DataGuard

WAS PASSIERT BEI EINEM AUDIT DER INFORMATIONS- SICHERHEIT?

5. Oktober 2021

Christian Taube

CHRISTIAN TAUBE

Team Lead Information Security

Zertifizierter ISMS Security Officer
und Auditor nach ISO 27001

ICO-CERT
International Certification Organization

ERFAHRUNG

Geschäftsführer, LanguageWire München GmbH

Chief Solutions Officer, Xplanation NV (Leuven)

Mitgründer, Technischer Leiter und Aufsichtsrat,
Matrix Communications AG (München)

Einführung von DS-GVO + ISO 27001 Compliance und erfolgreiche Audits nach TISAX und ISO 27001 in internationalen Unternehmen

AUSBILDUNG

Studium in Stuttgart,
Eugene (Oregon) und München

AGENDA

- Warum Informationssicherheit?
- Was ist ein Audit?
- Welche Standards gibt es?
- Was passiert bei einem Audit?
- Top 5 Takeaways
- Zeit für Ihre Fragen!

WARUM INFORMATIONSSICHERHEIT?

Feuer im Rechenzentrum

3,4 Millionen Webseiten von Brand beim größten französischen Cloudbetreiber betroffen

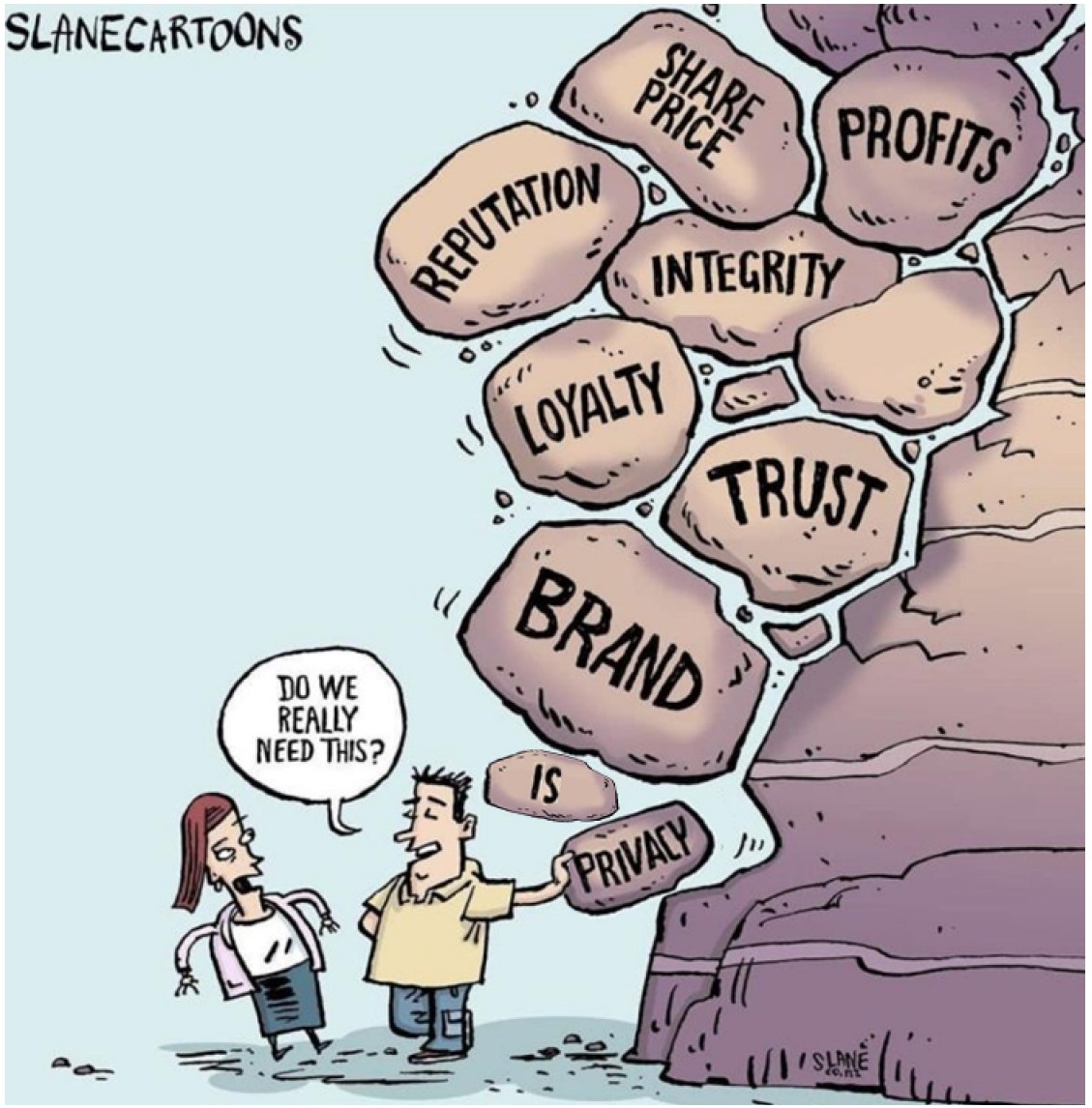
„Nach Angaben des französischen Webzeitung „Le Journal du net“ gab es in dem zerstörten Datenzentrum nur Alarmsysteme, doch keine Sprinkleranlagen oder ähnliche automatische Mittel zur Feuerbekämpfung.“

