TeleTrusT
Pioneers in IT security.

Informationstag "Ersetzendes Scannen"

Berlin, 19.04.2013

"Umsetzung der Richtlinie – Modularer Anforderungskatalog"

Dr. Astrid Schumacher/Dietmar Bremser, BSI

Bundesamt
für Sicherheit in der
Informationstechnik

TR RESISCAN 03138

Umsetzung der Richtlinie – Modularer Anforderungskatalog

Dietmar Bremser

TeleTrusT Informationstag „Ersetzendes Scannen“
19.04.2013

Agenda

- TR RESISCAN: Von der Motivation zur Umsetzung
- Der modulare Anforderungskatalog
- Die Zertifizierung

Bundesamt
für Sicherheit in der
Informationstechnik

Agenda

- TR RESISCAN: Von der Motivation zur Umsetzung
- Der modulare Anforderungskatalog
- Die Zertifizierung

Erinnerung an die Motivation

- **Rechtlich-technischer Lösungsansatz der TR:**
  - **Beweiswerterhalt** der dem Papier immanenten Sicherheitsmerkmale zum Integritäts- und Authentizitätsschutz beim Medienwechsel von analogen zu elektronischen Daten
  - **Zulässigkeit** des ersetzenden Scannes

- **Aspekte der TR**:

  → rechtlich begründete *technisch-organisatorische Anforderungen an den Scanprozess und das Scanprodukt*

  → Erreichung eines möglichst hohen, dem Original angenäherten Beweiswert des Scanproduktes für ein Gerichtsverfahren

Von der Motivation zur Umsetzung

Rechtsansätze

Zulässigkeit
Aktenführungs- und Dokumentationspflichten in der **Logik der Berufsstände (Fachrecht)**

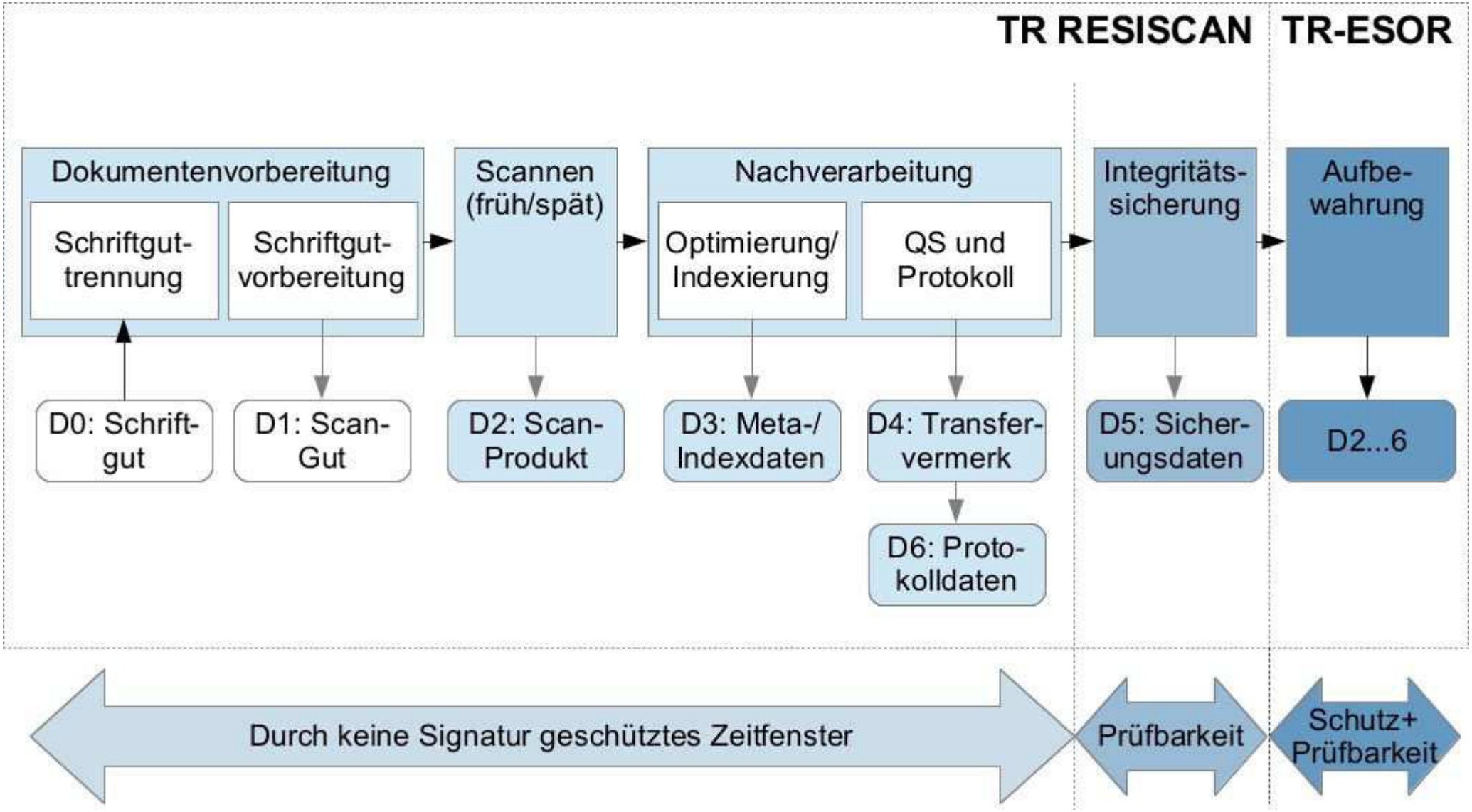
Beweiswert
Gegenstand des Augenscheins **laut Gesetz** (§ 371 Abs. 1 S. 2 ZPO, §7 EGovG-E)

