> Der sichere Pfad durch den Datensecurity Jungle

Angela Espinosa, LH Systems AG

25. November 2014

Lufthansa Systems

IT that makes your life easier

> Agenda

- **Vorstellung LH Systems AG**
- Definition Informationssicherheit
- Gründe für Standards in der Informationssicherheit
- Gesetzliche Vorgaben
- Branchenregeln/Normen
- Relevante Normen für mein Unternehmen
- Umsetzung auf Datenbankebene
- IT Sicherheitsgesetz

> Vorstellung Lufthansa Systems AG

> Vorstellung Lufthansa Systems AG

- Full Service Provider → Unterstützung bei Optimierung von Prozessen und IT-Landschaften
- weltweit führende Position in der Aviation-Industrie
- mehrere Standorte in Deutschland und 16 weiteren Ländern mit 2.800 Mitarbeitern (Hauptstandort: Frankfurt am Main)
- 6.800 Quadratmeter Rechenzentrumsfläche mit über 2.500 Servern
- Kunden: Fluggesellschaften, Unternehmen aus Industrie, Transport und Logistik, Energie, Medien und Verlage, Touristik und Gesundheitswesen
- ISO 27001, PCI-DSS und PS951/ISAE3402 geprüft und zertifiziert

> Agenda

- Vorstellung LH Systems AG
- **Definition Informationssicherheit**
- Gründe für Standards in der Informationssicherheit
- Gesetzliche Vorgaben
- Branchenregeln/Normen
- Relevante Normen für mein Unternehmen
- Umsetzung auf Datenbankebene
- IT Sicherheitsgesetz

> Definition Informationssicherheit

- Eigenschaften von informationsverarbeitenden und -lagernden *(technischen oder nicht-technischen)* Systemen, welche Schutzziele sicherstellen:

- **Vertraulichkeit**
- **Verfügbarkeit**

- **Integrität**

- dient dem **Schutz vor Gefahren bzw. Bedrohungen**, der **Vermeidung von wirtschaftlichen Schäden** und der **Minimierung von Risiken**

(Quelle: Wikipedia)

> Agenda

- Vorstellung LH Systems AG
- Definition Informationssicherheit
- **Gründe für Standards in der Informationssicherheit**
- Gesetzliche Vorgaben
- Branchenregeln/Normen
- Relevante Normen für mein Unternehmen
- Umsetzung auf Datenbankebene
- IT Sicherheitsgesetz

> Gründe für Standards in der Informationssicherheit

- (digitale) Speicherung von Unternehmensdaten, personenbezogene Daten/Kreditkartendaten in großer Zahl
- Angriffsvektor für Hacker von intern sowie extern vergrößert sich
- Risiken für Unternehmen und öffentliche Einrichtungen steigen, erheblichen Schaden zu erleiden
- Druck durch Gesetzgeber und Kunden auf Unternehmen und öffentliche Einrichtungen wächst, Maßnahmen zur Informationssicherheit durchzuführen
- gesetzlichen Anforderungen an Compliance und Transparenz von Finanz- und Rechnungswesen steigt

→ sicherer Umgang mit Daten und informationsverarbeitenden Systemen erfordert Sicherheitsstandards

> Agenda

- Vorstellung LH Systems AG
- Definition Informationssicherheit
- Gründe für Standards in der Informationssicherheit
- **Gesetzliche Vorgaben**
- Branchenregeln/Normen
- Relevante Normen für mein Unternehmen
- Umsetzung auf Datenbankebene
- IT Sicherheitsgesetz

> Gesetzliche Vorgaben (Auszug)

- Dreh- und Angelpunkt → KonTraG (1998)
  → das Gesetz zur Kontrolle und Transparenz im Unternehmen

- Verbesserung der Corporate Governance deutscher Unternehmen

  - verbindliche Regeln und ein unternehmensweites Risikomanagement

  - Risiken müssen bewertet und darauf aufsetzend sinnvolle Maßnahmen formuliert werden

  - Vorstand wird verpflichtet „geeignete Maßnahmen zu treffen, insbesondere ein Überwachungssystem einzurichten und damit den Fortbestand der Gesellschaft gefährdende Entwicklungen früh erkannt werden"

KonTraG

> Gesetzliche Vorgaben (Auszug)

- Bundesdatenschutzgesetz (BDSG)
- → Sicherstellung des Schutzes personenbezogener Daten

- Personenbezogene Daten sind zum Beispiel Name, Alter, Familienstand, Geburtsdatum etc.
- Auftragsdatenverarbeitung-Vereinbarung (ADV-Vereinbarung) zwischen Vertragspartnern
- im Detail beschrieben, welche Rechte, Pflichten und Maßnahmen
- Datenschutzbeauftragter wirkt auf Einhaltung des BDSG hin

