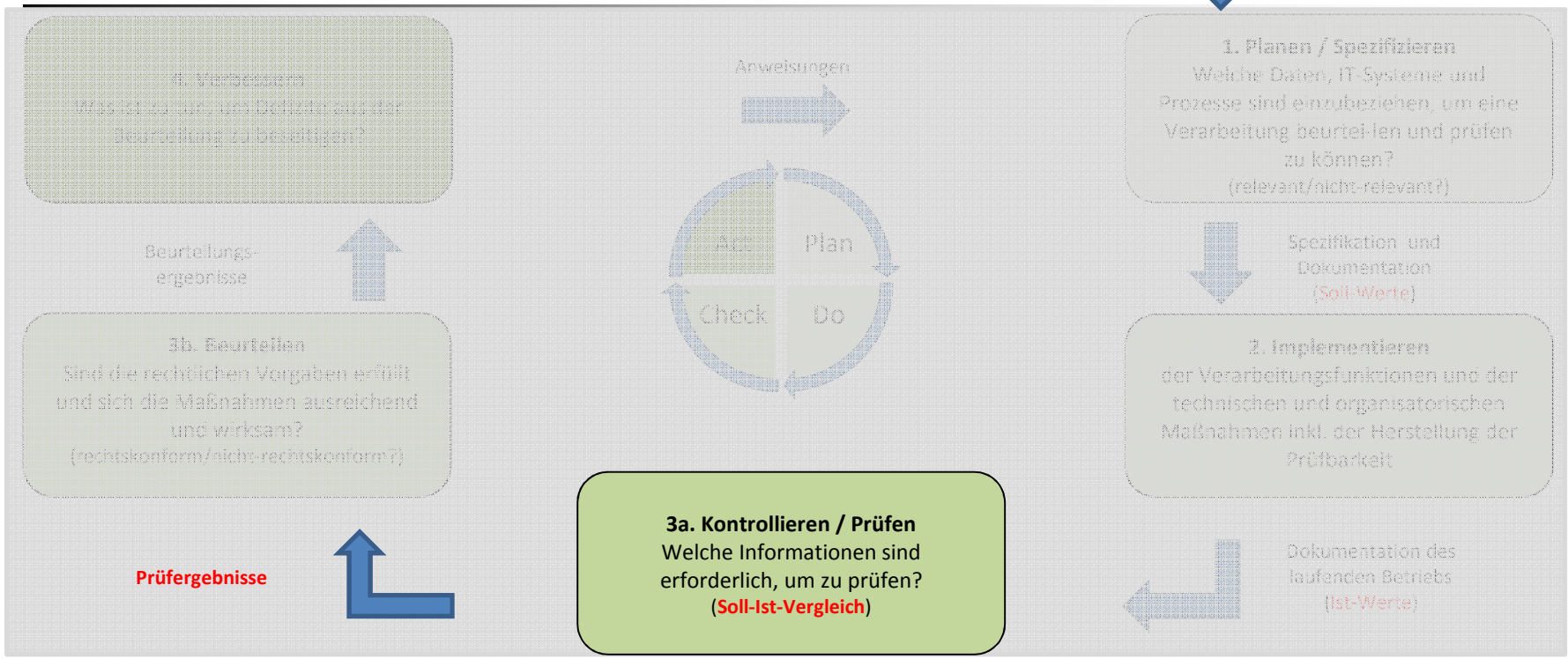
2) Protokollierung

Was ist zu protokollieren?