Sicherheitsziele
an das Scan-Produkt

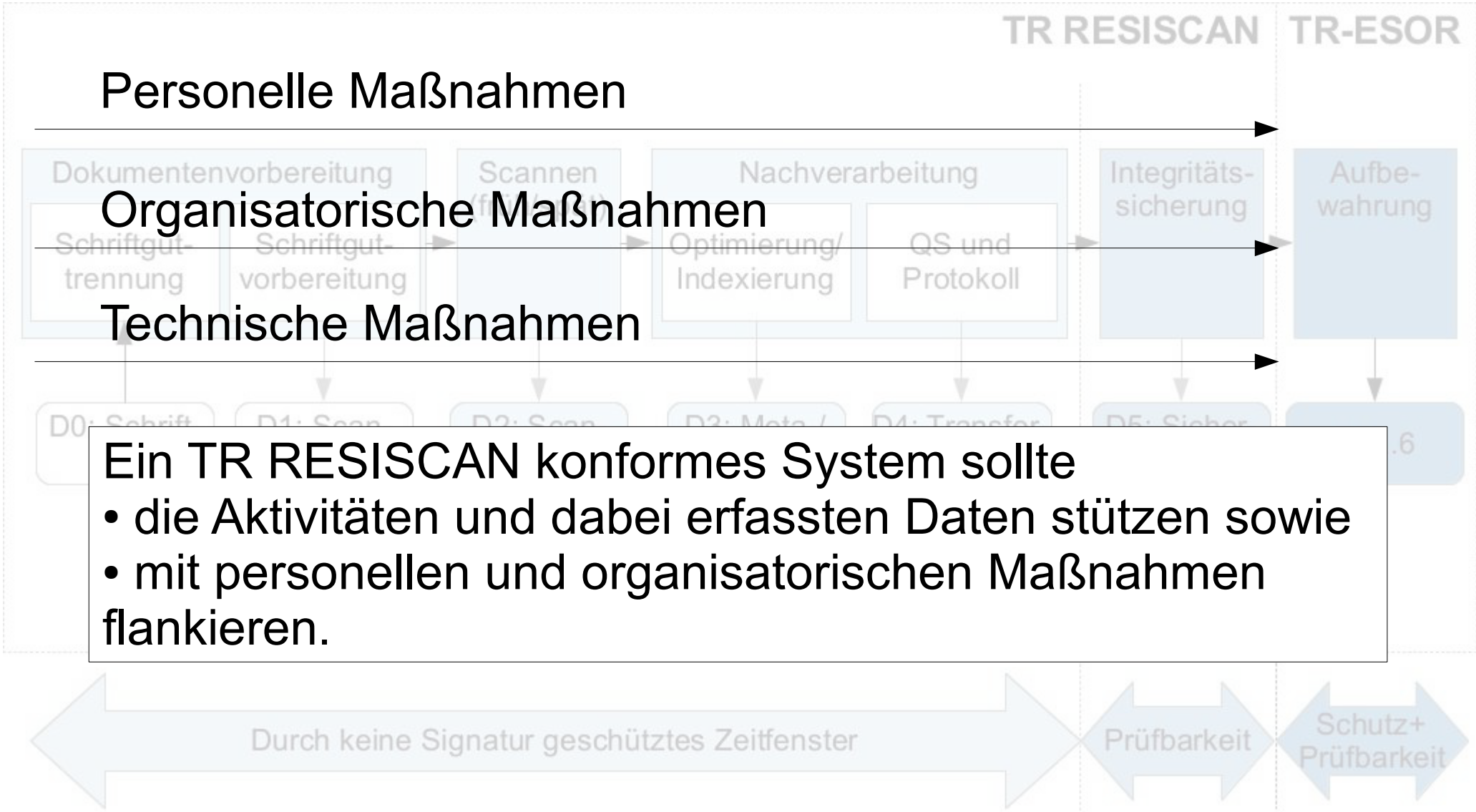
?