- Handelsgesetzbuch (HGB)

- → Buchführung „ordnungsmäßig“ (Schutzziele Integrität und Verfügbarkeit)
- Paragraf zur Verletzung der Geheimnispflicht (Schutzziel Vertraulichkeit)

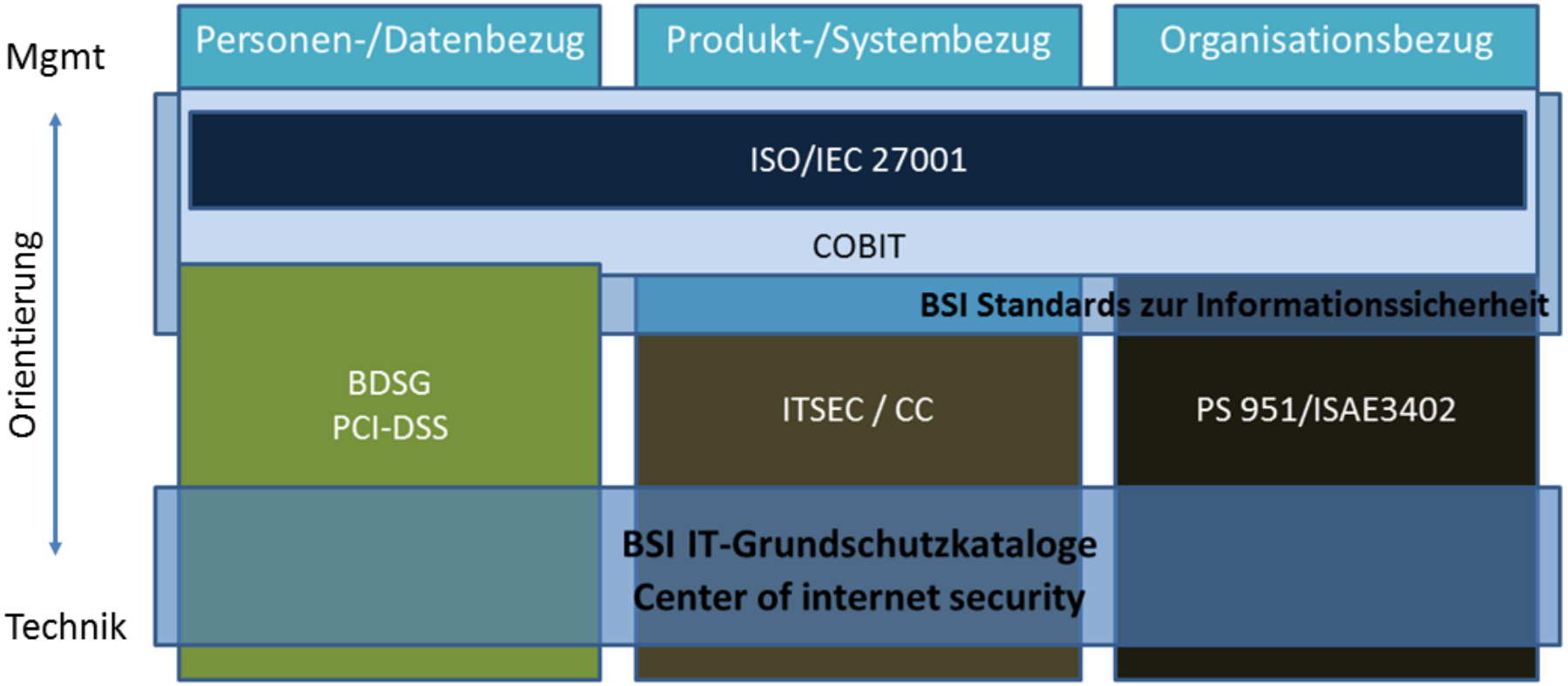
> Agenda

- Vorstellung LH Systems AG
- Definition Informationssicherheit
- Gründe für Standards in der Informationssicherheit
- Gesetzliche Vorgaben
- **Branchenregeln/Normen**
- Relevante Normen für mein Unternehmen
- Umsetzung auf Datenbankebene
- IT Sicherheitsgesetz

> Branchenregeln/Normen (Auszug)

- ISO/IEC 27000 (Informationssicherheits-Managementsysteme),
- BSI-IT Grundschutz und BSI Standards zur Informationssicherheit,
- CObit (Control Objectives for Information and related Technology),
- 20 Critical Security Controls,
- PCI-DSS (Payment card industry-Data Security Standard),
- IDW PS951/ ISAE3402 (Prüfstandards),
- ISO/IEC 20000 (Service Management),
- ITIL (IT Infrastructure Library)
- …

