

Informationssicherheit in der BA

Klaus Pietsch – FTVI & FTRI 2010 – 25.03.2010



IT-Sicherheit



IT-Systemhaus

Aufbau der Bundesagentur für Arbeit (BA)

- ... rechtsfähige bundesunmittelbare Körperschaft des öffentlichen Rechts mit Selbstverwaltung (nach § 367 SGB III – Sozialversicherungsträger)
- ... Zentrale mit **10** Regionaldirektionen, **176** Arbeitsagenturen, **660** Geschäftsstellen und **7** besonderen Dienststellen
- ... mit gut **100.000** Mitarbeiterinnen und Mitarbeitern

Aufgaben der Bundesagentur für Arbeit

1. Integration / Leistungsgewährung Alg I

- Vermittlung von Leistungsbeziehern
- Vermittlung von Arbeitslosigkeit Bedrohten
- Auszahlung der Versicherungsleistung Alg I
- Akquirierung geeigneter Arbeitsplätze

2. Integration / Betreuung und Leistungsgewährung Alg II

- Aktivierende Leistungen
- Vermittlung von Leistungsbeziehern
- Gewährung der Grundsicherung Alg II

3. Markttransparenz und -ordnung

- Statistik/Arbeitsmarkt und Berufsforschung
- Selbstinformationssysteme/Internet-Stellenbörse

4. Auftragsleistung / steuer- oder umlagefinanzierter Dienstleistungen

- Kindergeld
- Insolvenzgeld
- Winterbauförderung
- Arbeitsmarktpolitische Länderprogramme
- Programme des europäischen Sozialfonds

Informationstechnik der BA

■ ■ Hauptsitz:	Nürnberg
■ ■ CIO:	Klaus Vitt
■ ■ IT-Mitarbeiter/innen:	1.800
■ ■ Liegenschaften	1.900
■ ■ Vernetzte PC:	167.000
■ ■ Server:	11.000
■ ■ Druckseiten:	29 Mio. Seiten monatlich

Organisation – BA-Informationstechnik

■ IT-Steuerung

- IT-Strategie
- Anforderungsmanagement
- IT-Sicherheit

IT-Steuerung -
Zentrale der BA

Demand

■ IT-Systemhaus

- IT-Dienstleister für BA und ARGE n
- Systementwicklung
- Betrieb / Infrastruktur
- Betreuungsservice für IT-Anwender/innen und PCs