Qualifizierte Elektronische Signatur
für Schutz der Integrität des Produktes und der Authentizität des Ausstellers?

Zu sichernde Elemente im Scan-Prozess

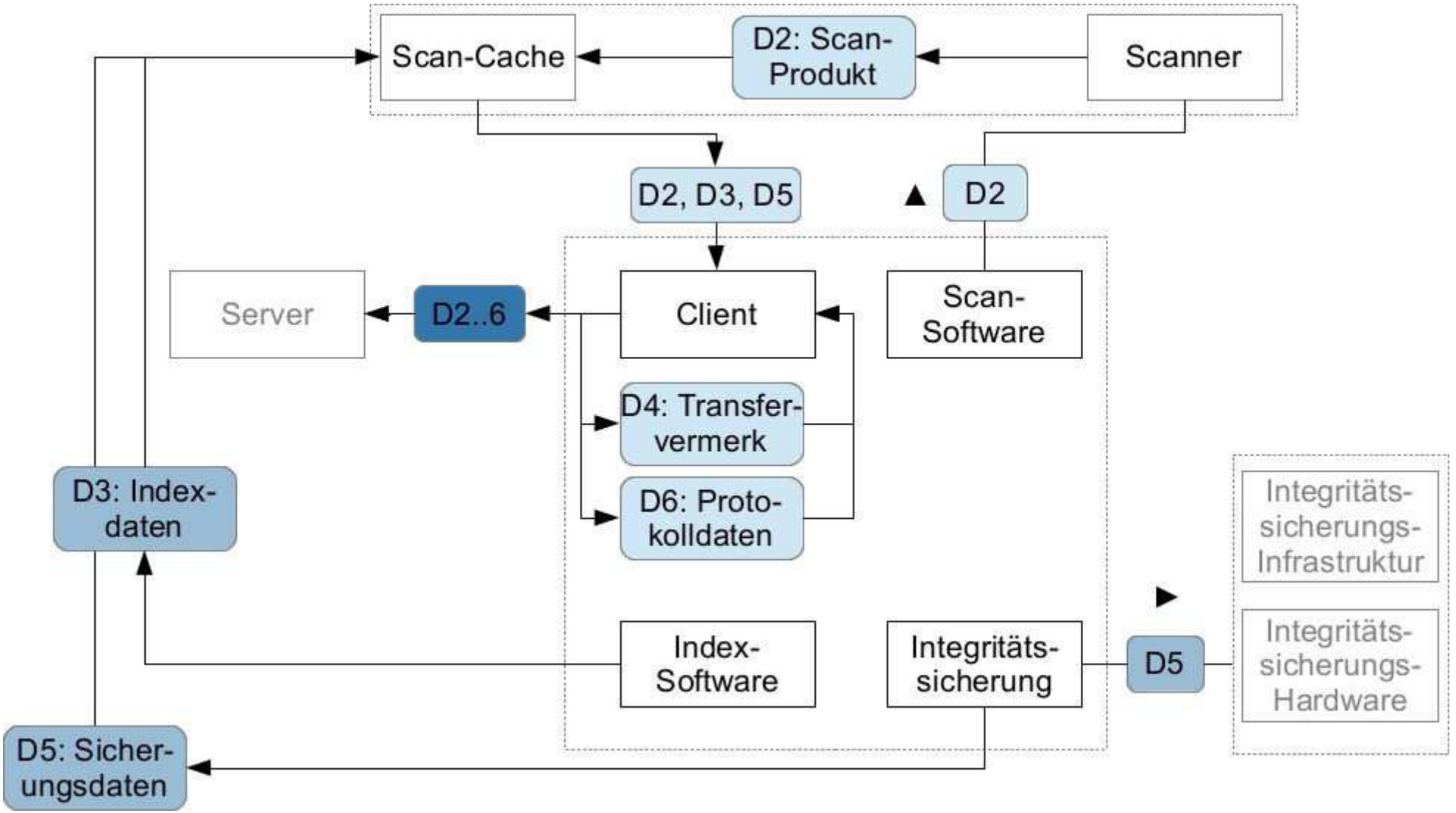


Zu sichernde Elemente im Scan-Prozess

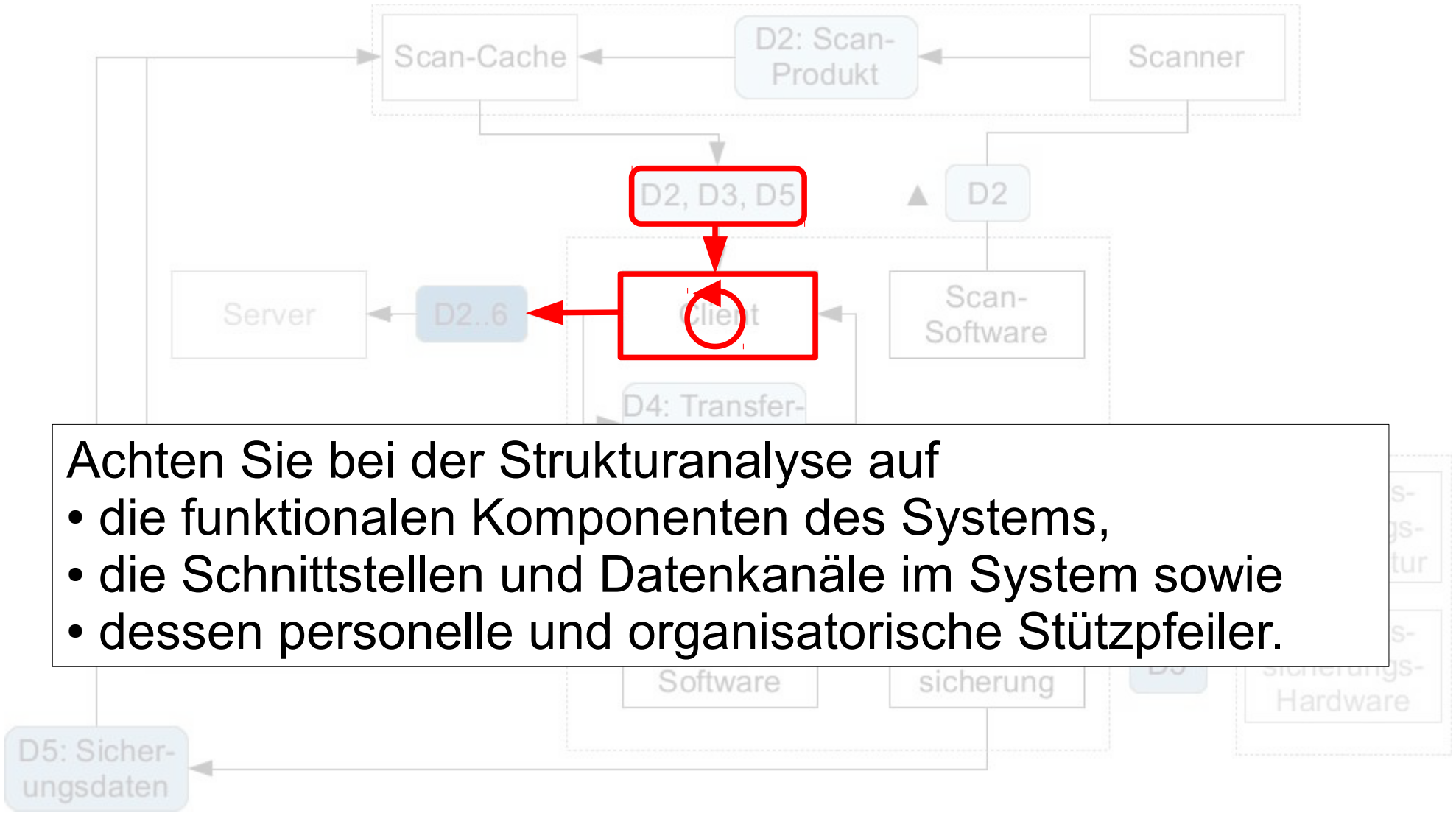


Ein TR RESISCAN konformes System sollte
- die Aktivitäten und dabei erfassten Daten stützen sowie
- mit personellen und organisatorischen Maßnahmen flankieren.

Zu sichernde Elemente im Scan-System



Zu sichernde Elemente im Scan-System



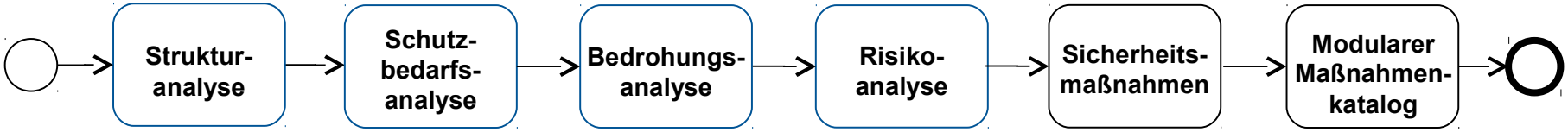
Achten Sie bei der Strukturanalyse auf
- die funktionalen Komponenten des Systems,
- die Schnittstellen und Datenkanäle im System sowie
- dessen personelle und organisatorische Stützpfeiler.

