Bundesamt
für Sicherheit in der
Informationstechnik

WIRTSCHAFTS
UNIVERSITÄT
WIEN VIENNA
UNIVERSITY OF
ECONOMICS
AND BUSINESS

Einführung in den BSI PIA-Leitfaden
-
Methodische Interpretation und Umsetzung des PIA Frameworks für RFID

Harald Kelter & Marie Oetzel

25. November 2011

Agenda

- **Ausgangspunkt und Entwicklung des BSI PIA-Leitfaden**
- Einsatz des BSI PIA-Leitfaden im Unternehmen
- Die BSI PIA-Methodik und ihre Anwendung anhand eines Beispiels
- Schlussfolgerungen und PIA Tool

Ausgangspunkt

- EUC-Recommendation vom 12.05.2009 fordert PIA für RFID-Einsatz
  - Hinweis auf die Umsetzung von Privacy-by-Design.
- Anerkennung des PIA Frameworks für RFID durch A29WP wurde am 11.02.2011 erklärt.
  - Generisches Rahmenwerk; prozessuale Umsetzung offen.
- BSI Technische Richtlinie 03126
  - Konzentriert sich auf den sicheren Einsatz von RFID.
  - Beinhaltet bereits Betrachtungen zum technologischen Datenschutz und entsprechende Empfehlungen.
  - Diese Datenschutzbetrachtungen sollen systematisiert und vervollständigt werden.

Ziele bei der Entwicklung des BSI PIA-Leitfaden

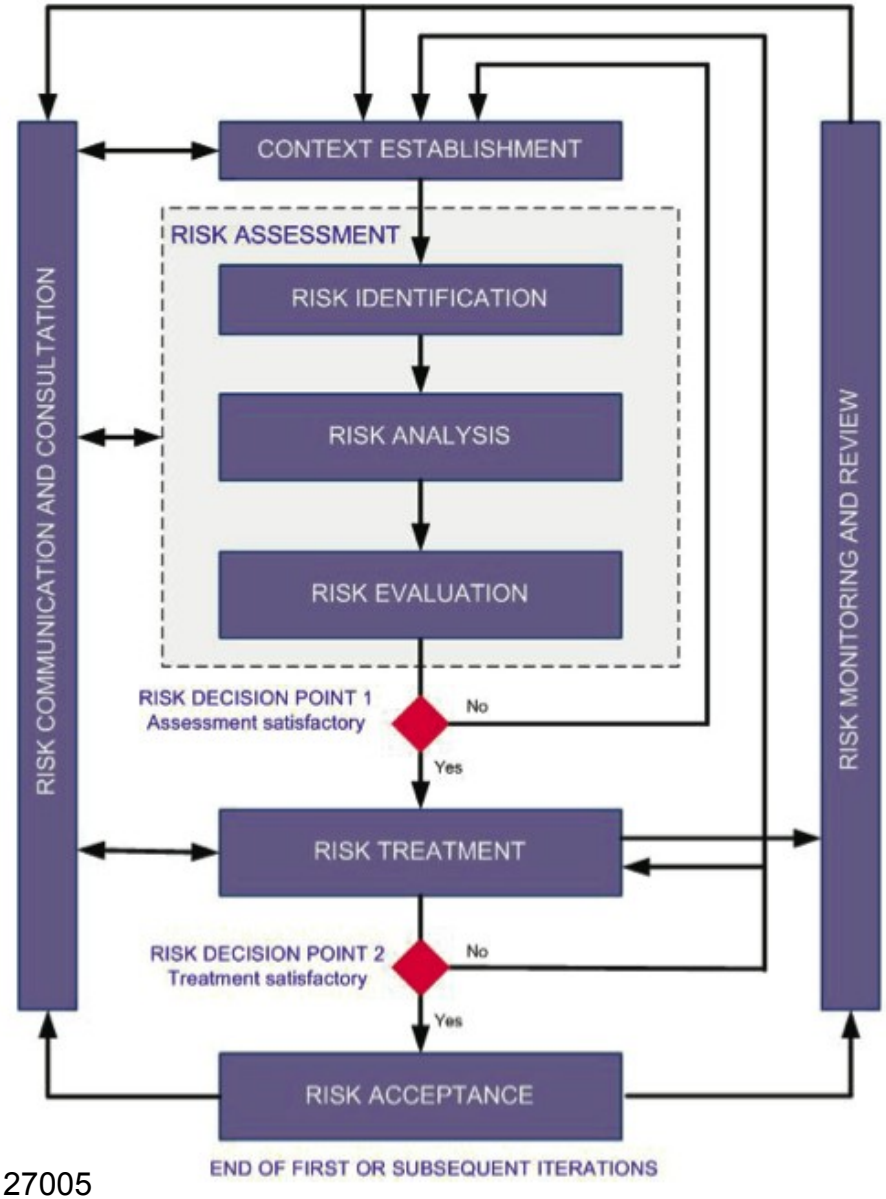
- Entwicklung einer PIA-Methodik, die eine **Schritt-für-Schritt** Umsetzung ermöglicht!
- Ermöglichen einer späteren **Integration** mit bereits existierenden Prozessen um so die Akzeptanz zu fördern!

- Konsequenz: Aufbauen auf standardisierten Risikomanagement Verfahren und existierenden PIAs:
  - ISO 27005: Information Security Risk Management
  - NIST SP 800-30: Risk Management Guide for Information Technology Systems
  - ENISA: Emerging and Future Risks Framework
  - UK PIA Handbook