IT-Systemhaus

Supply

■ RITS

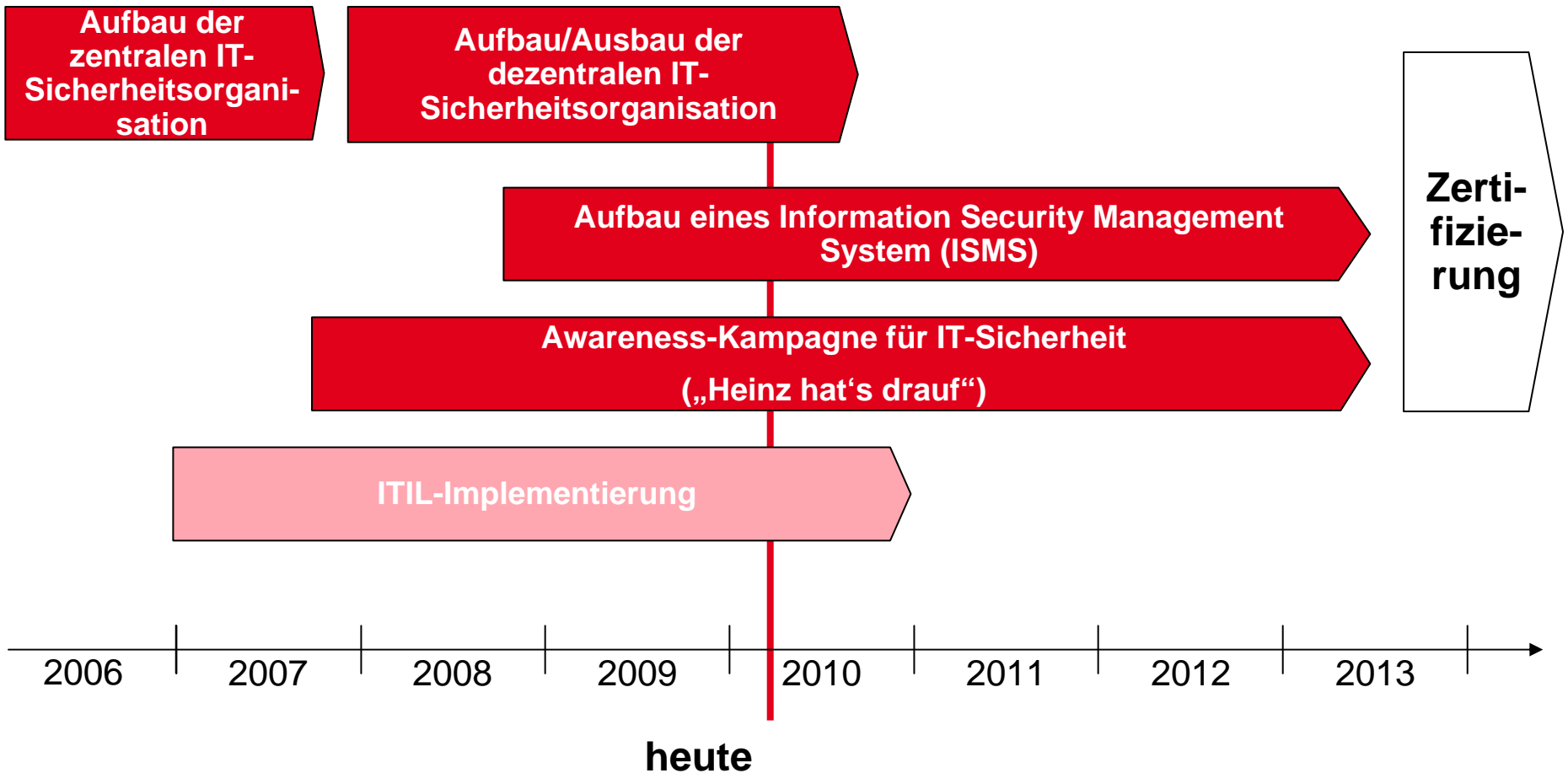
- Fachlich dem IT-Systemhaus unterstellt
- Organisatorisch in dezentrale Serviceeinheiten integriert
(zusammen mit Personal, Finanzen und Infrastruktur)