Agenda

- TR RESISCAN: Von der Motivation zur Umsetzung
- Der modulare Anforderungskatalog
- Die Zertifizierung

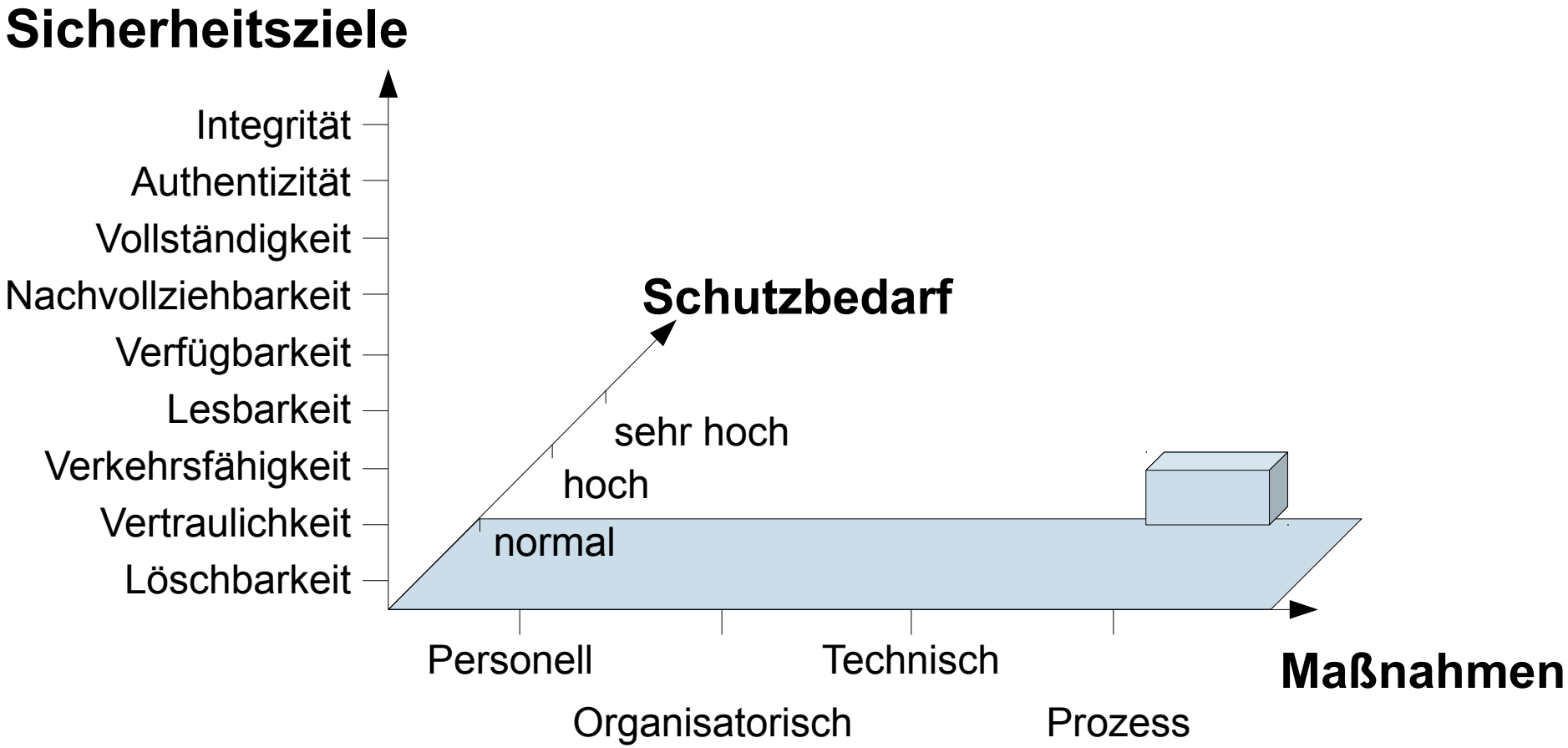
Von der Analyse zu den Anforderungen

- Frage 1: Wie hoch ist mein Schutzbedarf?