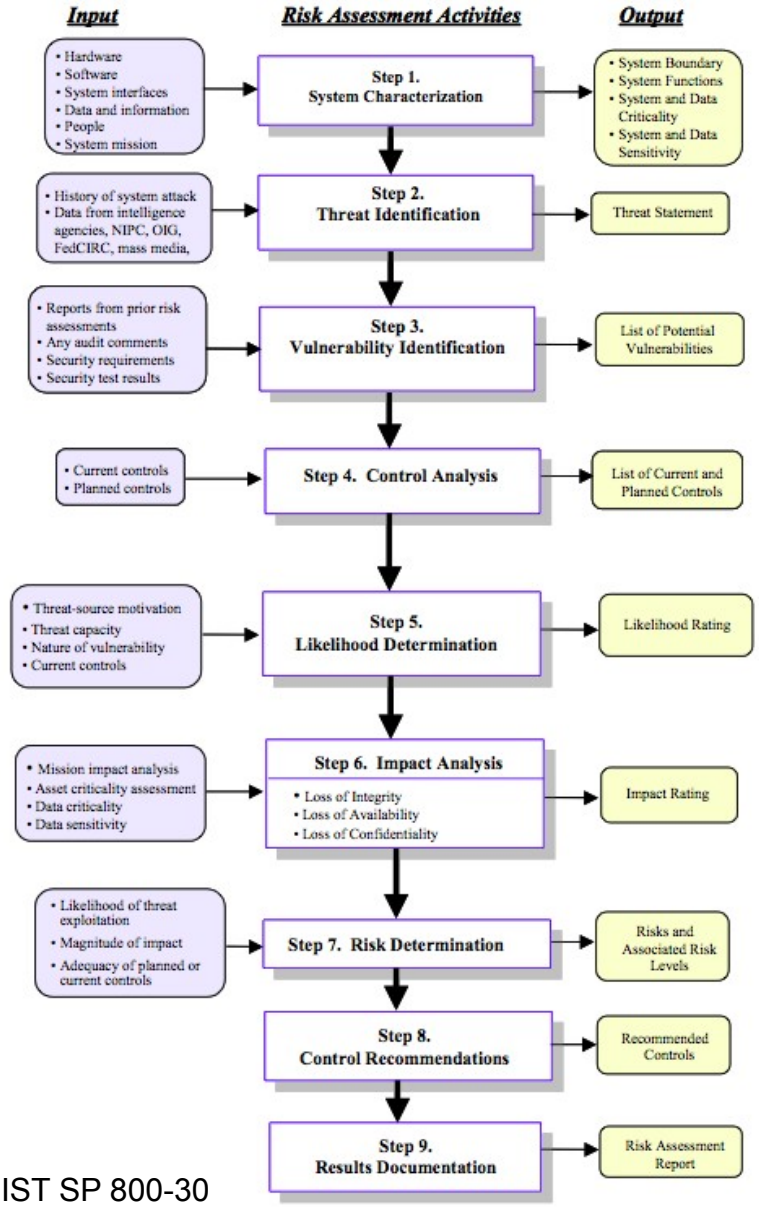
Bundesamt
für Sicherheit in der
Informationstechnik