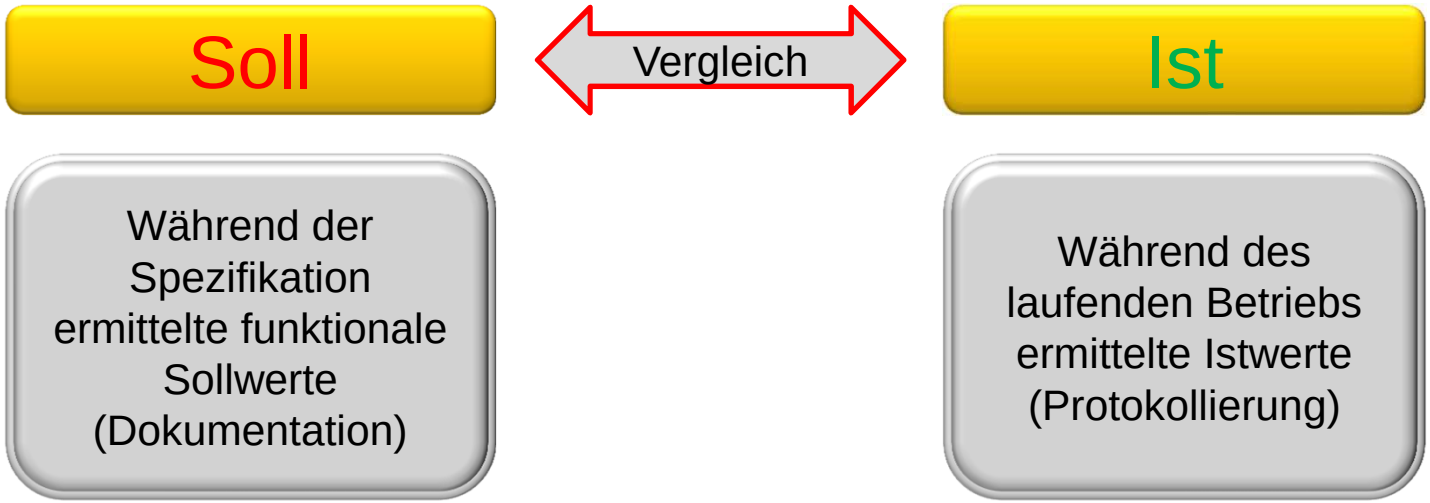
a. Zeitkomponente („Wann?“)
b. Instanz, die eine Aktivität auslöst („Wer?“)
c. Aktivität bzw. Ereignis, das durch die Instanz ausgelöst wurde („Was?“)
d. Speicherinstanz (Quelle und Ziel), die diese Protokolldaten speichert („Protokollierung durch wen?“)

Datenschutzmanagement

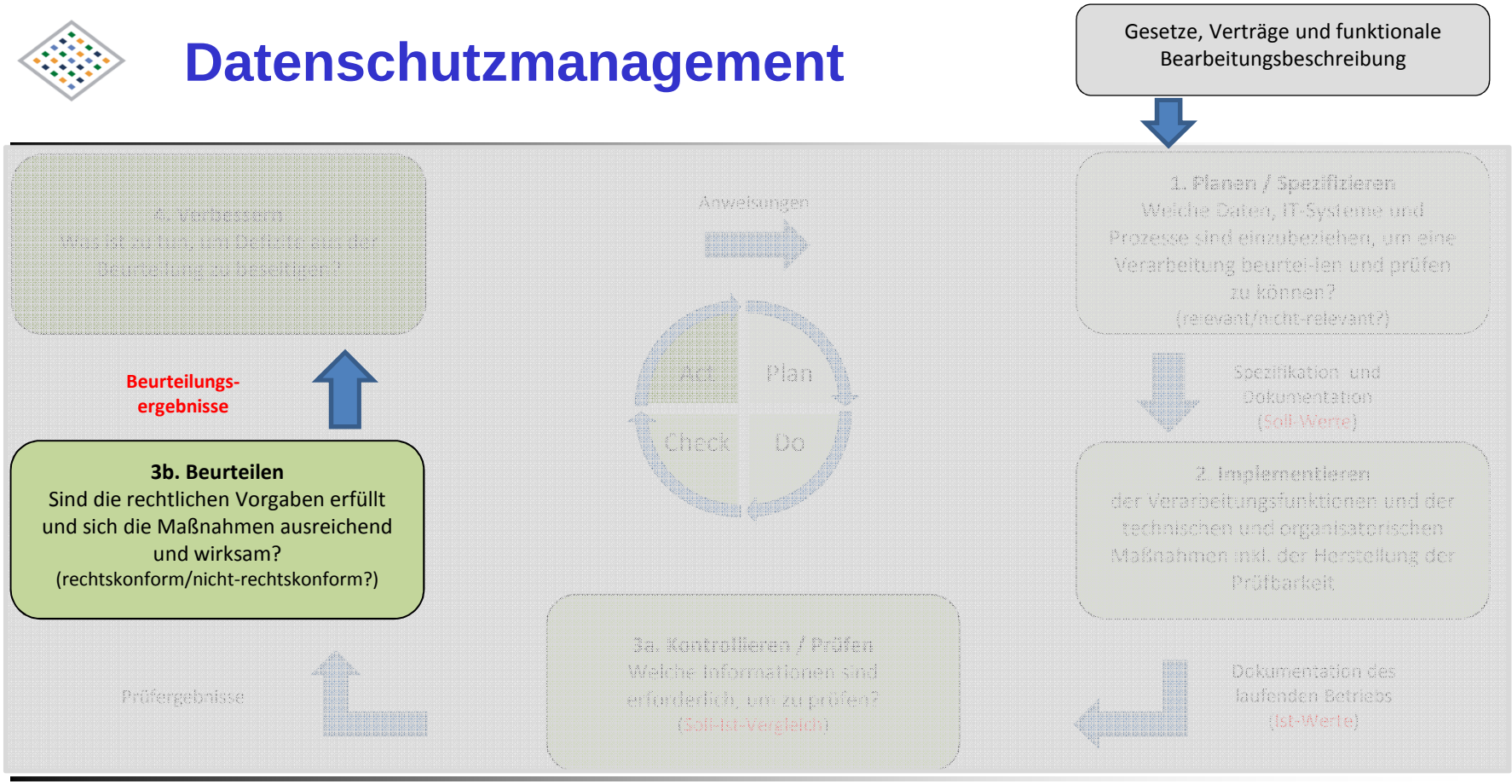
Gesetze, Verträge und funktionale Bearbeitungsbeschreibung