> Branchenregeln/Normen – Überblick



- Quelle: Andreas J. Henke: Informationssicherheit für KMU (2014)

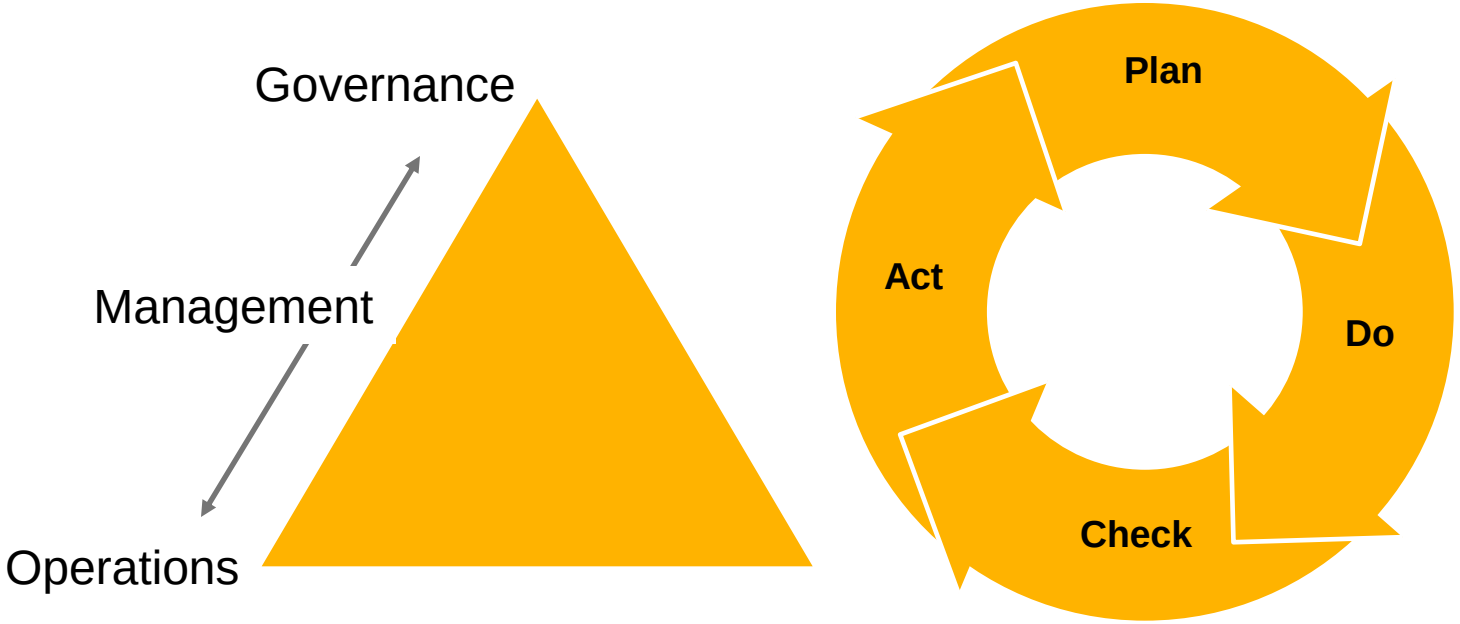
> Branchenregeln/Normen - Gegenüberstellung von 3

	ISO/IEC 27000	IDW PS951/ISAE3402	PCI-DSS
Betrachtung	Momentaufnahme	Gesamtes Rechnungsjahr	Einmal jährlich (dafür monatliche Vulnerability Scans, einer in 3 Monaten grün)
Stichproben	Willkürlich	Nach statistischen Regeln festgelegt (Vertrauensintervall)	100%
Motivation	Kundenforderung, Gesetzesanforderung	Ausgelagerte oder eigene Rechnungslegung, Gesetzesanforderung	Verarbeitung von Kreditkartendaten, zwingender Branchenstandard
Schwerpunkt auf	Governance und Management	Management und Operations	Management und Operations
Prüfer	Auditoren	Wirtschaftsprüfer	PCI DSS Auditoren
Systeme zur Überprüfung	ISMS (Information security management system) • Aspekt der kontinuierlichen Verbesserung ist Kernpunkt • Maßnahmen und Rückschau	IKS (Internes Kontrollsystem) Einhaltung von Regelungen wird überprüft.	Mehr Kontrollsystem Weniger Verbesserungspotenzial, da kein Managementsystem dahinter.