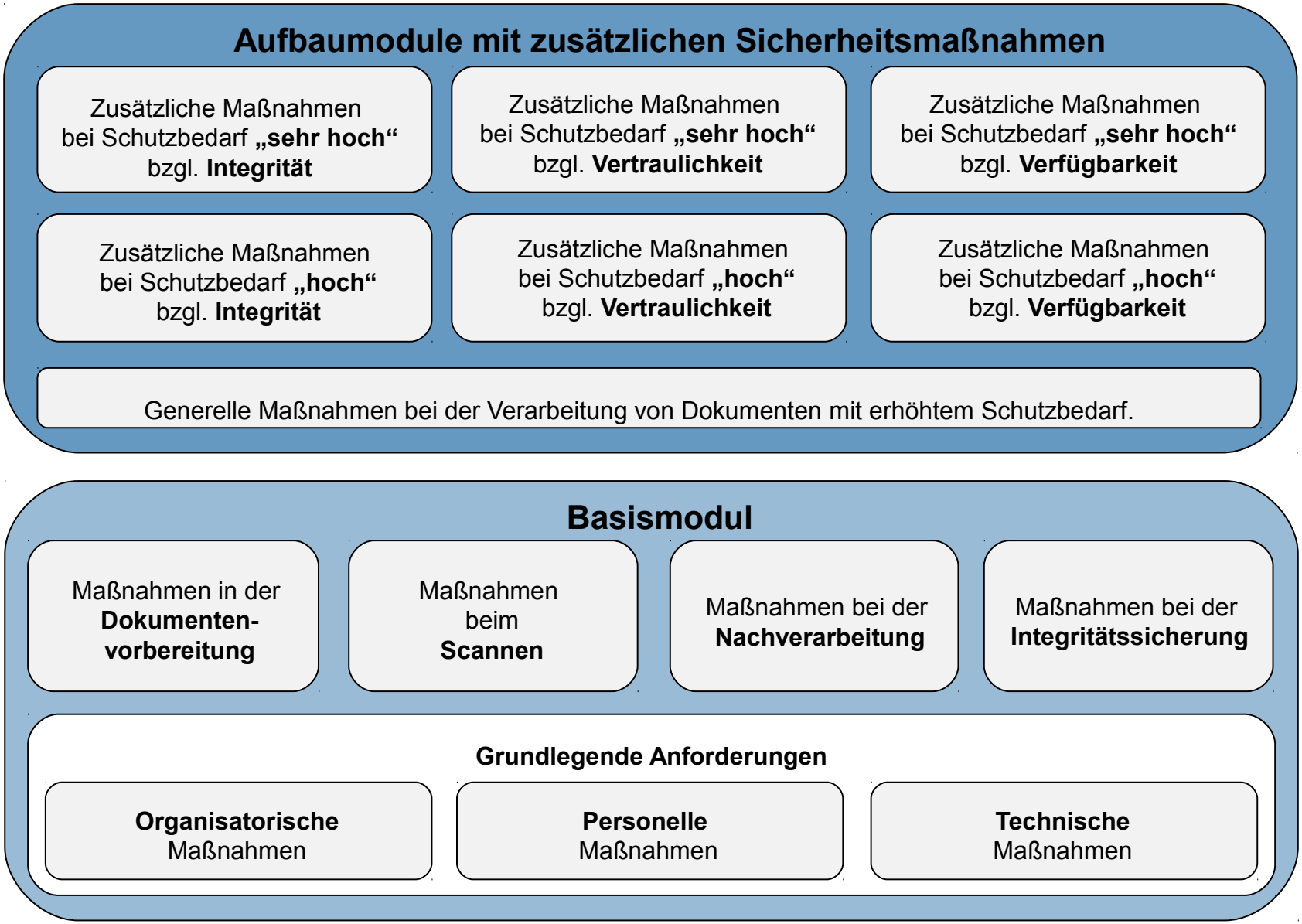


Achtung: eine Schutzbedarfsbewertung ist selten gleich für zwei verschiedene Organisationen.

Frage 2: Wie erreiche ich meinen Schutzbedarf?