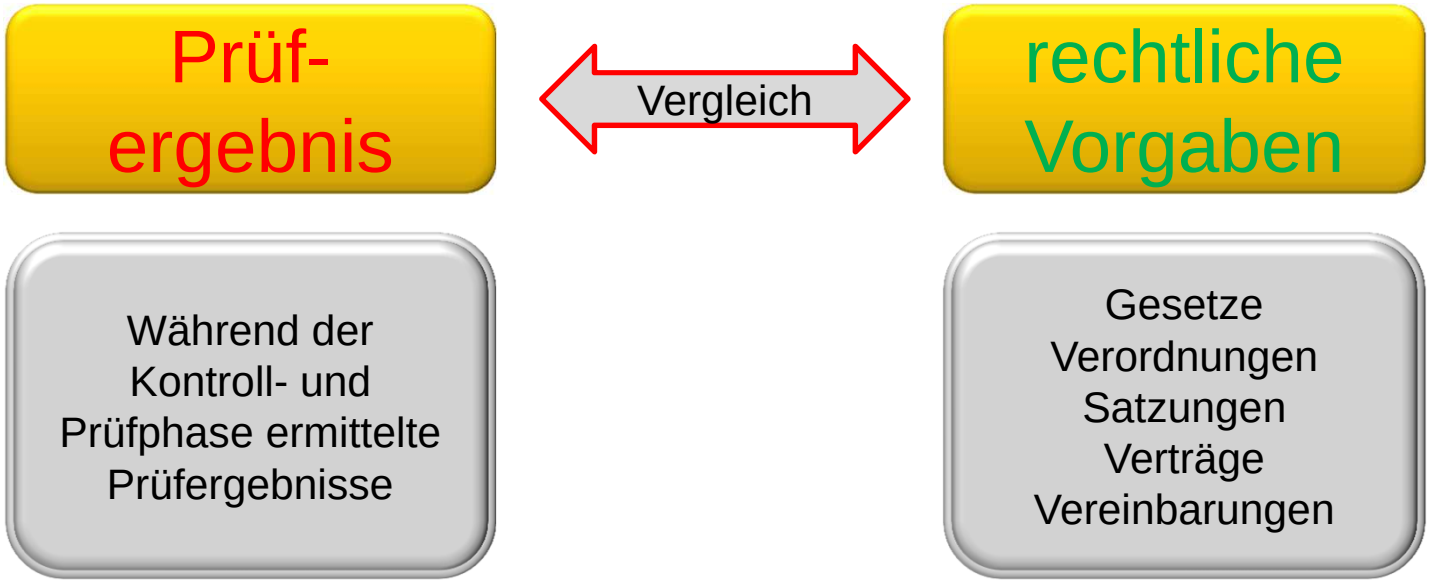
3a) Kontrollieren / Prüfen



Datenschutzmanagement



3b) Beurteilen

