Musterprozesse für das Datenschutzmanagement

Dr. Martin Meints

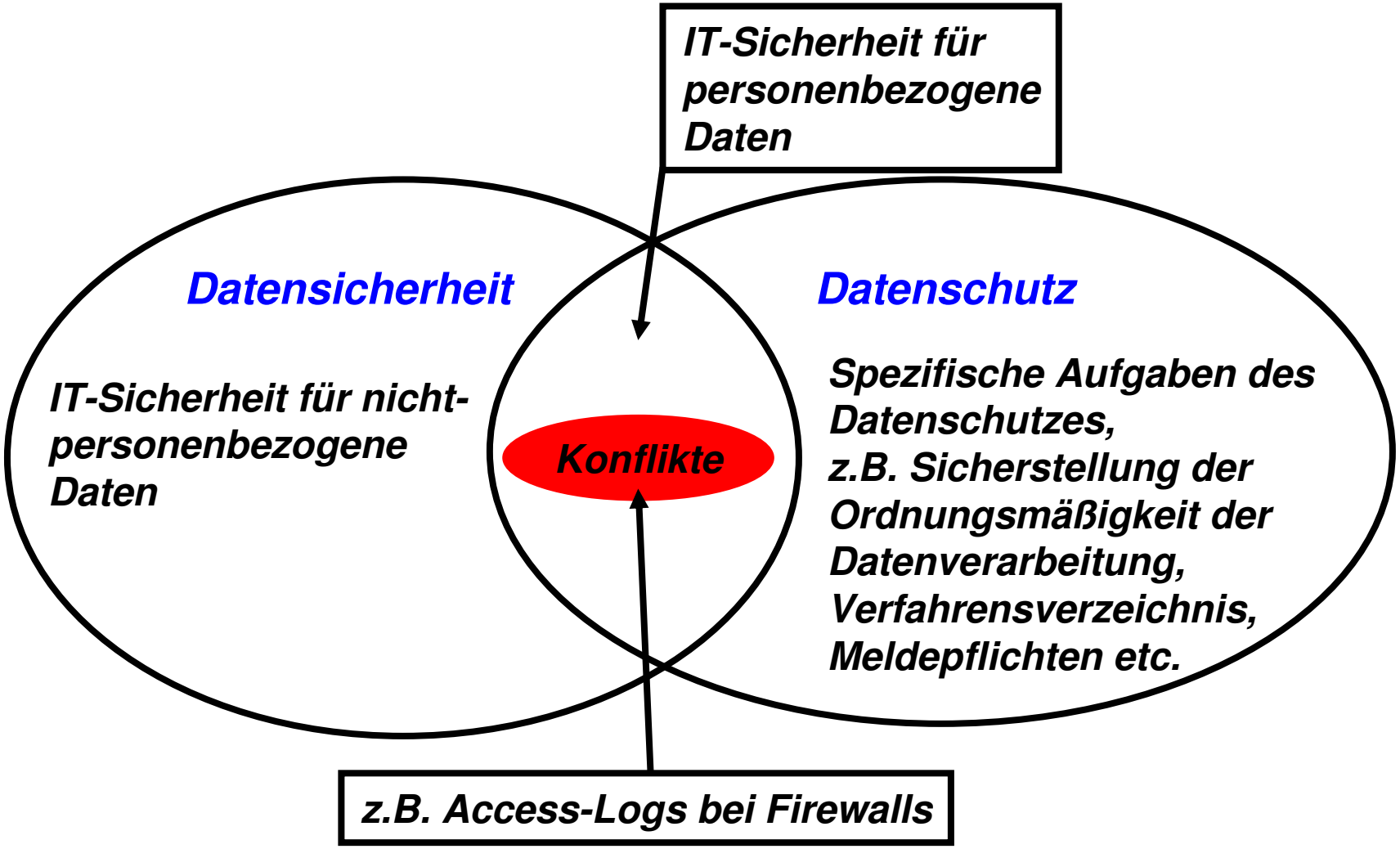
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

ULD61@datenschutzzentrum.de

Inhalt

- Was kann modernes Datenschutzmanagement von Qualitätsmanagement, IT-Sicherheitsmanagement und IT-Governance lernen?
- Kernelemente eines prozessorientierten Datenschutzmanagements
- Beispiel 1: Musterprozess für die Integration von Datenschutzmanagement in IT-Grundschutz
- Beispiel 2: Der gleiche Musterprozess unter dem Gesichtspunkt der Integration mit ITILv2

Datenschutz und Datensicherheit



Die 7 goldenen Regeln des Datenschutzes („Control Objectives" des Datenschutzes)

- Rechtmäßigkeit
  - Rechtsgrundlage: Rechtsgrundlage für die Verarbeitung oder Einwilligung
- Einwilligung
  - Regeln für die Wirksamkeit einer Einwilligung
- Zweckbindung
  - Daten dürfen nur für den Zweck verarbeitet werden, für den sie auch erhoben wurden
- Erforderlichkeit
  - Datensparsamkeit, Datenvermeidung
- Transparenz
  - Betroffenenrechte
- Datensicherheit
  - Angemessenheit, Stand der Technik
- Kontrolle