*Quelle: FAZ online

Warum Informationssicherheit?

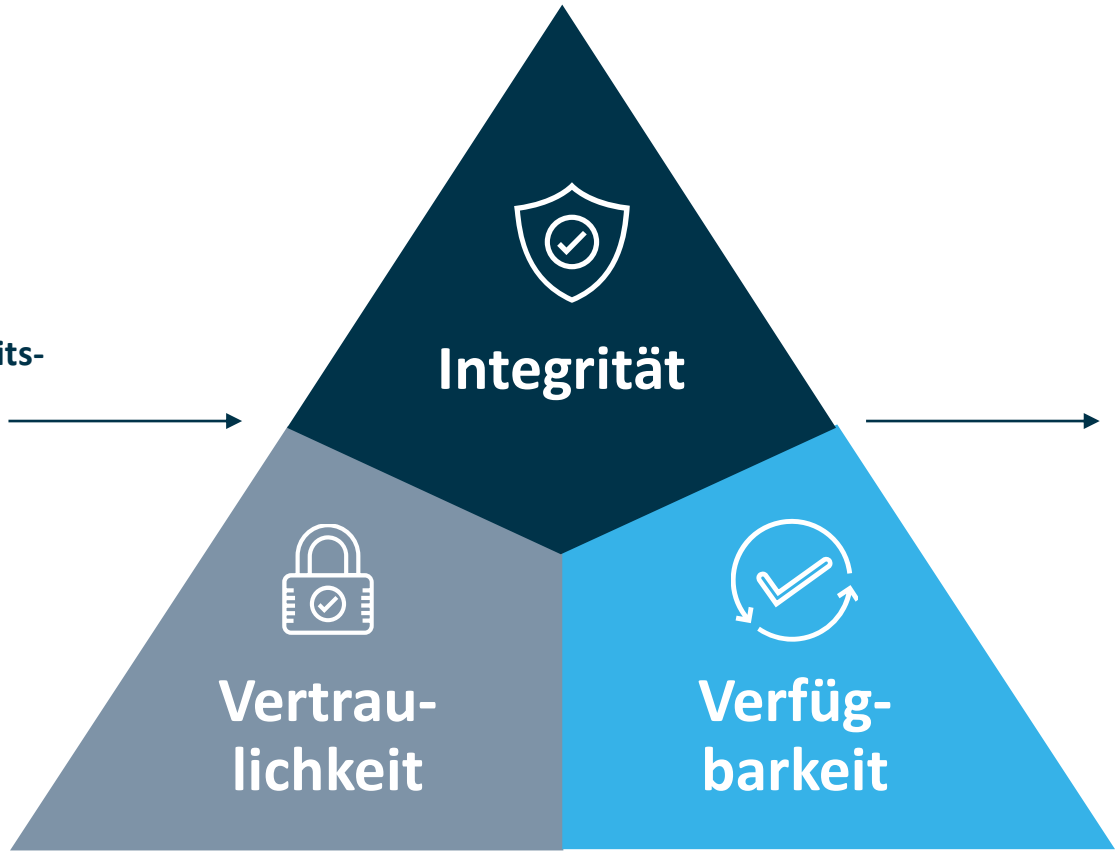
Datenschutz als fundamentaler Wert

Informationssicherheit als zweiter fundamentaler Wert



Was versteht man unter Informationswerten?

Das Informationssicherheits-Managementsystem schützt die



Ihrer Informationswerte vor Risiken und Schwachstellen

WELCHE STANDARDS GIBT ES?

Welche Standards gibt es?