Regionaler IT-Service

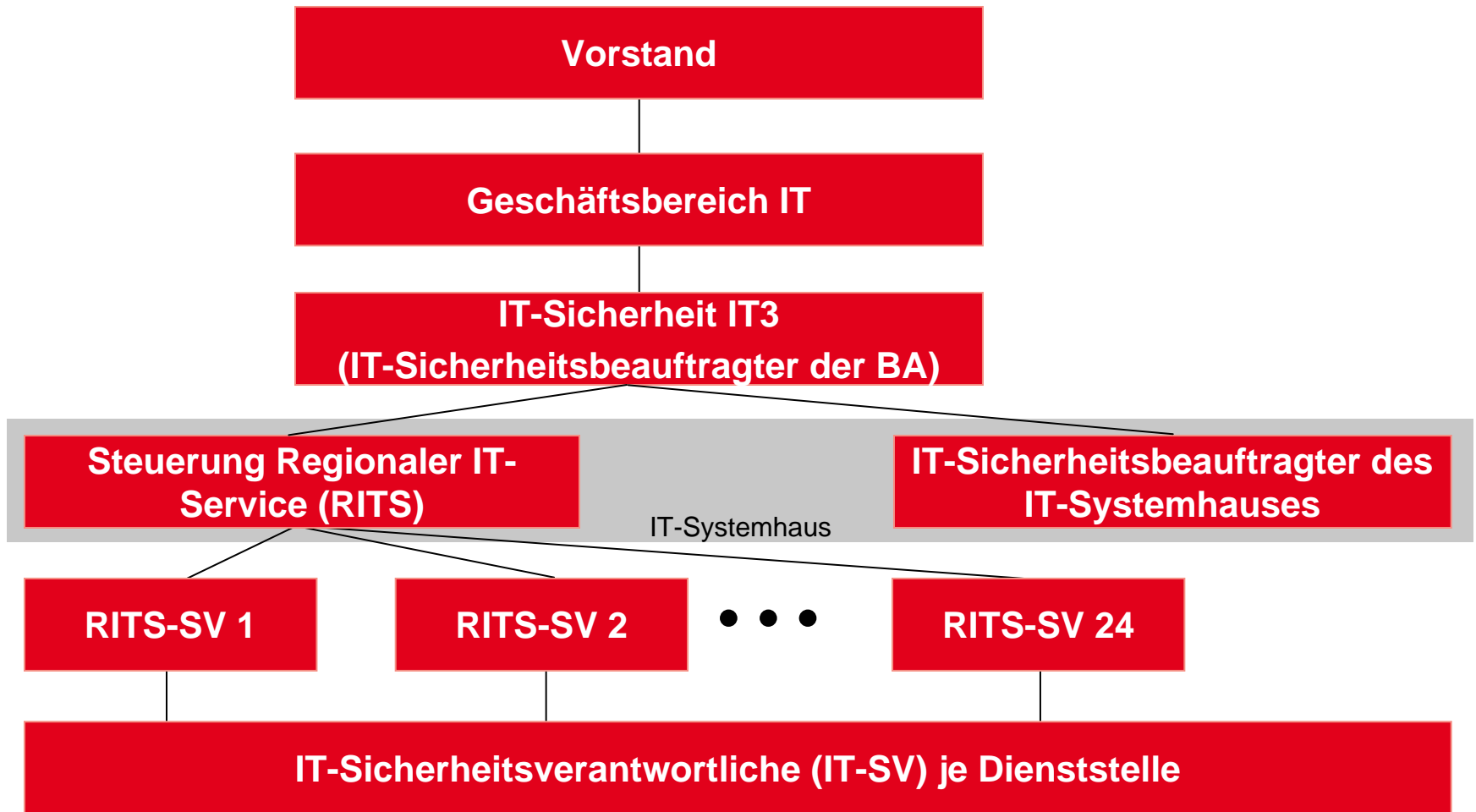
Ziele der Informationssicherheit

- Sicherheitsansprüche des öffentlichen Bereichs erfüllen
- Unterstützen der geschäftspolitischen Ziele im Rahmen der IT-Strategie der BA
- Informationssicherheit in alle IT-Planungs- und Realisierungsprozesse integrieren
 - Software-Design und -Entwicklung
 - IT-Betrieb
 - IT-Nutzung
- ISMS (Informations-Sicherheits-Management-System) bis 2013 zertifizieren zu lassen