(nach Dr. Johann Bizer, DuD 5/2007)

Allgemeine Vorüberlegungen

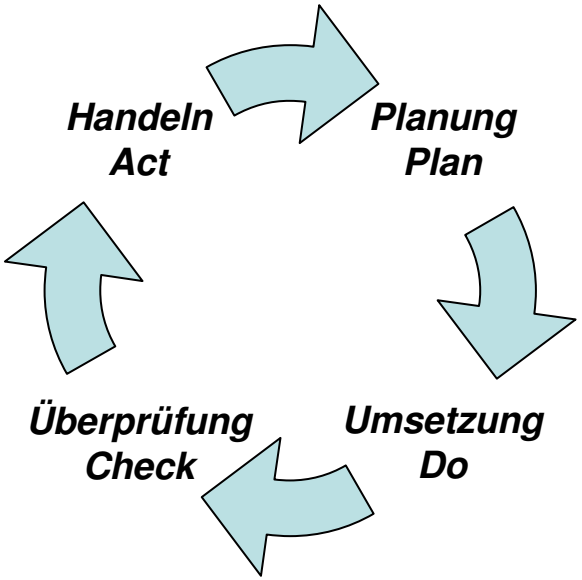
- Datenschutzanforderungen sind nicht einheitlich
  - Je nach Art der Organisation, dem zugehörigem staatlichen Sektor oder dem Bundesland gibt es unterschiedliche rechtliche Grundlagen
  - Verfahren zur Verarbeitung personenbezogener Daten sind sehr verschieden
  - Als Folge gibt es keine einheitliche Metrik für ein geeignetes (ausreichendes) Datenschutzniveau

- Datenschutz ist eine Daueraufgabe
  - Die Dynamik der Verfahren zur Verarbeitung personenbezogener Daten fordert eine ständige Sicherstellung des benötigten Datenschutzniveaus

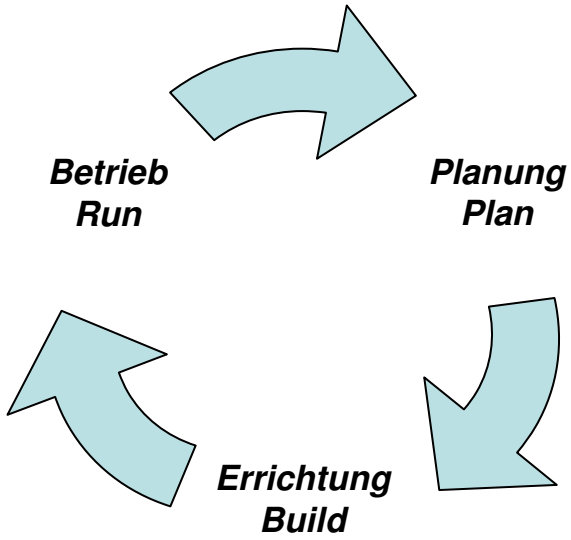
Allgemeine Überlegungen (fort.)

- Wie geht man mit derartigen Daueraufgaben um?
  - Geeignete Strukturen schaffen (Organigramm, Aufbauorganisation)
  - Ressourcen bereitstellen
  - Persönliche Verantwortung schaffen
  - Prozesse statt Projekte
    - Prozesseigentümer
    - Prozessverantwortlicher
    - Dokumentation
    - Qualitätsmanagement (z.B. unter Nutzung von KPI und Prozess-Reifegrad-Modellen)
  - Abdeckung aller Ebenen des Handelns einer Organisation
    - Strategie (durch Leitlinien (Policies))
    - Taktik (durch Konzepte)
    - Operatives Handeln (Maßnahmen, Dokumentation)
  - An entscheidenden Stellen werden zyklische Prozesse (Kreisprozesse) benötigt