ISO 27001	Managementsystem für Informationssicherheit – normativer MUSS-Katalog
TISAX®	Ableitung ISO 27001 für Automobil-Industrie, mit konkreten Reifegraden
BSI Grundschutz	Konkrete Maßnahmen für „mittleres, angemessenes und ausreichendes Schutzniveau“
ISO 27701	Erweiterung der ISO 27001 um ein Datenschutz-Managementsystem
SOC-2	Standard der Certified Public Accountants für allg. interne Kontrollsysteme
NIST 800-53	Sicherheits- u. Datenschutzkontrollen für Informationssysteme in US-Bundesbehörden

Maßnahmenziele der ISO 27001:2013

- A.5 Sicherheitsleitlinie (ISMS Policy)
- A.6 Organisation der Informationssicherheit
- A.7 Personelle Sicherheit
- A.8 Management organisationseigener Werte (assets)
- A.9 Zugangskontrolle
- A.10 Kryptographie
- A.11 Physische und umgebungsbezogene Sicherheit
- A.12 Betriebssicherheit der IT
- A.13 Betriebs- und Kommunikationsmanagement
- A.14 Beschaffung, Entwicklung, Wartung von Informationssystemen
- A.15 Beziehungen zu Zulieferern
- A.16 Umgang mit Informationssicherheitsvorfällen
- A.17 Sicherstellung des Geschäftsbetriebs (Business Continuity Management)
- A.18 Einhaltung von Vorgaben (Compliance)

Umfassendes Managementsystem – nicht nur IT-Sicherheit!

WAS IST EIN AUDIT?

Ziel und Zweck von Audits

Ein Audit ist…

… ein systematischer, unabhängiger und dokumentierter Prozess

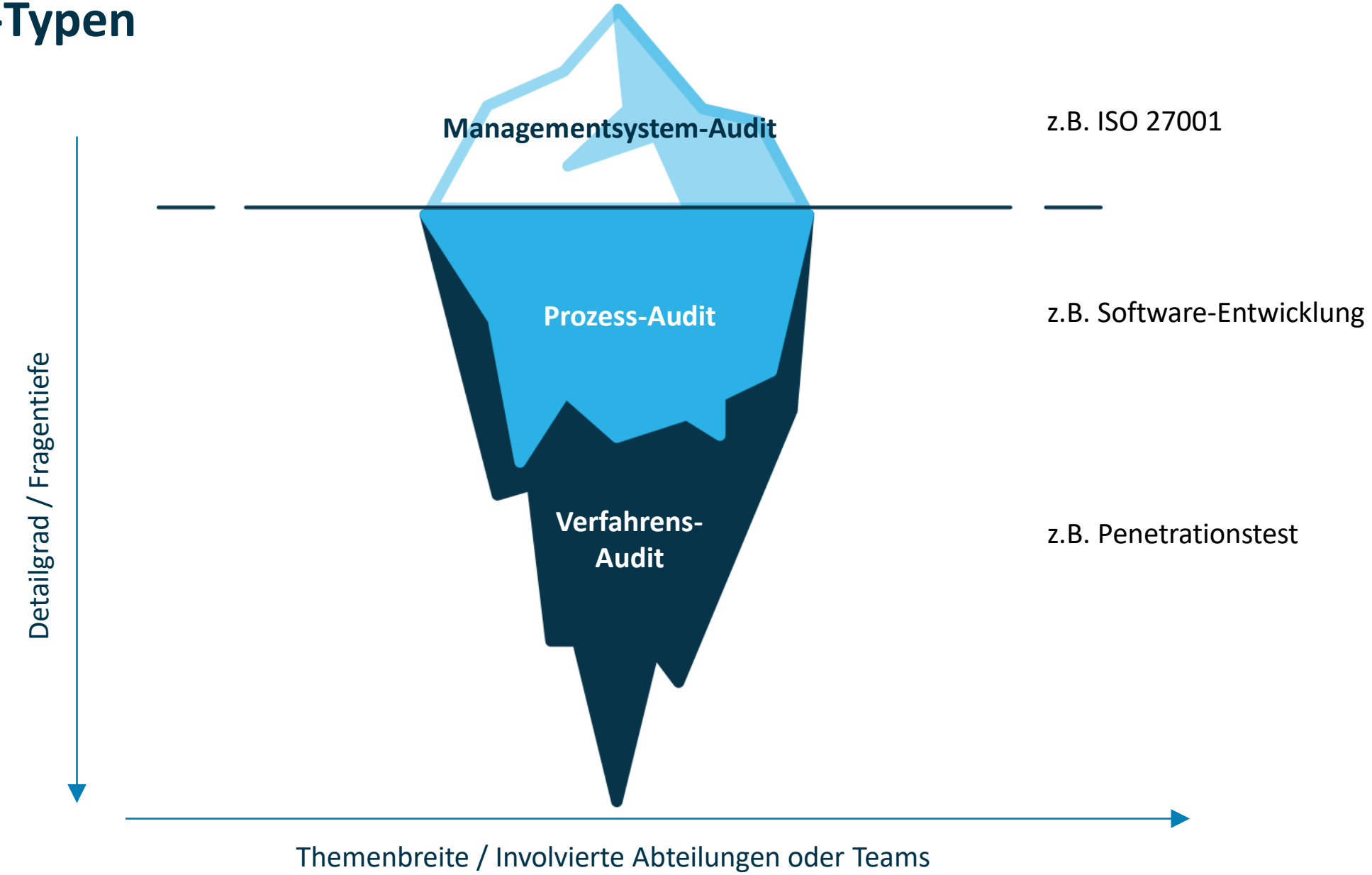
- *Klarer Prüfplan*
- *Kein Audit der eigenen Arbeit*
- *Aufzeichnung der Tätigkeiten*