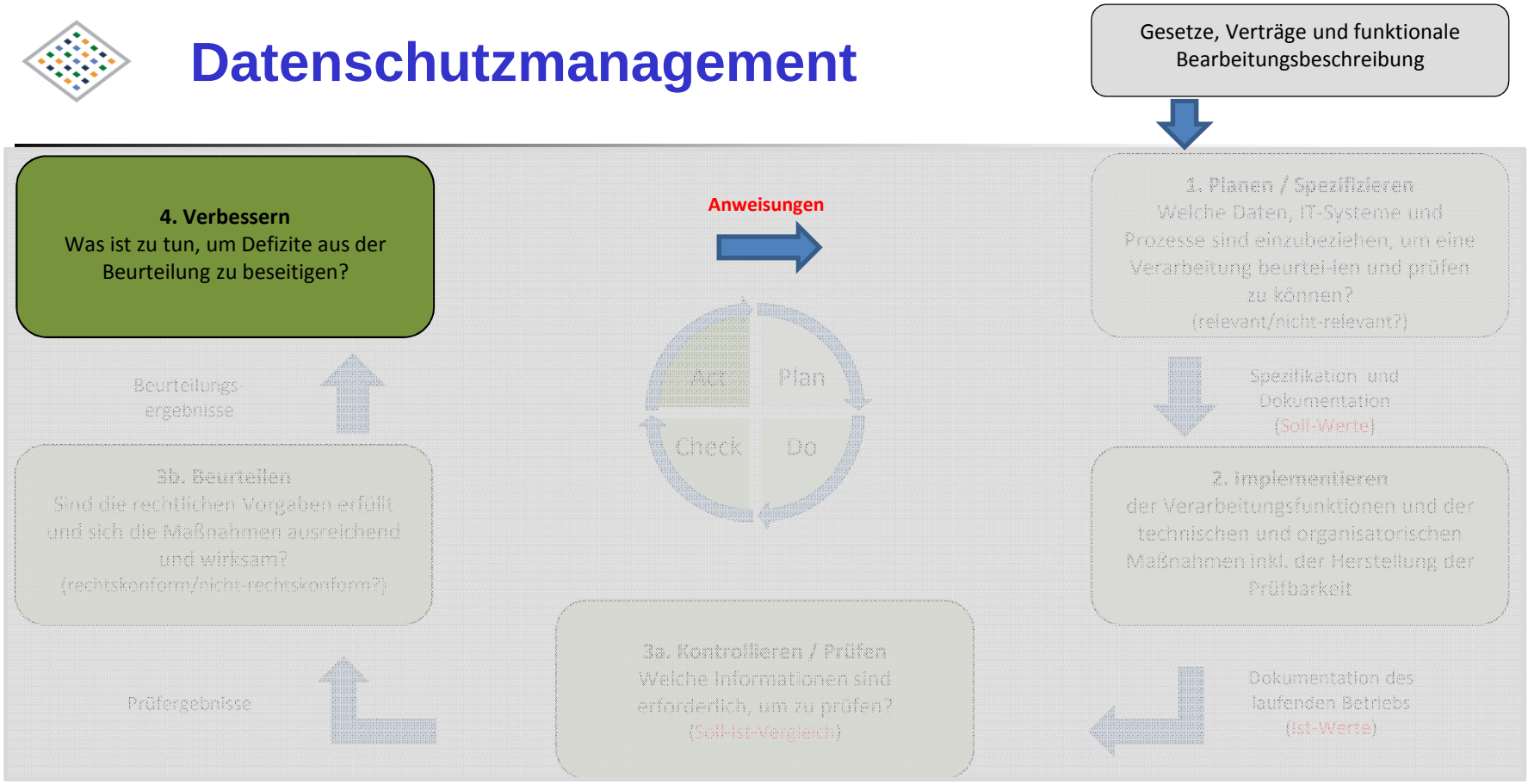


3b) Beurteilen

Zentrale Frage: Ist die Verarbeitung rechtskonform?