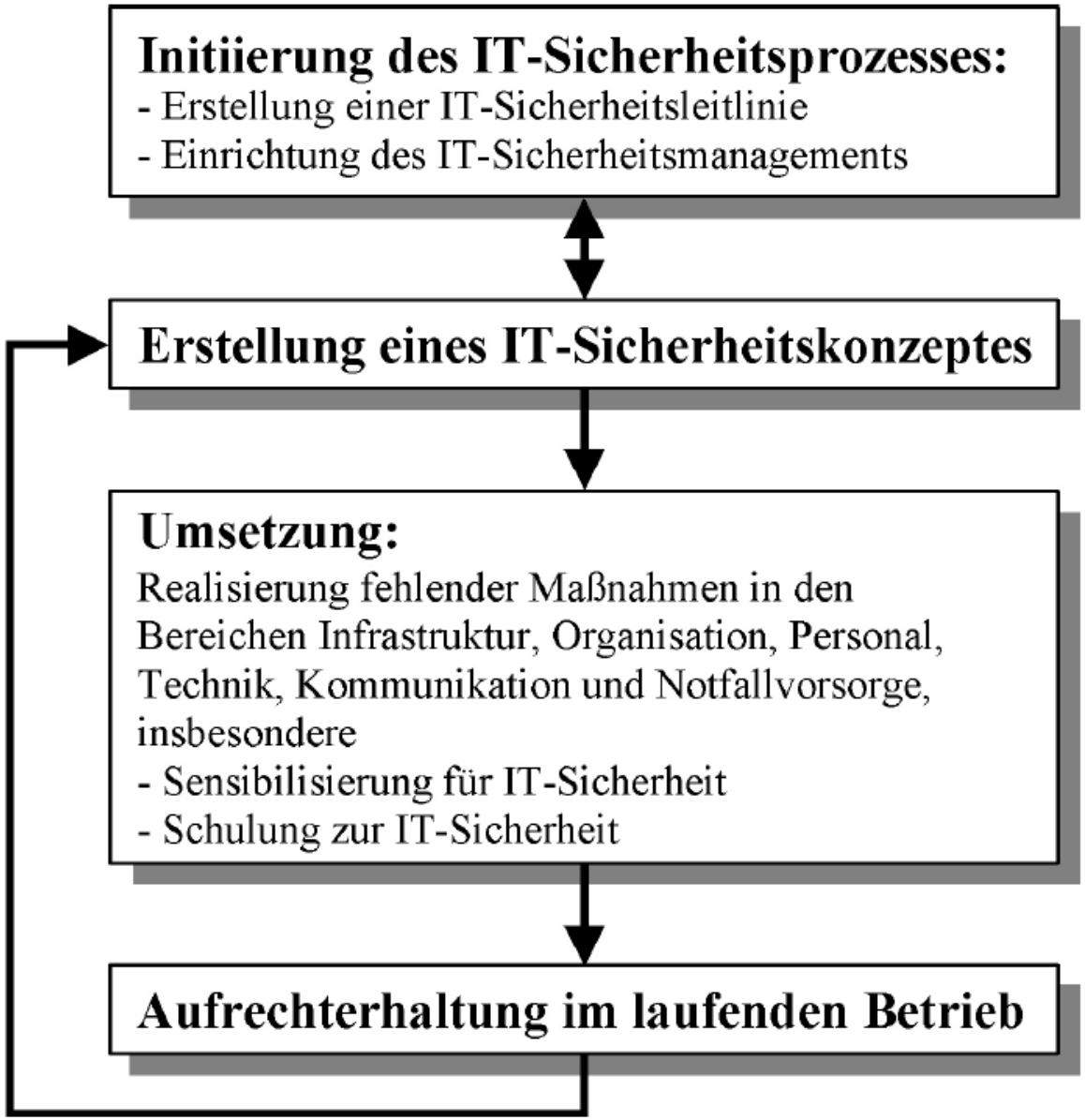
Wesentliche Prozesselemente



Deming-Zyklus



Lebenszyklen für IT-Verfahren

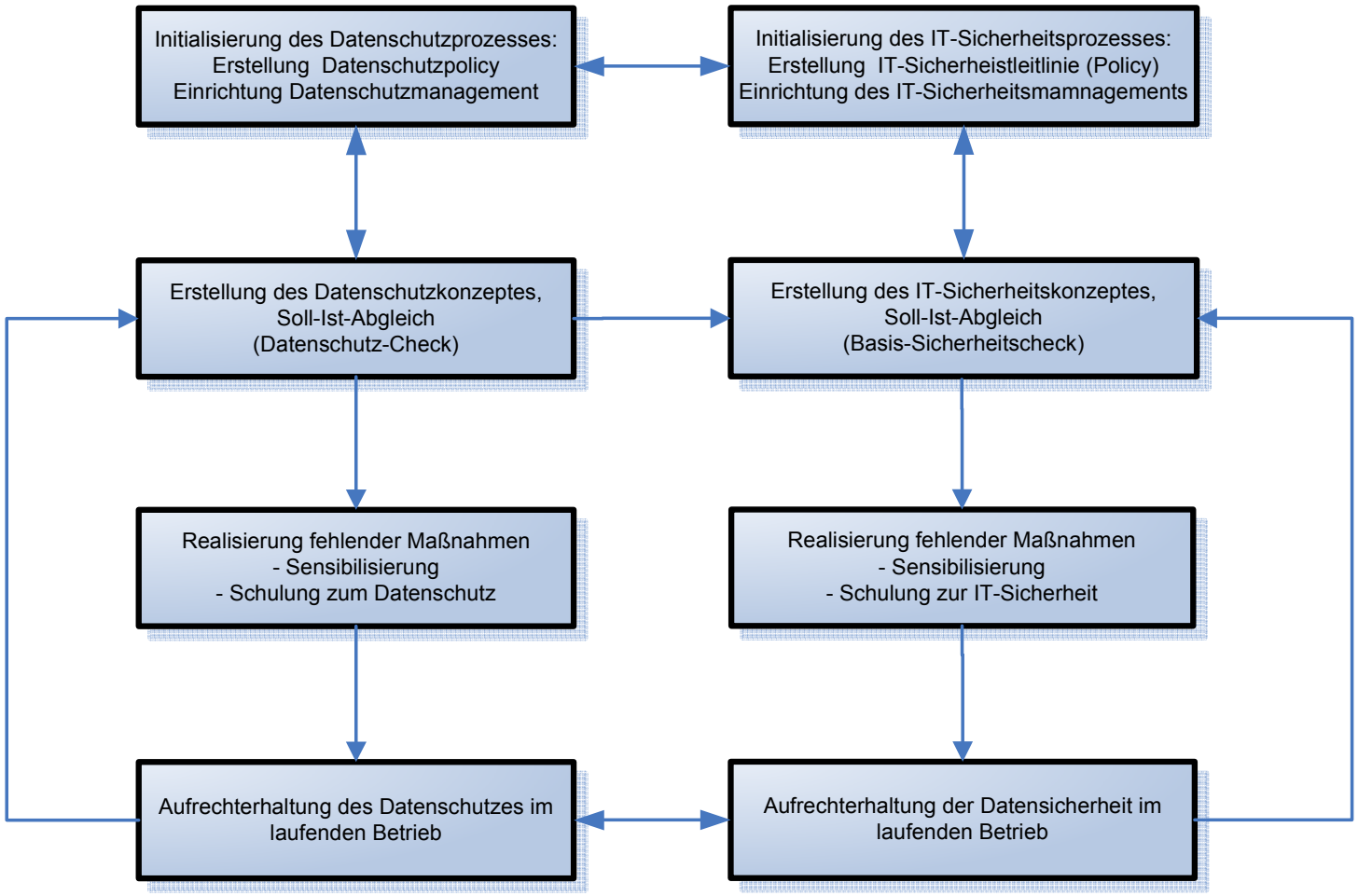


Quelle:
BSI-Standard 100-2

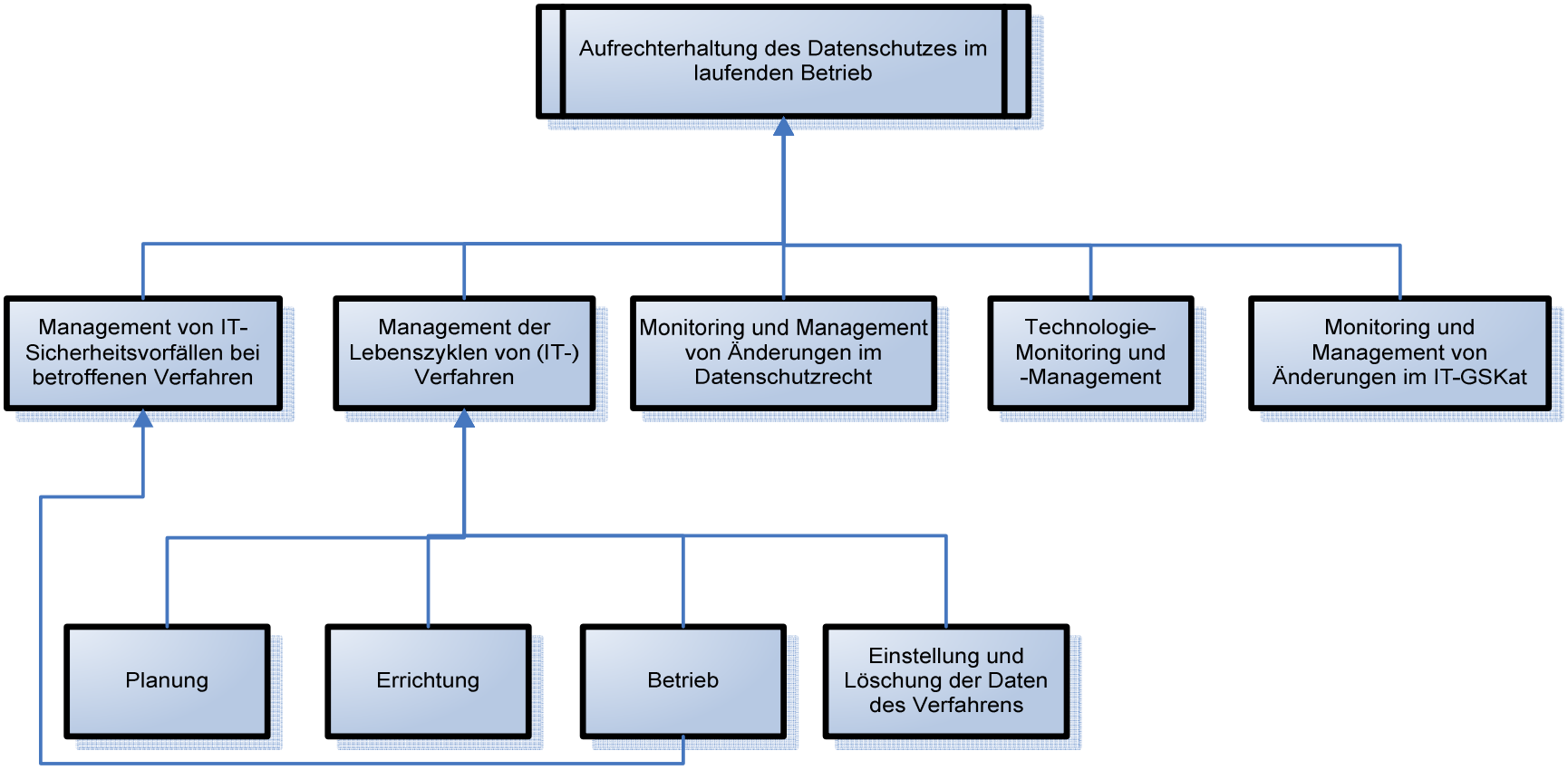
Musterprozess

- Ablauf und Prozessschritte sind sehr ähnlich wie bei Grundschutz
- Herzstück: Datenschutzkonzept
  - Kern: Verfahrensverzeichnis
  - Feststellung der rechtlichen Grundlagen für jedes Verfahren
  - Auswahl notwendiger (organisatorischen und technischen) Maßnahmen
- Integration von Datenschutz- und Datensicherheitsmanagement ist möglich
  - Z.B. bei kleinen Organisationen
  - Unterschiede in den Zielen und Aufgaben müssen jedoch berücksichtigt werden
- Unterstützungsprozesse für spezifische Aufgaben und der Prüfung, ob der Kernprozess neu gestartet werden muss

Datenschutz- und Datensicherheitsmanagement



Datenschutz- und Datensicherheits-management - Unterstützungsprozesse



Baustein „Datenschutz"

- Gefährdungslagen
  - **G 6.1 Fehlende Zulässigkeit der Verarbeitung personenbezogener Daten**
  - **G 6.2 Nichteinhaltung der Zweckbindung bei der Verarbeitung personenbezogener Daten**