Initiativen und Projekte



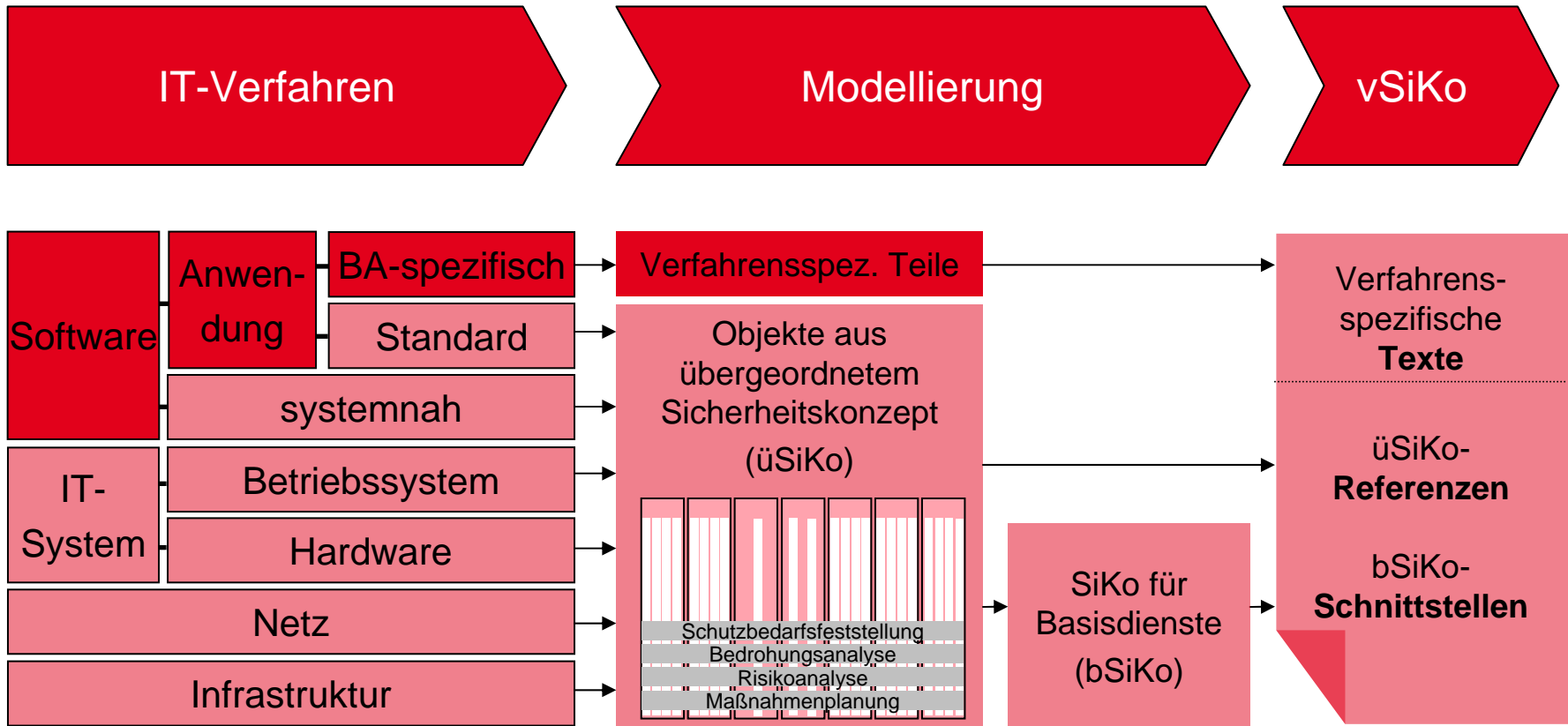
Fachliche Struktur und Kommunikation der IT-Sicherheit



Zertifizierung der IT-Sicherheit gem. ISO 27001 auf Basis von IT-Grundschutz des BSI

- Forderung des Vorstands der BA
- Anforderungen
 - Aktuelle Sicherheitskonzepte für alle IT-Verfahren
 - Aktuelle IT-Sicherheitsrichtlinien/-Regelwerke
 - Aktuelle Prozesse
 - Funktionsfähige IT-Sicherheitsorganisation
 - Ausreichend sensibilisierte Mitarbeiter/Innen
- Umsetzung der Anforderungen erfolgt im Rahmen eines Stufenkonzeptes