- Beurteilung wird bewusst als extra Phase ausgewiesen
- die Prüfergebnisse aus der Phase Kontrollieren/Prüfen werden mit den rechtlichen Vorgaben verglichen
- der Zweck des SDM besteht also auch darin, die rechtliche Prüfung einer Datenverarbeitung zu unterstützen
- die Ergebnisse der Phase 3 bilden die Grundlage zur Behebung von Defiziten (Verbessern).

Datenschutzmanagement



4) Verbessern

Verarbeitung
ist (noch) nicht
rechtkonform

Verarbeitung
verbessern und
Änderungen
anweisen

Verarbeitung
ist
rechtkonform

kein unmittelbarer
Handlungsbedarf

4) Verbessern

Indikatoren für fehlende Rechtskonformität:

- eine Verarbeitung wurde nicht nachweislich hinreichend geplant und spezifiziert
- es liegen keine hinreichende Dokumentation und keine Protokolldaten zur Kontrolle
- es erfolgt keine methodischen Prüfung oder Beurteilung einer Verarbeitung
- der laufende Betrieb einer Verarbeitung unterliegt keiner fortwährenden Kontrolle und Prüfung
- festgestellte Mängeln führen nicht zu wirksamen Aktivitäten, die zur Verbesserung führen

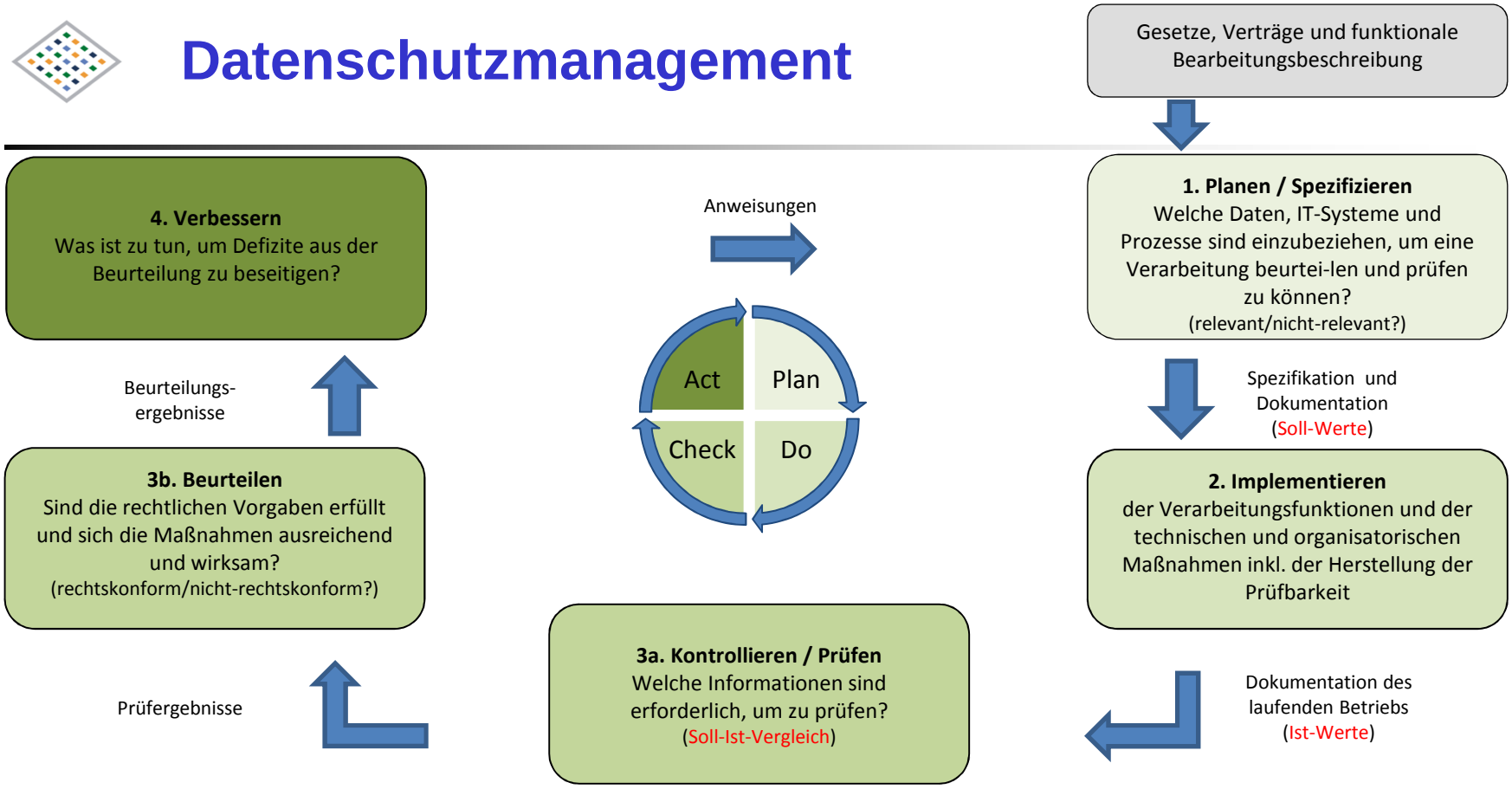
Einrichtung des Datenschutzmanagement-Systems