Standards für Sicherheitsrisikomanagement

WIRTSCHAFTS
UNIVERSITÄT
WIEN VIENNA
UNIVERSITY OF
ECONOMICS
AND BUSINESS



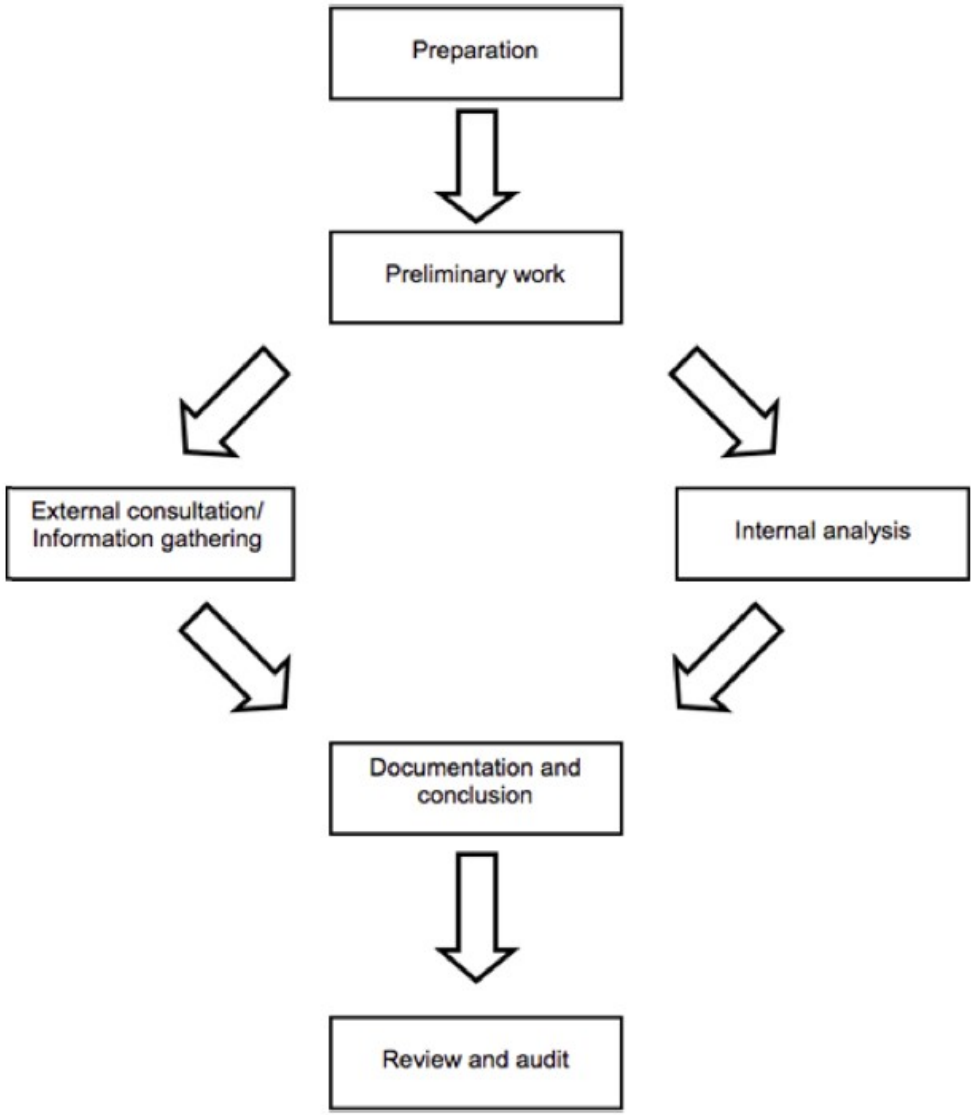
ISO 27005



NIST SP 800-30

Generisches UK PIA

Full Scale and Small Scale PIA Process Map



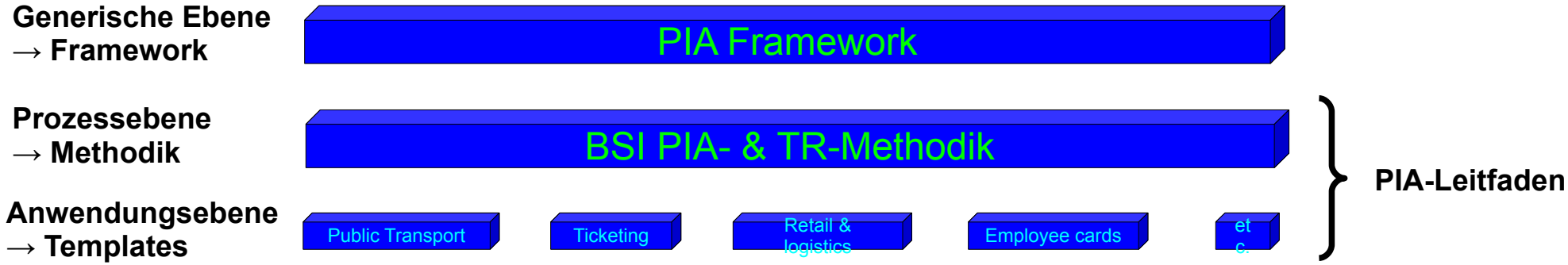
Weitere Ziele bei der Entwicklung des BSI PIA-Leitfaden

- Möglichst vollständige Betrachtung relevanter Datenschutzanforderungen
  - Europäische Datenschutzrichtlinie als Basis.
  - Anknüpfen an die Vorgehensweise des PIA Frameworks.
  - Detaillierung und Konkretisierung der Datenschutzziele des PIA Frameworks zur Förderung der Anwendbarkeit.

- Verknüpfung mit der BSI TR 03126 → Leitfaden für den **sicheren und datenschutzgerechten** RFID-Einsatz

Der BSI PIA-Leitfaden und das PIA Framework: Komplementäre Ansätze

- PIA-Framework legt die Rahmenbedingungen für die Betrachtung fest
- BSI PIA-Methodik beschreibt die schrittweise Vorgehensweise
- „Templates“ enthalten die Festlegungen für spezielle Anwendungsgebiete



Agenda

- Ausgangspunkt und Entwicklung des BSI PIA-Leitfaden
- **Einsatz des BSI PIA-Leitfaden im Unternehmen**
- Die BSI PIA-Methodik und ihre Anwendung anhand eines Beispiels
- Schlussfolgerungen und PIA Tool

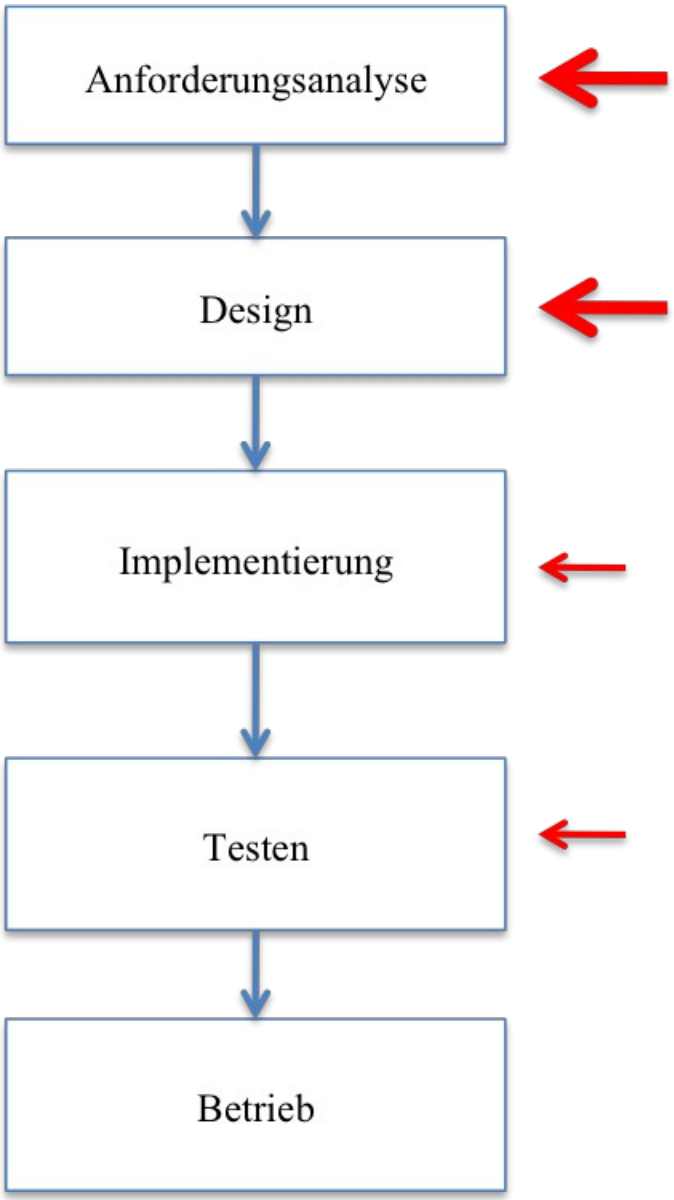
Verantwortlichkeit

- Wer ist verantwortlich für die Durchführung eines PIA?
  - Das PIA Framework sieht den jeweiligen Betreiber der RFID Anwendung in der Verantwortung.
  - Beim Betrieb von schlüsselfertigen RFID-Anwendungen durch mittlere und kleine Betriebe
    - sollte der Hersteller der Anwendung ein PIA bereits während der Entwicklung durchführen,
    - und den Betreiber unterstützen ein einsatz-spezifisches PIA vor Ort durchzuführen.
- Bei RFID-Anwendungen, die massenhaft in einem identischen Einsatzszenario verwendet werden (Bsp: Wegfahrsperre im Auto), reicht die Durchführung eines PIA.