> Fazit Branchenregeln/Normen

- Modelle unterscheiden sich bei ihren Gewichtungen bezüglich Hierarchie und Komponenten
- Einzel-Maßnahmen auf technischer Ebene oft deckungsgleich
- Effektives Kontrollsystem über alle Hierarchie-Ebenen - Governance, Management, Operations
- Umfang aller Komponenten - Organisation, technische Maßnahmen und physische Maßnahmen

(Quelle: Andreas J. Henke)



> Agenda

- Vorstellung LH Systems AG
- Definition Informationssicherheit
- Gründe für Standards in der Informationssicherheit
- Gesetzliche Vorgaben
- Branchenregeln/Normen
- **Relevante Normen für mein Unternehmen**
- Umsetzung auf Datenbankebene
- IT Sicherheitsgesetz

> Relevante Normen für mein Unternehmen

- **Orientierung der Entscheidung**
  an Art des eigenen Geschäftsmodells und an den Ansprüchen Dritter:

  - Fordern ggf. Kunden eine spezifische Zertifizierung?
  - Gibt es in Ihrer Branche eine Norm also einen quasi Branchenstandard und/oder einen Wettbewerbsvorteil?
  - Verarbeiten Sie Kreditkartendaten?

- → Wenn Dritte (Geschäftspartner, Gesetzgeber ..) Anforderungen stellen, dann sollte das ökonomisch sinnvollste gewählt werden.

- **Freie Entscheidung:**

  - Wo unterliegen Sie einer gewissen Exposition?
  - Wo liegt das höchste Risiko für Ihren Geschäftszweck?
  - Wie sichern Sie sich am effizientesten und effektivsten ab?

  (Quelle: Andreas J. Henke)

> Agenda

- Vorstellung LH Systems AG
- Definition Informationssicherheit
- Gründe für Standards in der Informationssicherheit
- Gesetzliche Vorgaben
- Branchenregeln/Normen
- Relevante Normen für mein Unternehmen
- **Umsetzung auf Datenbankebene**
- IT Sicherheitsgesetz

> Umsetzung auf Datenbankebene

- **Transparenz auf DB-Ebene durch Prozessbeschreibungen und technischer Umsetzung von Regeln**

- Beschreibung von Prozessen
  - Usermanagement (inklusive Passwortmanagement)
  - Patchmanagement
  - Aufbau/Abbau und Standards
  - Administrationskonzept
  - Härtungskonzept und regelmäßige Checks
  - Schutzbedarffestellung für eigene Systeme
  - Umgang mit Ausnahmen

- Härtungsregeln
  - Unterstützung im Internet, zur Definition:
    - Center for Internet Security → Security Benchmarks für Datenbanken auch für Oracle
    - BSI IT Grundschutzkataloge
    - PCI DSS gibt es klare, vorgeschriebene Regeln
  - Regelmäßige Checks

> Umsetzung auf Datenbankebene

- **Passwortregeln**
  - Passwort Verify Funktion → sichere Passwörter
  - Profile einrichten (Reuse Max, Idle Time, Expire Time, Password Lock Time, Failed Login Attempts) und Benutzern zuweisen
- **Nachvollziehbarkeit**
  - Usermanagement
  - Persönliche Benutzer auf DB-Ebene verteilen
  - Auditing aktivieren
- **Minimierung von Privilegien**
  - Entfernen von unnötigen Rechten (PUBLIC, DBA …)
- **Sicherheitsparameter einstellen**
- **Minimierung der Komponenten**
- **Standardeinstellungen ändern**

> Agenda

- Vorstellung LH Systems AG
- Definition Informationssicherheit
- Gründe für Standards in der Informationssicherheit
- Gesetzliche Vorgaben
- Branchenregeln/Normen
- Relevante Normen für mein Unternehmen
- Umsetzung auf Datenbankebene
- **IT Sicherheitsgesetz**

>IT Sicherheitsgesetz (Entwurf)

- gilt für Betreiber kritischer Infrastrukturen (KRITIS) → Wer ist das?

- Einführung einer Meldepflicht für KRITIS-Betreiber
- Einführung von IT-Sicherheitsstandards
- Einführung verpflichtender IT-Audits (BSI)

- Ziel des Entwurfs: Verbesserung der IT-Sicherheit in Deutschland

- ABER: Unzureichende Definitionen und fehlenden Präzisierungen des Entwurfs

- Offene Fragen:
- Welche Unternehmen fallen unter die Regelungen?
- Und damit unter die vorgesehenen Meldepflichten?
- Was ist genau zu melden (Tatbestände)?

> Danke für Ihre Aufmerksamkeit! Fragen?