Datenschutzmanagement-System (DSMS)

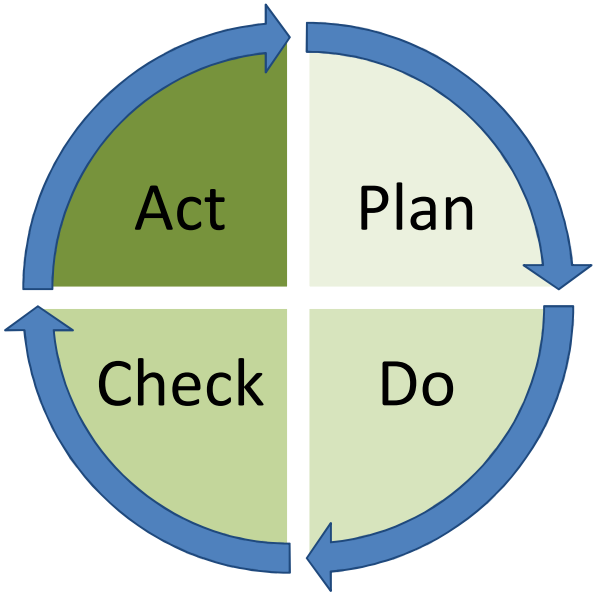
Einrichtung des DSMS:

- Verantwortlichen für DSMS benennen („Projektmanager“)
- Klärung der Rolle des Datenschutzbeauftragten (in kleineren Organisationen oft Personenidentität)
- Abgrenzung zur IT-Revision und zum IT-Sicherheitsbeauftragten
- Erarbeitung, Spezifizierung und Dokumentation der Prozesse des DSMS
- Verzeichnis der Verarbeitungstätigkeiten als zentrales Dokument heranziehen
- Ressourcen „sichern“ (Personal, Instrumente, Zeit, Budget)

Datenschutzmanagement



Datenschutzmanagementprozess



Weiterführende Informationen

- SDM-Methode Version 1.1
  https://www.datenschutz-mv.de/static/DS/Dateien/Datenschutzmodell/SDM-Methode_V_1_1.pdf

- Bausteine des Referenz-Maßnahmenkatalogs:

  - Datenschutzmanagement
    https://www.datenschutz-mv.de/static/DS/Dateien/Datenschutzmodell/Bausteine/SDM-V1.1_80_Datenschutzmanagement_V1.0_uagsdmbs_final.pdf/
  - Planung und Spezifikation
    https://www.datenschutz-mv.de/static/DS/Dateien/Datenschutzmodell/Bausteine/SDM-V1.1_41_Planung_Spezifikation_V1.0_uagsdmbs_final.pdf
  - Dokumentation
    https://www.datenschutz-mv.de/static/DS/Dateien/Datenschutzmodell/Bausteine/SDM-V1.1_42_Dokumentation_V1.0_uagsdmbs_final.pdf
  - Protokollierung
    https://www.datenschutz-mv.de/static/DS/Dateien/Datenschutzmodell/Bausteine/SDM-V1.1_43_Protokollierung_V1.0_uagsdmbs_final.pdf

Der Landesbeauftragte für Datenschutz und Informationsfreiheit
Mecklenburg-Vorpommern

Werderstraße 74a

19055 Schwerin

Telefon: 0385-59494-0

Telefax: 0385-59494-58

E-Mail: info@datenschutz-mv.de

Internet: www.datenschutz-mv.de
www.informationsfreiheit-mv.de
www.medienscout-mv.de