Umfang eines PIA

- Small- versus full-scale PIA
  - Beide Varianten erfordern das vollständige Durchlaufen der BSI PIA-Methodik.
  - Small-scale PIA ist weniger formalisiert und erfordert weniger Aufwand von Zeit und Personal.
- Es besteht keine Verbindung zu den möglicherweise zu identifizierenden Risiken, d.h.
  - ein small-scale PIA kann zur Aufdeckung massiver Datenschutzrisiken führen,
  - und ein full-scale PIA kann zu dem Schluss gelangen, dass ein datenschutzfreundliches Anwendungs-Design vorliegt und keine oder nur geringe Datenschutzrisiken bestehen.

Integration in bestehende Prozesse und Einbindung der Stakeholder



- Wann sollte das PIA durchgeführt werden?
  - Während der Anforderungsanalyse und in der fachlichen und technischen Designphase.
  - Im Sinne des Privacy-by-Design.
  - Nicht einmalig, sondern iterativ und wiederkehrend!
- Einbindung der Stakeholder
  - So früh wie möglich.
  - Einbeziehung der Datenschutzpräferenzen der Stakeholder in die Formulierung der Schutzziele.

Organisation und Aufwand

- Integration in bestehende Risikomanagement Prozesse
  - Der Aufwand eines PIA ist dann gleichzusetzen mit einem bestehenden Sicherheitsrisikomanagement.
- Organisatorische Umsetzung
  - Dedizierte Benennung einer Person/eines Teams und Zuweisung von Personen, die fachlich und technisch versiert sind.
    - Small-scale PIA: Beauftragung des Datenschutzbeauftragten
    - Full-scale PIA: Benennung eines Teams aus mindestens 3 Personen (Techniker, Fachexperte, Jurist)

Vorteile der Umsetzung des BSI PIA

- Qualitätskontrolle und garantierte Vollständigkeit durch die Systematik der BSI PIA-Methodik
- Frühzeitige Erkennung von Datenschutzrisiken
  - Ermöglicht kontrolliertes Risikomanagement.
- Ermöglicht proaktiven Datenschutz und verhindert das nachträgliche Anbauen von Techniken und Methoden, die Datenschutzkonformität sicherstellen.
  - Wirkt sich positiv auf die Gesamtfunktionalität, Performanz und Benutzbarkeit der Anwendung aus.
- Erleichtert die Umsetzung von datenschutzkonformen Prozessen innerhalb des Unternehmens sowie in der Kommunikation nach außen.

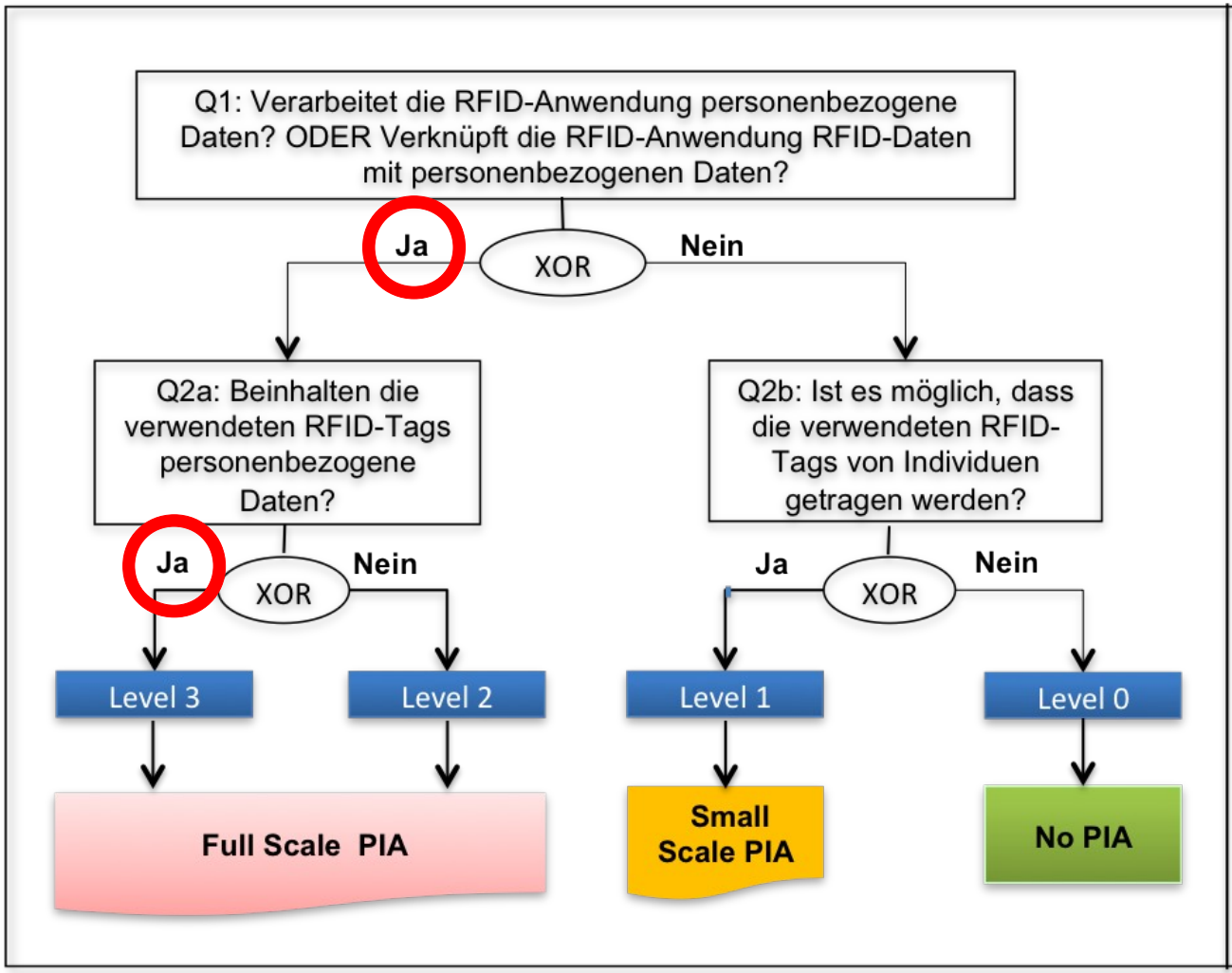
Agenda

- Ausgangspunkt und Entwicklung des BSI PIA-Leitfaden
- Einsatz des BSI PIA-Leitfaden im Unternehmen
- **Die BSI PIA-Methodik und ihre Anwendung anhand eines Beispiels**
- Schlussfolgerungen und PIA Tool