  - **G 6.3 Überschreitung des Erforderlichkeitsgrundsatzes bei der Verarbeitung personenbezogener Daten**
  - **G 6.4 Fehlende oder unzureichende Datenvermeidung und Datensparsamkeit bei der Verarbeitung personenbezogener Daten**
  - **G 6.5 Verletzung des Datengeheimnisses bei der Verarbeitung personenbezogener Daten**
  - **G 6.6 Fehlende oder nicht ausreichende Vorabkontrolle**

Baustein „Datenschutz" (2)

- Gefährdungslagen
  - **G 6.7 Gefährdung der Rechte Betroffener bei der Verarbeitung personenbezogener Daten**
  - **G 6.8 Fehlende oder unzureichende Absicherung der Datenverarbeitung im Auftrag bei der Verarbeitung personenbezogener Daten**
  - **G 6.9 Fehlende Transparenz für den Betroffenen und die Datenschutz-Kontrollinstanzen**
  - **G 6.10 Gefährdung vorgegebener Kontrollziele bei der Verarbeitung personenbezogener Daten**
  - **G 6.11 Fehlende oder unzureichende Absicherung der Verarbeitung personenbezogener Daten im Ausland**
  - **G 6.12 Unzulässige automatisierten Einzelfallentscheidungen oder Abrufe bei der Verarbeitung personenbezogener Daten**
  - **G 6.13 Fehlende oder unzureichende Datenschutzkontrolle**

Baustein „Datenschutz" (3)

- Maßnahmen
- Planung und Konzeption
  - **M 7.1 (C) Datenschutzmanagement**