Modularer Maßnahmenkatalog



Das Basismodul

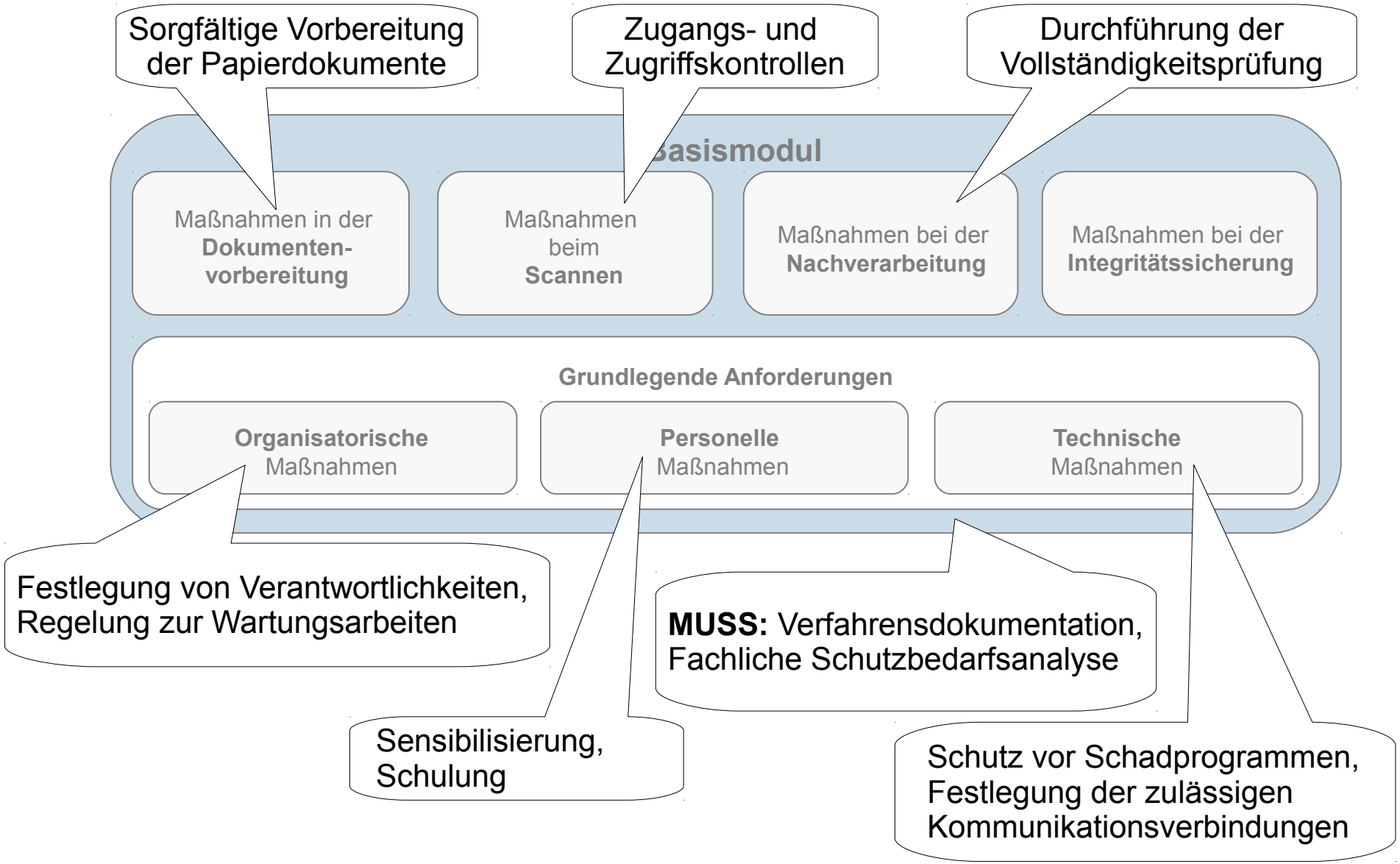
- **Mindeststandard**: die Maßnahmen sind mit typischen personellen und organisatorischen Mitteln und technischen Standardwerkzeugen erreicht!

- Von den 35 Maßnahmen sind
  - 43% organisatorisch-personeller Natur
  - 57% technischer Natur

- Zahlreiche **Empfehlungen** (SOLL).

- Deckt den **Mindestbedarf zur grundsätzlichen Verarbeitung personenbezogener Daten.**