Beispielszenario: RFID-basierte Kundenkarte im Handel

- RFID-Tag der Kundenkarte beinhaltet eine ID, die mit den Kundendaten verknüpft ist.
- Der Kunde kann sich mit der Karte an Info- und Werbeterminals identifizieren.
- Die Karte wird an der Kasse ausgelesen und die Bondaten werden im Kundenprofil gespeichert.

Initiale Analyse: Ist ein PIA notwendig?



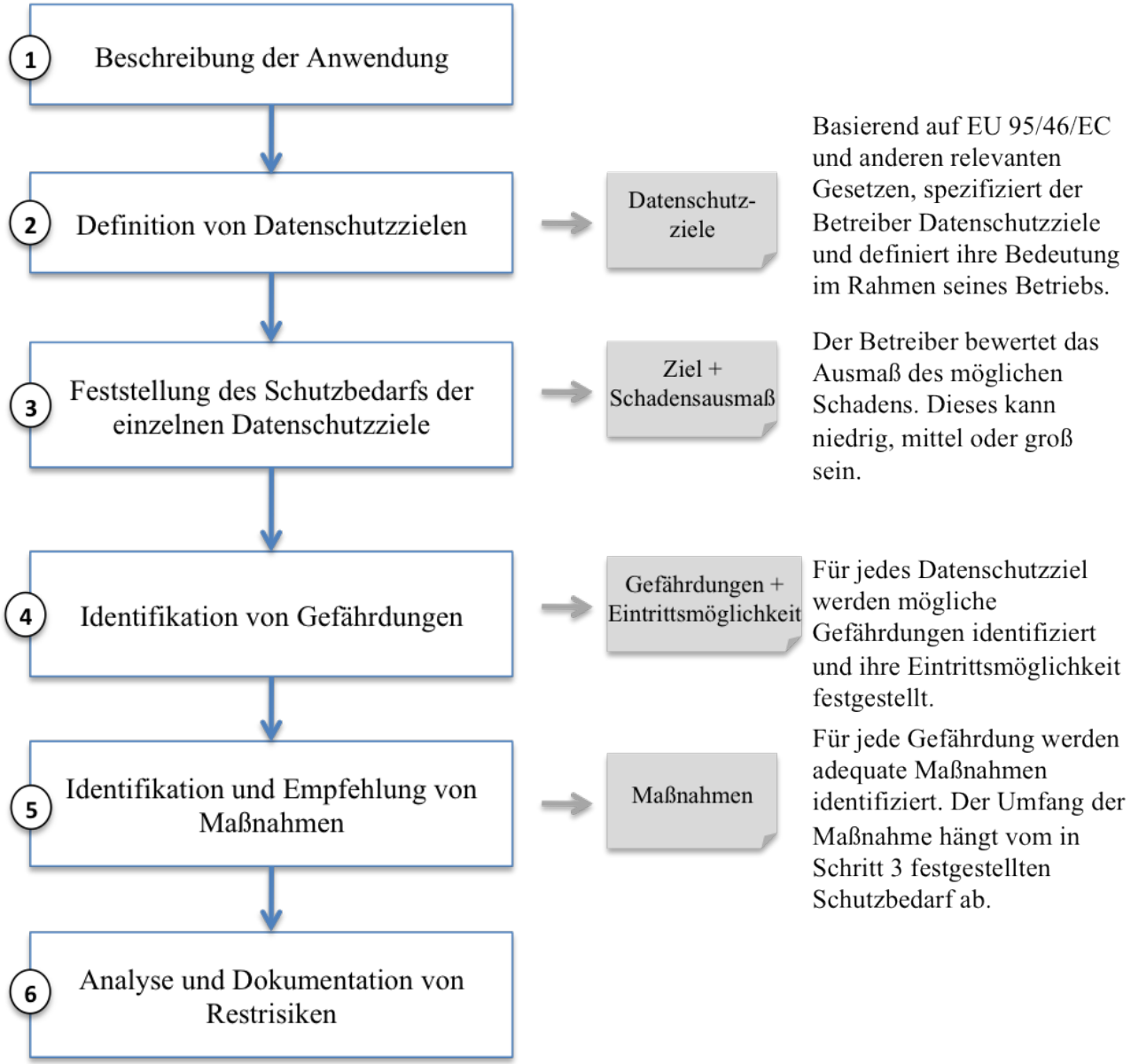
Notiz 1: "Personenbezogene Daten" werden von der Richtlinie 95/46/EC (Artikel 2) wie folgt definiert "alle Informationen über eine bestimmte oder bestimmbare natürliche Person ("betroffene Person"); als bestimmbar wird eine Person angesehen, die direkt oder indirekt identifiziert werden kann, insbesondere durch Zuordnung zu einen Kennummer oder zu einem oder mehreren spezifischen Elementen, die Ausdruck ihrer physischen, physiologischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität sind;"

Notiz 2: Eine "RFID-Anwendung" ist ein System, dass mit Hilfe von Tags und Lesegeräten Daten verarbeitet und von einem Backend-System sowie einer vernetzten Kommunikationsinfrastruktur unterstützt wird und damit auch Teil dieser ist.