… zur Erlangung von Nachweisen und zur deren objektiver Auswertung

- *„Wo steht das?“*
- *„Wie machen Sie das?“*
- *„Wie weisen Sie das nach?“*

… um zu ermitteln, inwieweit Audit-Kriterien erfüllt sind.

Audit-Typen


Managementsystem-Audit
Prozess-Audit
Verfahrens-
Audit
z.B. ISO 27001
z.B. Software-Entwicklung
z.B. Penetrationstest
Detailgrad / Fragentiefe
Themenbreite / Involvierte Abteilungen oder Teams

Audit-Arten für Managementsysteme

Remote-Audit

Vor-Ort-Audit

Interner Audit	Externer Audit	Externer Audit
„Second Party“	„Third Party“	
Ziel der *Zertifizierung*		
Innerhalb Ihrer Organisation unter eigener Verantwortung und Kontrolle	Ihre Organisation: - auditiert eine andere, z.B. Lieferanten-Audit - wird durch eine andere auditiert	Ein Auditor auditiert Ihre Organisation *im Auftrag* > Er *entscheidet* nicht über das Endergebnis > Akkreditierungsstelle

Audit-Ergebnisse

Konformität	Wirksamkeit des ISMS ist erwiesen.
Beobachtung	Wirksamkeit des ISMS ist erwiesen. Detailaspekt könnte verändert > verbessert werden.
Nebenabweichung	Wirksamkeit des ISMS ist insgesamt erwiesen. Jedoch fehlen einzelne Nachweise für die Umsetzung der beschriebenen Maßnahme in einem gegebenen Kontrollbereich / ist eine Maßnahme nur teilweise wirksam umgesetzt. Frist für „Heilung“: Bis zum nächsten Überwachungs-Audit (i.d.R. ein Jahr)
Hauptabweichung	Wirksamkeit des ISMS ist *nicht* erwiesen. Es fehlen wirksame Richtlinien in einem gegebenen Kontrollbereich / Maßnahmen sind in einem kompletten Kontrollbereich nicht vorhanden oder nachweisbar. Frist für „Heilung“: 90 Tage nach dem Audit

WAS GESCHIEHT IM AUDIT?

7 Audit-Prinzipien

Prinzipien für den Auditor

1. Integrität der Person
2. Sachlichkeit der Darstellung
3. Angemessene Sorgfalt

Prinzipien für den Audit

4. Vertraulichkeit der Informationen
5. Unabhängigkeit der Auditoren
6. Basis in Fakten und Verifizierbarkeit
7. Berücksichtigen von Risiken und Chancen

Audit-Ziele definieren

Konformität

- Richtlinien werden eingehalten
- Regeln werden befolgt

Quellen:

- Gesetze
- Normen
- Richtlinien
- Verfahren

Effektivität

- Die verfolgten Ziele werden tatsächlich erreicht
- Services + Produkte entsprechen den (eigenen u. fremden) Vorgaben

Ziele:

- SLAs
- Prozessziele
- …

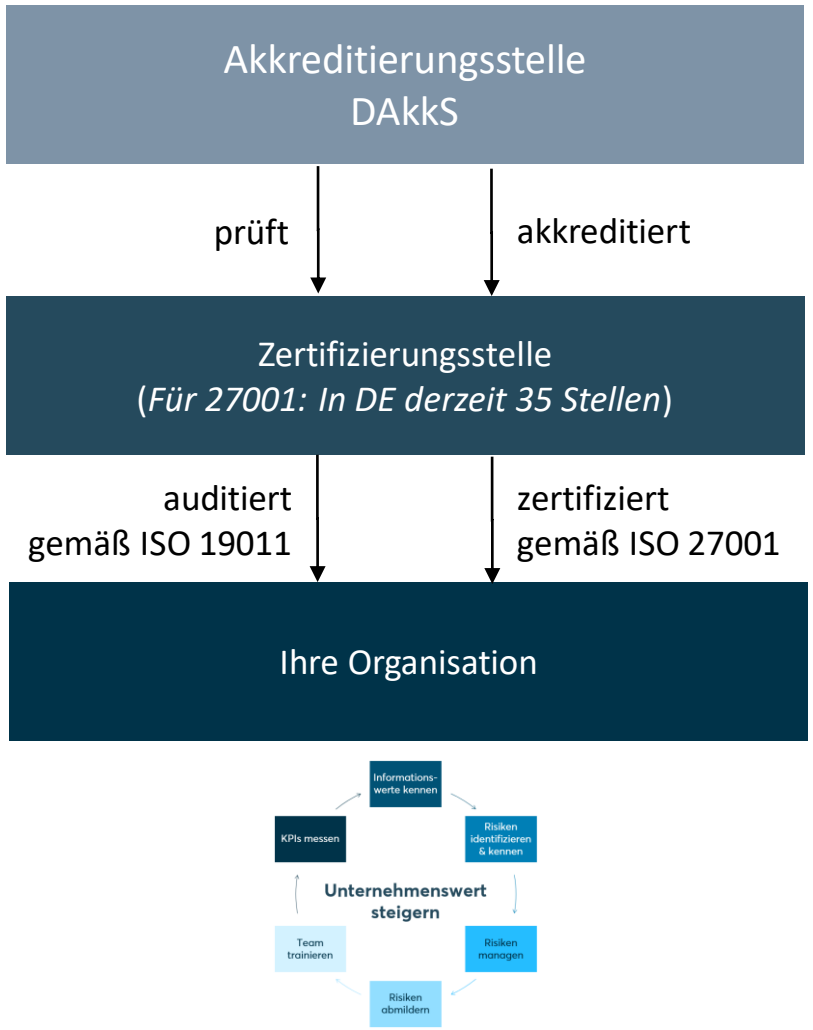
Effizienz

- Einsatz von Mitteln wird überwacht, beurteilt und optimiert
- Ressourcen werden verhältnismäßig eingesetzt

Ressourcen:

- Finanziell
- Personell
- Physisch
- Technisch

Der Weg zur ISO 27001-Zertifizierung



- Angebot durch Zertifizierungsstelle
- Fragebogen zum Scope beantworten
- Auftrag erteilen
- Initiales Assessment / Voraudit (*optional*)
- Zertifizierungsaudit Stufe 1
- Zertifizierungsaudit Stufe 2
- Erteilung Ihres Zertifikats

ISO 27001 Zertifizierungsaudit

Ist Ihr Managementsystem zertifizierungsfähig?

- Notwendige Informationen zum Geltungsbereich
- Prüfen Ihrer Dokumentation
- Zentrale Fragestellung:
  - Status der Implementierung des Managementsystems?
  - Lässt das vorhandene Managementsystem sowie dessen Implementierungsgrad grundsätzlich eine Zertifizierung zu?
  - Fehlen noch entscheidende Details?
- Ergebnis:
  Auditplan für das weitere Zertifizierungsaudit > Stufe 2, basierend auf dem erlangten Wissen über die Organisation.

Ist Ihr Managementsystem wirksam?

- Stichproben zu allen Anforderungen und
- in allen Prozessen bzw. Abteilungen innerhalb des Geltungsbereichs
- basierend auf:
  - Auditplan
  - Normforderungen
  - Dokumenten der Organisation
  - Grundlagen (z.B. Gesetze, weiterführende, branchenspezifische, erforderliche Normierungen)
- Abschlussgespräch
- Ggf. Korrekturmaßnahmen festlegen
- Nachfolgend: Verifizierung der Ursachenanalyse und der nachgewiesenen Maßnahmen

Was darf / wird ein Auditor tun und was nicht?