  - **M 7.2 (B) Regelung der Verantwortlichkeiten im Bereich Datenschutz**
  - **M 7.3 (A) Aspekte eines Datenschutzkonzeptes**
  - **M 7.4 (A) Prüfung rechtlicher Rahmenbedingungen und Vorabkontrolle bei der Verarbeitung personenbezogener Daten**
  - **M 7.5 (A) Festlegung von technisch-organisatorischen Maßnahmen entsprechend dem Stand der Technik bei der Verarbeitung personenbezogener Daten**

Baustein „Datenschutz" (4)

- Maßnahmen - Umsetzung
  - **M 7.6 (A) Verpflichtung/Unterrichtung der Mitarbeiter bei der Verarbeitung personenbezogener Daten**
  - **M 7.7 (A) Organisatorische Verfahren zur Sicherstellung der Rechte der Betroffenen bei der Verarbeitung personenbezogener Daten**
  - **M 7.8 (A) Führung von Verfahrensverzeichnissen und Erfüllung der Meldepflichten bei der Verarbeitung personenbezogener Daten**
  - **M 7.9 (C) Datenschutzrechtliche Freigabe**
  - **M 7.10 (A) Meldung und Regelung von Abrufverfahren bei der Verarbeitung personenbezogener Daten**
  - **M 7.11 (A) Regelung der Auftragsdatenverarbeitung bei der Verarbeitung personenbezogener Daten**
  - **M 7.12 (A) Regelung der Verknüpfung und Verwendung von Daten bei der Verarbeitung personenbezogener Daten**