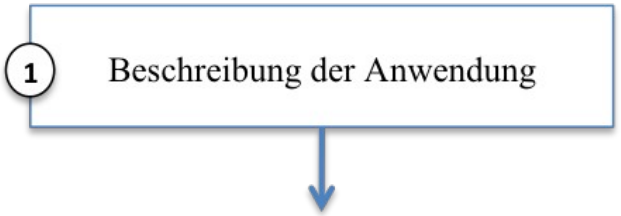
Bundesamt
für Sicherheit in der
Informationstechnik

BSI PIA-Methodik – Ein Überblick

WIRTSCHAFTS
UNIVERSITÄT
WIEN VIENNA
UNIVERSITY OF
ECONOMICS
AND BUSINESS

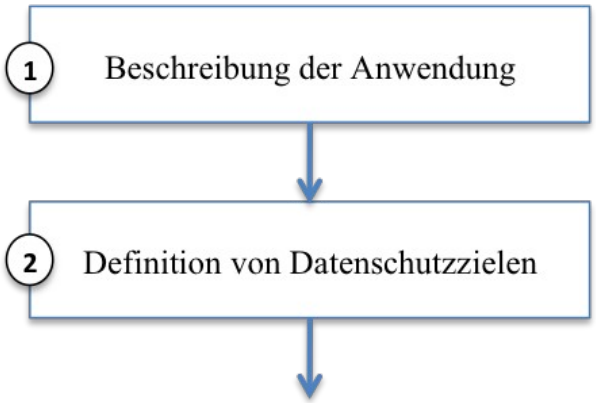


Schritt 1: Beschreibung der Anwendung



- Umfang und Detailgrad der Beschreibung haben Auswirkung auf die erfolgreiche Durchführung des PIA.
  - Fehlende Informationen können dazu führen, dass Risiken nicht erkannt werden.
- Beschreibung umfasst u.a.:
  - Anwendungs- und Systemkomponenten
  - Rollen
  - Generische Geschäftsprozesse
  - Detaillierte Anwendungsfälle
  - Datenflussdiagramme
  - Verarbeitete Datenkategorien

Schritt 2: Definition von Datenschutzzielen



- Betreiber definiert Datenschutzziele …
  - basierend auf der Direktive 95/46/EC und anderen relevanten Gesetzen und Regulationen
- … und erläutert ihre Bedeutung im Rahmen seines Betriebs.
- Der PIA-Leitfaden bietet zur Orientierung
  - 8 übergeordnete Datenschutzziele
  - 16 konkretisierte Datenschutzziele
  - abgeleitet aus der Direktive 95/46/EC
- Betreiber kann diese wiederverwenden und erweitern.

Zusammenhang zwischen übergeordneten und konkretisierten Datenschutzzielen

	Übergeordnetes Datenschutzziel
P1	Sicherstellung der Qualität der Daten
P2	Zulässigkeit der Verarbeitung von personenbezogenen Daten
P3	Zulässigkeit der Verarbeitung von sensitiven personenbezogenen Daten
P4	Information der betroffenen Person
P5	Wahrung des Auskunftsrecht der betroffenen Person
P6	Wahrung des Widerspruchsrecht der betroffenen Person
P7	Sicherstellung der Vertraulichkeit und Sicherheit der Verarbeitung
P8	Wahrnehmung der Meldepflicht

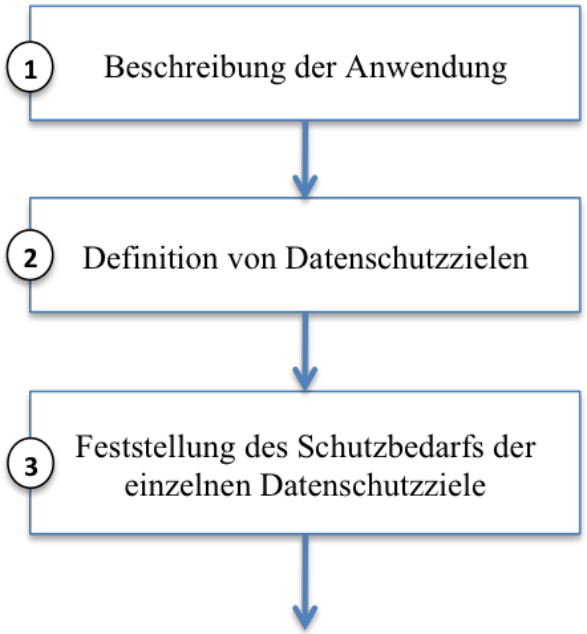
	Konkretisiertes Datenschutzziel
P1.1	Sicherstellung einer fairen und gesetzmäßigen Verarbeitung durch Transparenz
P1.2	Festlegung von Zweckbestimmung und -begrenzung
P1.3	Sicherstellung von Datenvermeidung und -minimierung
P1.4	Sicherstellung der Qualität der Daten
P1.5	Sicherstellung der begrenzten Datenspeicherung

Beispielszenario Kundenkarte: Schritt 1 - Datenschutzziele

	Konkretisiertes Datenschutzziel
P1.1	Sicherstellung einer fairen und gesetzmäßigen Verarbeitung durch Transparenz
P1.2	Festlegung von Zweckbestimmung und -begrenzung
P1.3	Sicherstellung von Datenvermeidung und -minimierung
P1.4	Sicherstellung der Qualität der Daten
P1.5	Sicherstellung der begrenzten Datenspeicherung

- Dem Kunden muss genau erklärt werden, wie die Kundenkarte funktioniert.
  - inkl. Erläuterung der RFID-Technologie
  - z.B. Webseite, Flyer
- Die Zweckbestimmung der im Rahmen der Kundenkarte erhobenen Daten muss festgeschrieben werden.
  - intern und extern wichtig!
  - z.B. Loyalitätsprogramm, aber nicht Produktentwicklung

Schritt 3: Feststellung des Schutzbedarfs



- Betreiber bestimmt das Schadensausmaß, das eintreten kann, wenn Datenschutz-anforderungen nicht eingehalten werden.
- Ziel ist die Feststellung des Schutzbedarfs für jedes der in Schritt 2 definierten Datenschutzziele.
- Der Schutzbedarf kann sein:
  - Gering (1): Die Auswirkungen eines Verlusts oder Schadens sind limitiert und kalkulierbar.
  - Mittel (2): Die Auswirkungen eines Verlusts oder Schadens sind erheblich.
  - Groß (3): Die Auswirkungen eines Schadens oder Verlusts sind verheerend.