Modellierung von IT-Sicherheitskonzepten



Erfolgreiche Optimierungsmaßnahmen

Ziel	Maßnahme	Ergebnis
Erstellungsaufwand verringern	Standardisierung	Verringerung des Aufwandes bei der Modellierung durch Referenzieren auf üSiKo-Objekte (BA-Standards) und Basis-Sicherheitskonzepte (bSiKo) Keine Prüfung des Umsetzungsstandes von Maßnahmen aus üSiKo-Objekten notwendig
	Gruppierung	Anstelle detaillierter Untersuchung von Einzelsystemen werden reale Objekte (HW/SW) sinnvoll gruppiert und damit die Anzahl der verwendeten Objekte reduziert (Clustern) Aktualität: Änderung eines Einzel-Systems erfordert nicht Änderung des vSiKo
	Fokussierung	Fokussierung auf den definierten Sicherungsbereich und Beschreibung der Anforderungen an Schnittstellen (Kapselung) Verringerung der Komplexität
FBT und PV entlasten	Nutzung vorhandener Informationsquellen	Beschleunigung der Abstimm-Prozesse durch Fokussierung auf offene Fragen Zielgruppenspezifische Besprechung fachlicher Details mit FBT Vermeidung von Mehrfachaufwänden zur Dokumentenerstellung
	Nutzung ITIL	Durch ITIL-Prozesse CON, AVA, SEC erfasste technische Dokumentation ist nutzbar für vSiKo und verringert den Erstellungsaufwand um ca. 60% (Restaufwand: Clustern, Kapseln)
Effizienz und Referenzierbarkeit erreichen	Einsatz Template/Leitfaden	Einheitlicher Standard für Erstellung, Vergleichbarkeit / Nachvollziehbarkeit der vSiKo
	Einsatz ISMS-Tool (geplant Q4 2009)	Entlastung der Erstellung durch Aufbau und Verwaltung der Referenzen zwischen üSiKo (Maßnahmen, Objekte, Umsetzungsstand), vSiKo (Objekte, verfahrensspezifische Maßnahmen, Realisierungspläne, ...) und bSiKo Referenzen zwischen vSiKo, üSiKo und bSiKo Nutzung von Checklisten bei der Erstellung von vSiKo
Qualität erhöhen, Wartbarkeit sichern	Einsatz ISMS-Tool (geplant Q4 2009)	Aufwand zur Sicherung der Aktualität verringert sich detailliert.

Awareness-Initiative

- Verständnis dafür schaffen, dass Informationssicherheit wirklich ALLE angeht.
- Informationssicherheit aus den „abgehefteten“ Regelwerken herausholen und täglich „unaufdringlich“ präsent halten.
- Unbewusst fehlerhaftes, traditionelles Verhalten und Handeln auf Dauer verändern.
- Im Dialog sowohl die dienstlichen als auch die privaten Sichtweisen thematisieren.



(Sich) sicher sein im angemessenen Umgang mit Informationen

Awareness 1

- IT-Sicherheitsrichtlinien für IT-Anwender (auch als Web based Training)
 - Klassifizierung und sicherer Umgang mit Geschäftsinformationen
 - Zugangs- und Zugriffsschutz
 - Nutzung von E-Mail
 - Nutzung des Internets
 - Nutzung des BA-Intranets
 - Schutz vor Schadensprogrammen
 - Installation und Nutzung von IT-Komponenten
 - Mobiles Arbeiten

Awareness 2

- Info-Veranstaltungen für obere Führungskräfte
 - Bis Dezember 2009 haben 90% der oberen Führungskräfte an Veranstaltungen zur IT-Sicherheit/Informationssicherheit teilgenommen
 - Vorstand ist eingebunden
- 9 Beiträge im BA Mitarbeiter-Fernsehn BA direkt
 - Thematisch auf den IT-Anwender ausgerichtet
 - Beitrag jeweils 2 – 3 min lang
 - Jeweils ca. 15.000 – 25.000 Zuschauer
- Jahres-Wandkalender seit 2007
 - Verteilte Auflage ca. 25.000 Stück
 - Je Monat ein Cartoon mit Sicherheitstipp
- Mitarbeiter-Zeitung „BA-Dialog“
 - 2-monatlicher Cartoon mit Sicherheitstipp
 - 2-3 x jährlich ein Textbeitrag zu IT-Sicherheitsthemen
 - Auflage ca. 120.000 Stück

Awareness 3

■ IT-Sicherheits-Flyer

- Kurzinformation für alle IT-Nutzer (BA und ARGE)
- Verhaltenstipps, Problembehandlung, Ansprechpartner
- Auflage 156.000 Stück

■ IT-Newsletter (für Abonnenten per E-Mail-Link)

- 2-monatlicher Cartoon mit Sicherheitstipp
- Einmal jährlich ein Textbeitrag zu IT-Sicherheitsthemen
- Ca. 20.000 Abrufe

■ IT-Sicherheitsumfrage

- Zwei freiwillige Umfragen (2008 und 2009)
- Auswertung über BA-Umfragezentrum
- Ableitung von Handlungserfordernissen
- Ca. 4600 Teilnehmer

Awareness 4

- Führungskräfte und IT-Sicherheit
 - Verantwortungsfunktion
 - Vorbildfunktion
 - Krisenmanagementfunktion im Problem- bzw. Schadensfall

IT-Sicherheit ist eine Führungsaufgabe