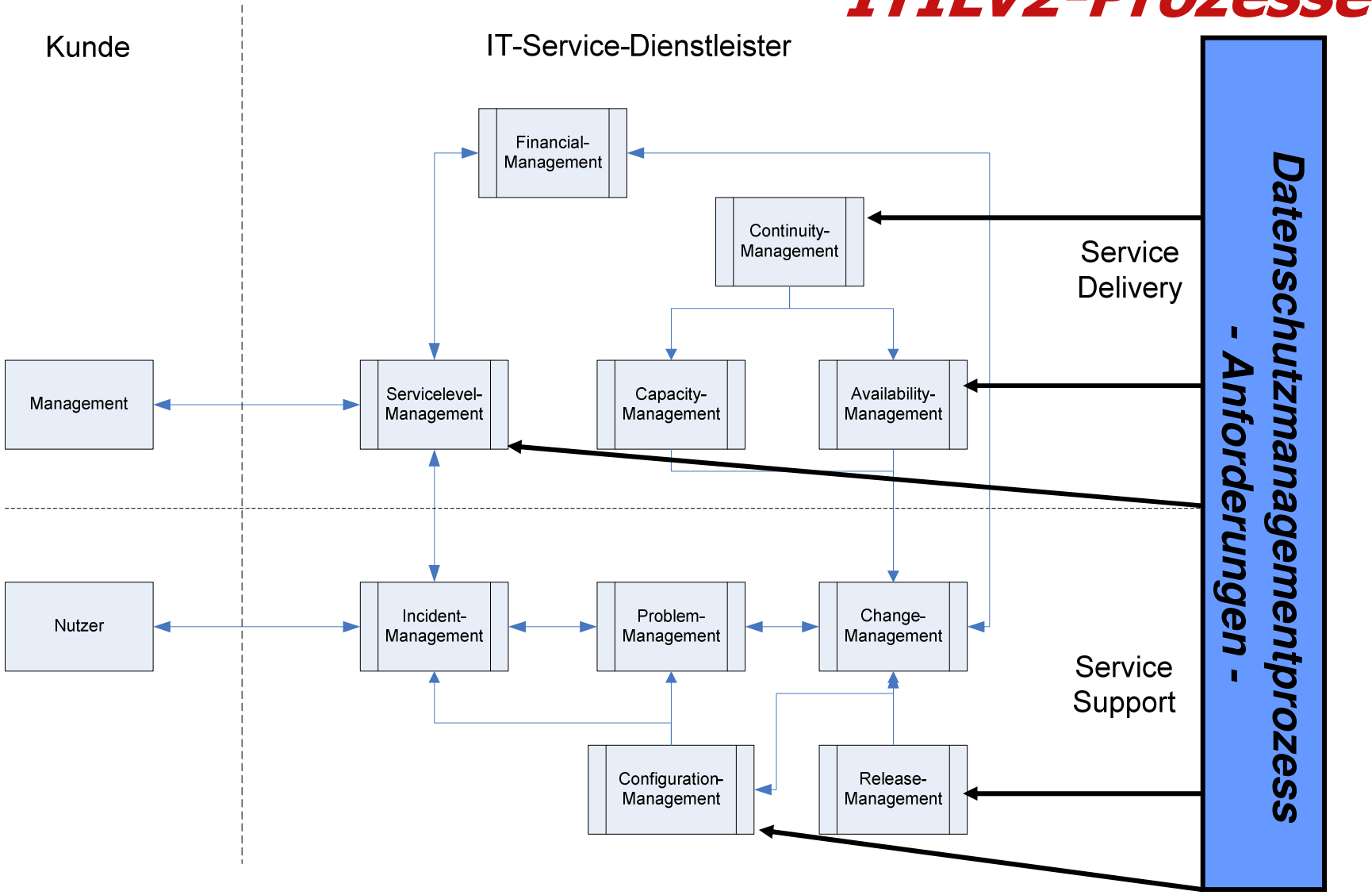
Baustein „Datenschutz" (5)

- Maßnahmen
- Betrieb
  - **M 7.13 (Z) Dokumentation der datenschutzrechtlichen Zulässigkeit**
  - **M 7.14 (A) Aufrechterhaltung des Datenschutzes im laufenden Betrieb**
  - **M 2.110 (A) Datenschutzaspekte bei der Protokollierung**
  - **M 7.15 (A) Datenschutzgerechte Löschung/Vernichtung**