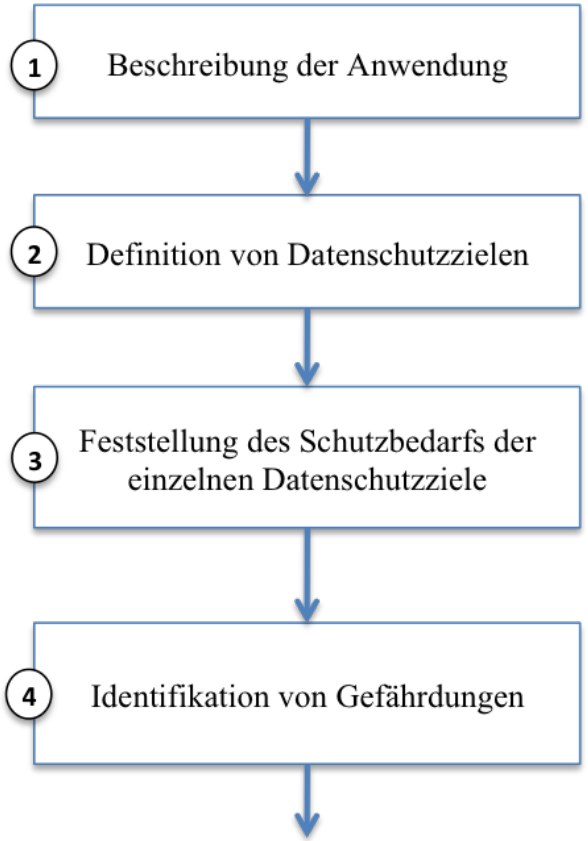
Beispielszenario Kundenkarte: Schritt 3 - Schutzbedarf

- Betrachtung von zwei Perspektiven notwendig
  - Betreiber
    - Auswirkungen auf Reputation und Markenwert
    - Finanzielle Verluste
  - Kunde
    - Auswirkungen auf Reputation
    - Finanzielles Wohlergehen
    - Persönliche Freiheit
- Einzelne Bewertung der Perspektiven vornehmen.
- Gesamtbewertung ergibt sich dann nach dem Maximum-Prinzip.

	Datenschutzziel
P1.2	Festlegung von Zweck-bestimmung und -begrenzung

- Was wäre wenn ...?
  - z. B. Daten des Kundenprofils gelangen in Hände Dritter
- Betreiber: 2, 1
- Kunde: 2, 2, 1
- Gesamt: 2

Schritt 4: Identifikation von Gefährdungen



- Betreiber identifiziert Gefährdungen für jedes Datenschutzziel.
  - Gegebenheiten, die die Sicherstellung des Ziels gefährden.
- Für jede Gefährdung wird die Eintrittsmöglichkeit bestimmt.
  - Ja oder nein.
- Der PIA-Leitfaden bietet zur Orientierung
  - 60 Gefährdungen zugeordnet zu den 16 Datenschutzzielen
- Betreiber kann diese wiederverwenden und erweitern.

Beispielszenario Kundenkarte: Schritt 4 - Gefährdungen

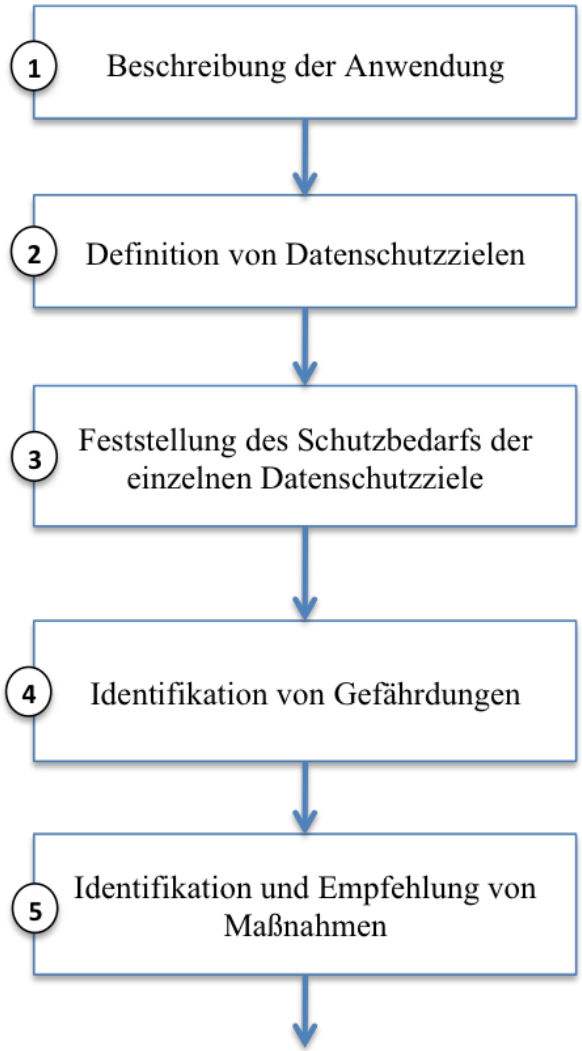
	Datenschutzziel
P1.2	Festlegung von Zweck-bestimmung und -begrenzung

Kann die Gefährdung eintreten?

Ja.

	Gefährdung
...	
T1.6	Die Informationen, die ein RFID-Emblem begleiten, beschreiben nicht alle Bereiche und Zwecke, für die RFID im Betrieb eingesetzt wird.
...	
T1.15	Der Zweck der Datenerhebung und -verarbeitung ist nicht festgelegt und ist für Kunden und Mitarbeitern somit nicht transparent.
...	
T1.17	Daten, die für einen festgelegten Zweck gespeichert und verarbeitet werden, sind nicht entsprechend markiert; z.B. mit entsprechenden Zugriffsrechten.
...	