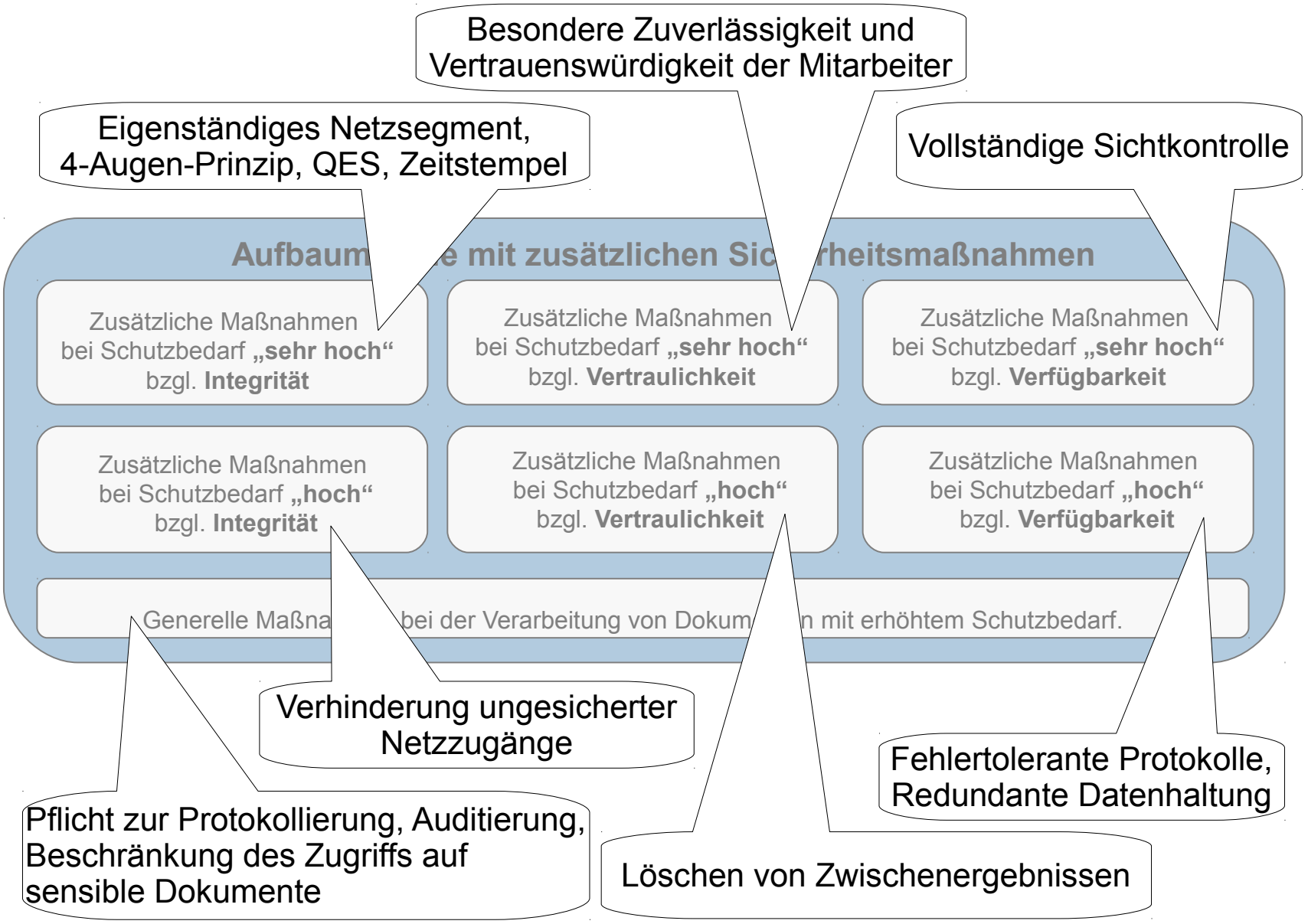
Das Basismodul (für alle) – Beispiele



Das Aufbaumodul

- Module ermöglichen **Kapselung eines Sicherheitszieles**, das nicht zwangsläufig ein anderes eskaliert.
- **Erweitert die Basisanforderungen** um den Schutzbedarf einer Organisation oder eines Berufsstandes (Zulässigkeit).
- Beinhaltet insgesamt 23 Maßnahmen
  - 47% der Maßnahmen sind organisatorisch-personeller Natur
  - 53% der Maßnahmen sind technischer Natur
- Anforderungen des § 3 IX BDSG in Modul „Vertraulichkeit“.

Aufbaumodul – Beispiele



Agenda

- TR RESISCAN: Von der Motivation zur Umsetzung
- Der modulare Anforderungskatalog
- Die Zertifizierung

Bundesamt
für Sicherheit in der
Informationstechnik

Zertifizierung und Konformitätsprüfung im BSI

1) Zertifizierung nach **CC** und ITSEC
(+ ggf. Bestätigung nach SigG)

2) Zertifizierung nach **TR**

3) Zertifizierung nach **IT-Grundschutz**

4) Neu: **Mindeststandard** nach § 8 I BSIG

Bundesamt
für Sicherheit in der
Informationstechnik

Zertifizierungsverfahren (TR)

Verfahrensablauf

- Konformitätsprüfung durch zertifizierte IT-Grundschutz Auditoren
- Zertifikatsgültigkeit: 3 Jahre
- Kosten
  - Zertifizierungsgebühren BSI (Erst-Zertifizierung): 2600,- € pauschal
  - + Kosten der Konformitätsprüfung
- Alternativen zur Zertifizierung durch BSI
  - Auditor-Testat
  - Konformitätserklärung

Weitere Informationen, Antragsformular, … unter: **www.bsi.bund.de/zertifizierungtr**

Zusammenfassung

- Basismodul ist **Mindeststandard**, der mit Standardmitteln erreicht werden kann.
- Basismodul für die grundsätzliche Verarbeitung personenbezogener Daten geeignet.

- **Erweiterungsmodule sind einzeln integrierbar.**
- Unterscheidung von **Authentizität (des Ausstellers)** und **Integrität (des Scanprodukts)**.
- Unterschiedliche Sicherungsmittel notwendig und sinnvoll, je nach Schutzbedarf (kann, soll, muss).
- **QES erst ab Schutzbedarf „Sehr Hoch“ Pflicht**.

Kontakt

Bundesamt für Sicherheit in der Informationstechnik (BSI)

Dietmar Bremser
Godesberger Allee 185-189
53175 Bonn

Tel: +49 (0)22899-9582-6056
Fax: +49 (0)22899-10-9582-6056

dietmar.bremser@bsi.bund.de
www.bsi.bund.de
www.bsi-fuer-buerger.de