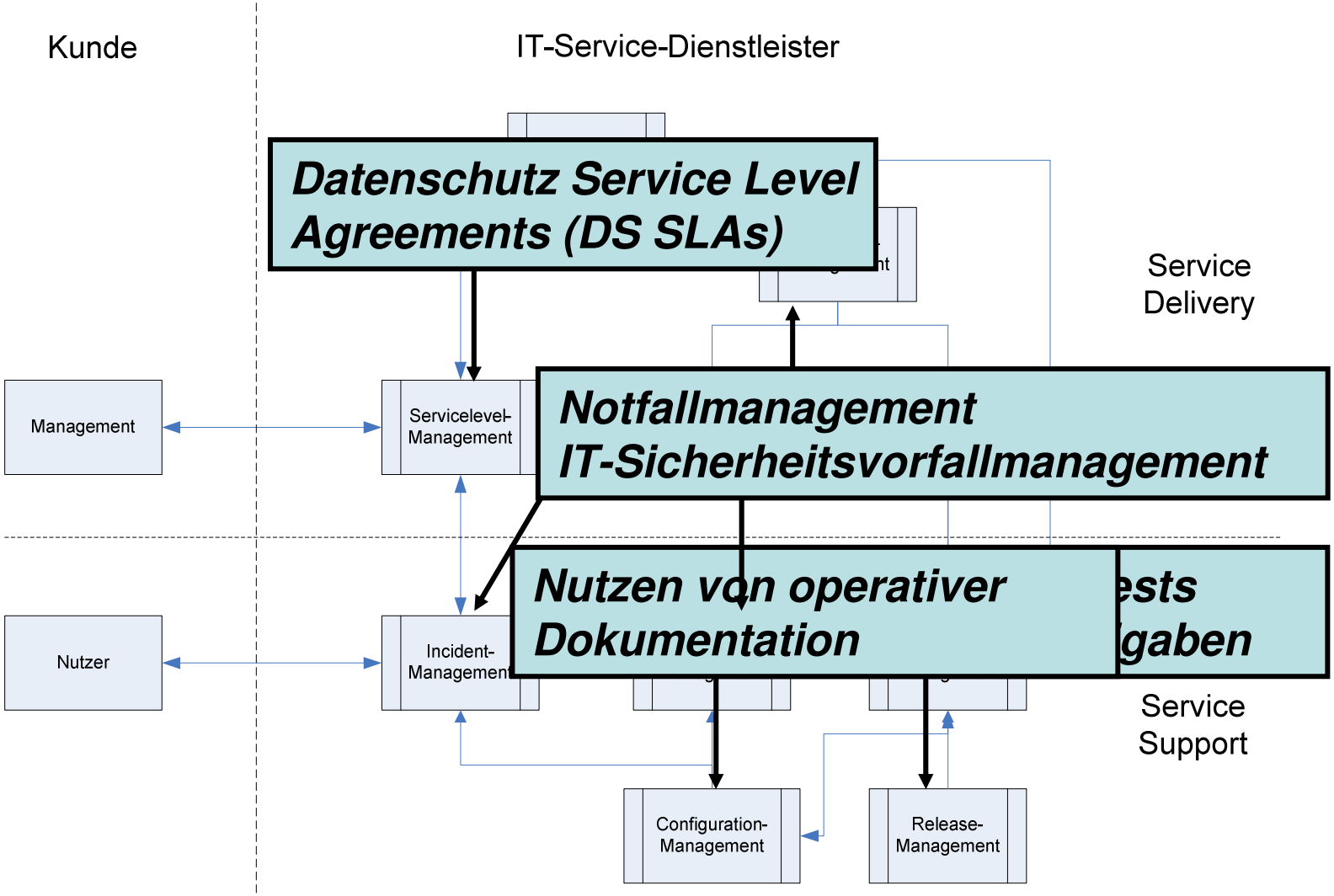
Nutzbarkeit von ITIL

- ITIL ist hochgradig auf den IT-Betrieb spezialisiert
- IT-betriebsbezogene Prozesse können genutzt werden
  - Einsteuern datenschutzspezifischer Aufgaben oder Prozessschritte
- Komplementäre Prozesse für Datenschutzaufgaben außerhalb des IT-Betriebs sind erforderlich