Schritt 5: Identifikation und Empfehlung von Maßnahmen



- Betreiber identifiziert Maßnahmen, die den Gefährdungen adäquat entgegenwirken.
- Maßnahmen sind in drei Ausprägungen definiert: gering (1), mittel (2), groß (3).
- Maßnahmen sollten so gewählt werden, dass ihre Ausprägung dem in Schritt 3 festgestellten Schutzbedarf entsprechen.
- Der PIA-Leitfaden bietet zur Orientierung
  - 27 Maßnahmen zugeordnet zu den 60 Gefährdungen und 16 Datenschutzzielen
- Betreiber kann diese wiederverwenden und erweitern.

Beispielszenario Kundenkarte: Schritt 5 - Maßnahmen

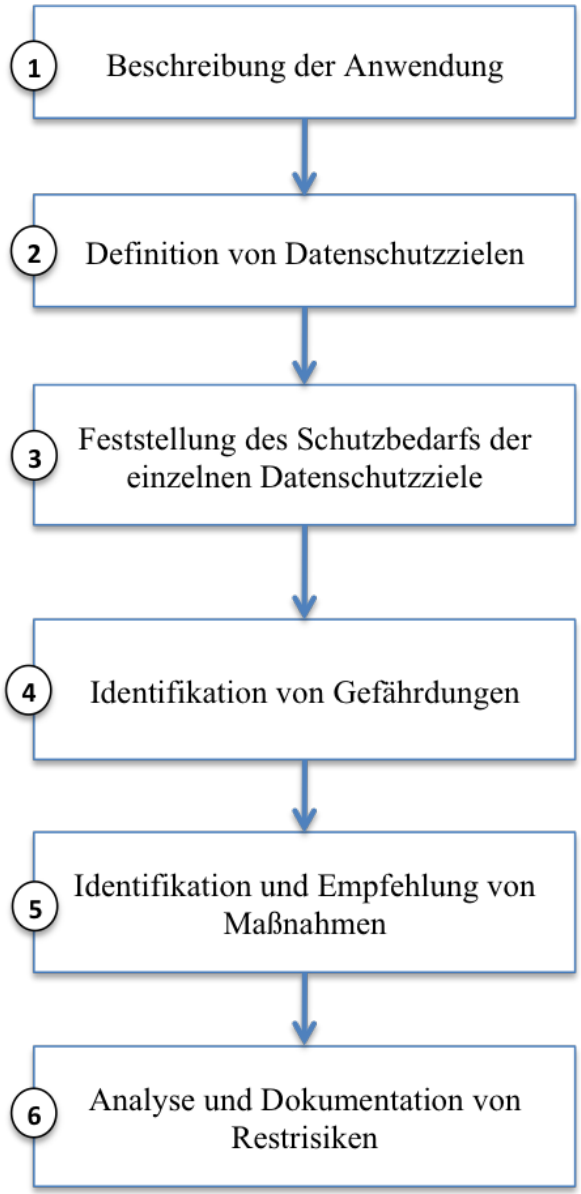
	Gefährdung
...	
T1.17	Daten, die für einen festgelegten Zweck gespeichert und verarbeitet werden, sind nicht entspr… markiert; z.B. mit entspre… Zugriffsrechten.
...	

	Datenschutzziel	
P1.2	Festlegung von Zweck-bestimmung und -begrenzung	2

C1.8		Sicherstellung der begrenzten Datenverarbeitung
	gering - 1	Mitarbeiter sind über die Zweck-bestimmung der erhobenen Daten informiert und sind aufgefordert diese einzuhalten.
	mittel - 2	Erhobene Daten werden mit Zugriffs-rechten, die der Zweckbestimmung entsprechen, geschützt. Die Zugriffs-rechte können grob-granular spezifiziert werden.
	groß - 3	Erhobene Daten werden mit Zugriffs-rechten, die der Zweckbestimmung entsprechen, geschützt. Die Zugriffs-rechte können fein-granular spezifiziert werden.

Ausprägung muss mit Schutzbedarf übereinstimmen!

Schritt 6: Analyse und Dokumentation von Restrisiken



- Es besteht die Möglichkeit, dass in Schritt 5 identifizierte und empfohlene Maßnahmen erst zu einem späteren Zeitpunkt oder gar nicht umgesetzt werden können.
- Möglicherweise gibt es Gefährdungen, die nach aktuellem technischen Kenntnisstand nicht verhindert werden können.
- Diese Restrisiken müssen dokumentiert werden.

PIA Report

- Dokumentation des Ergebnisses der initialen Analyse
- Dokumentation der 6 Schritte
  - Schritt 1 kann umfassende Dokumentation beinhalten.
  - BSI PIA-Methodik führt zu einer systematischen Gegenüberstellung von Gefährdungen und Maßnahmen.
- Plan für die Maßnahmenumsetzung einfügen
- Unterschrift leisten

- Der Report, der im Rahmen der BSI PIA-Methodik entsteht, stellt eine übersichtliche Grundlage für die Überprüfung durch die Behörden dar.

Agenda

- Ausgangspunkt und Entwicklung des BSI PIA-Leitfaden
- Einsatz des BSI PIA-Leitfaden im Unternehmen
- Die BSI PIA-Methodik und ihre Anwendung anhand eines Beispiels
- **Schlussfolgerungen und PIA Tool**

Schlussfolgerungen

- Die BSI PIA-Methodik ist die erste Schritt-für-Schritt Anleitung für ein PIA überhaupt!
- Der PIA-Leitfaden wurde zusammen mit verschiedenen Firmen erarbeitet.
- Der PIA-Leitfaden wurde mit dem BfDI abgestimmt.
- Die BSI PIA-Methodik ist generalisierbar:
  - Nicht nur für RFID-Anwendungen geeignet.
  - Verwendung in allen IKT Systementwicklungen möglich.

PIA Tool

intelligentPIA

- Der Einsatz des Tools „intelligentPIA“
  - fördert die Akzeptanz und Umsetzung der PIA-Methodik.
  - garantiert die „Accountability“ durch eingebaute Vollständigkeitskontrollen.

Vielen Dank für Ihre Aufmerksamkeit!

harald.kelter@bsi.bund.de & marie.oetzel@wu.ac.at