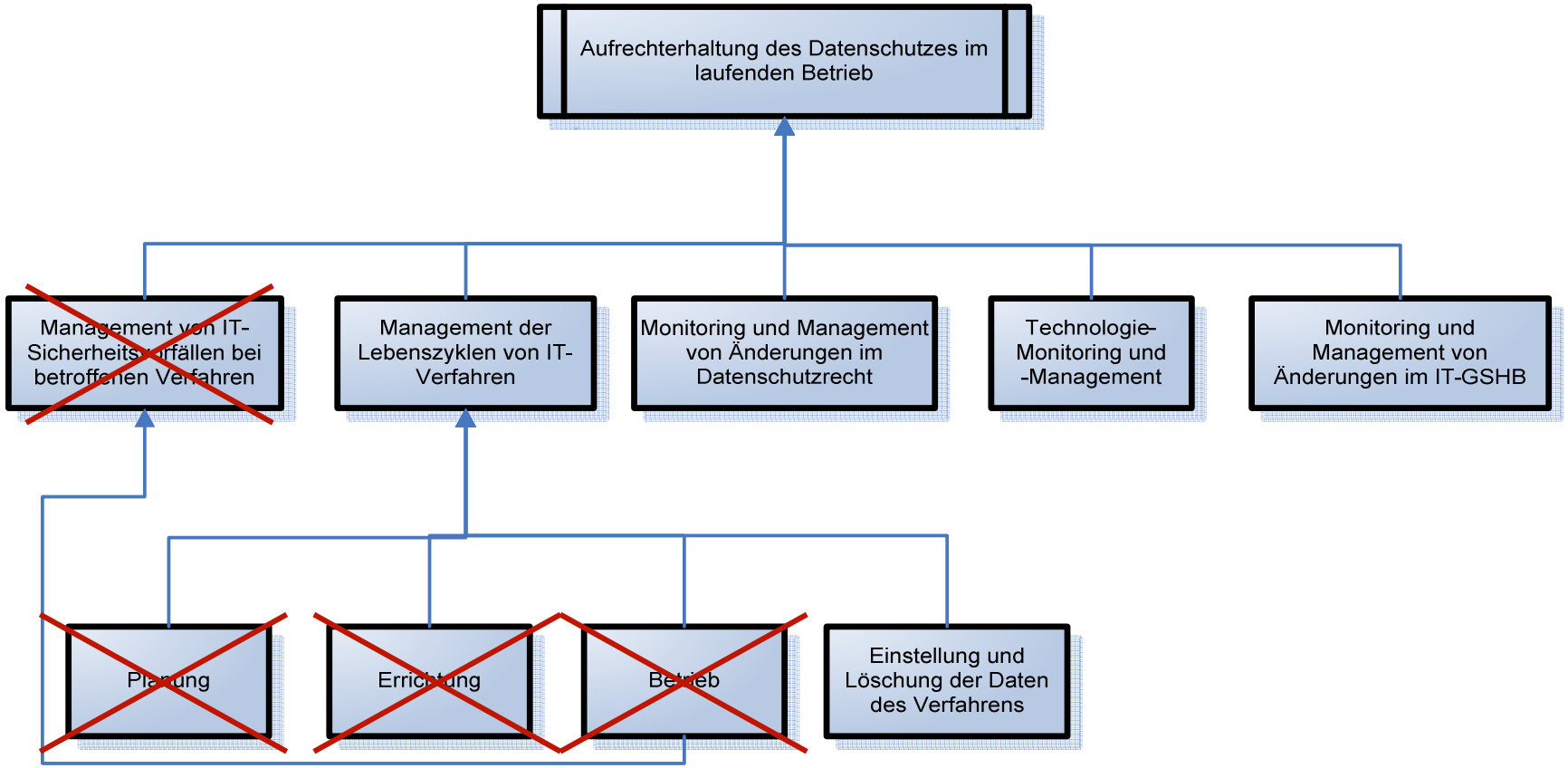
ITILv2-Prozesse



ITILv2-Prozesse



Datenschutz- und Datensicherheitsmanagement (2)



Zusammenfassung

- Musterprozesse, wie sie bereits erfolgreich u.a. im Qualitäts- und IT-Sicherheitsmanagement eingesetzt wurden, können auch im Datenschutzmanagement erfolgreich eingesetzt werden
- Als ein Beispiel wurde ein Musterprozess vorgestellt, der als Hilfsmittel in die IT-Grundschutz-Kataloge aufgenommen wurde
- Musterprozesse können so gestaltet werden, dass sie optimal bestehende Synergien mit bestehenden Musterprozessen erschließen
- Musterprozesse aus mehreren Bereichen (z.B. Datenschutz, IT-Sicherheitsmanagement und IT-Betrieb) können erfolgreich kombiniert werden

Quellen

- Meints, M., „Datenschutz durch Prozesse“, *Datenschutz und Datensicherheit* 31(2), Wiesbaden 2007.

- Hilfsmittel: Baustein B1.5 der IT-Grundschutzkataloge
  - http://www.bsi.de/gshb/baustein-datenschutz/index.htm
  - Der Baustein ist bereits in die Meta-Daten für das GSTool für die Grundschutz-Kataloge 2007 integriert
  - Zusätzliche Materialien des Bausteins:
    - Kreuzreferenztabellen für den Baustein B1.5
    - Zusätzlich sind Kreuzreferenztabellen für die Bewertung der Wirksamkeit von Grundschutzmaßnahmen bezogen auf die Sicherheitsziele aus der Anlage zu §9 Bundesdatenschutzgesetz (BDSG)

Vielen Dank für Ihre Aufmerksamkeit!

ULD

Unabhängiges Landeszentrum für
Datenschutz Schleswig-Holstein

Unabhängiges Landeszentrum für
Datenschutz Schleswig-Holstein
Dr. Martin Meints
Telefon: 0431 988 – 1226
ULD61@datenschutzzentrum.de
http://www.datenschutzzentrum.de/