DARF / WIRD:

- Den gesamten Standort des Unternehmens sehen / begehen.
- Auf Einhaltung des Zeitplans bestehen.
- Jede Person befragen, die er trifft.
- Seine Fragen erklären.
- So lange fragen, bis die Antwort für seine Bewertung hinreicht.
- Im Rahmen der Vertraulichkeit jedes Dokument sehen, das Audit-Inhalte betrifft.
- Auf Mängel hinweisen.

DARF NICHT / WIRD NICHT:

- Fragen außerhalb des Geltungsbereichs des Managementsystems stellen.
- Den Zeitplan nicht einhalten.
- Sie beraten.
- Annahmen treffen.
- Trickfragen / verdeckte Fragen stellen.
- Selbst Hand anlegen.

Was sollte ich im Audit tun und lassen?

OK:

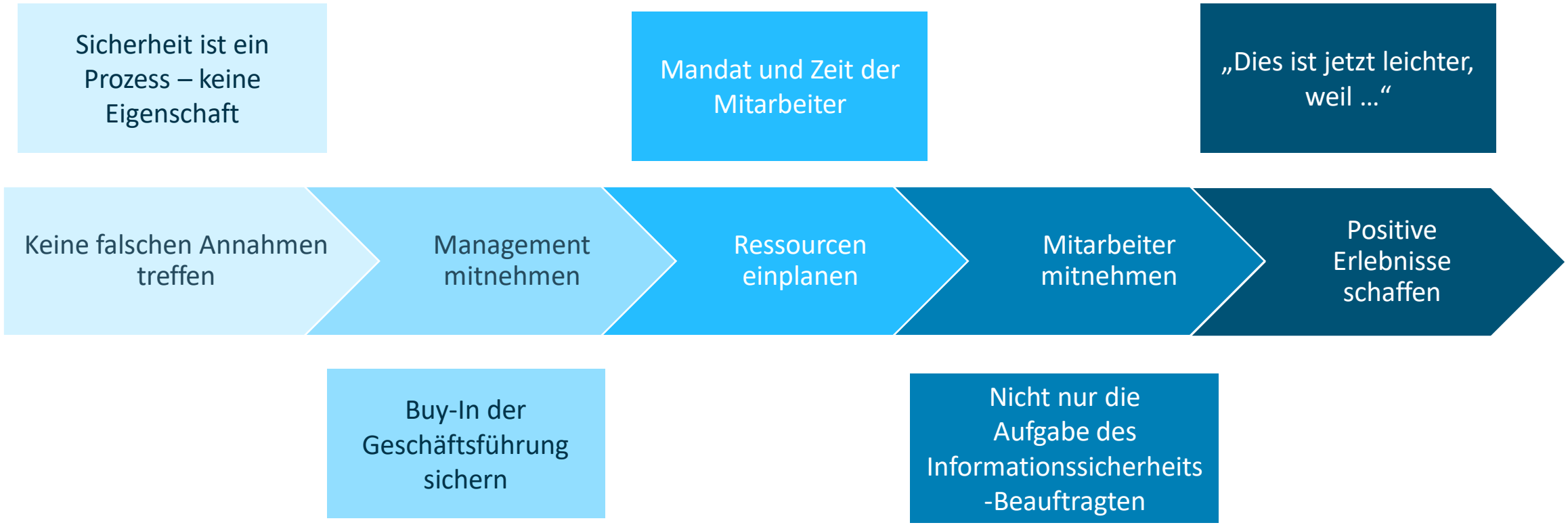
- Die eigenen Dokumente kennen.
- Die Fragen vollständig beantworten.
- Wenn die Antwort „Ich weiß es nicht“ ist – dann ist das die Antwort.
- Nichts verheimlichen.
- Bei Zweifeln nachfragen.
- Dem Auditor Zeit geben.
- Schweigen aushalten.

NICHT EMPFEHLENSWERT:

- Fragen beantworten, die nicht gestellt wurden.
- Nachfragen persönlich nehmen.
- Interne Audits nicht durchführen.
- Ihr Team nicht involvieren.
- Den Auditor überraschen.
- Bewusst täuschen.

ZUSAMMENFASSUNG

Top 5 Takeaways zum erfolgreichen ISO 27001-Audit



Zeit für Ihre Fragen!

Vielen Dank für Ihr Interesse!

Sie haben weitere Fragen?

So erreichen Sie mich.

E-Mail:

ctaube@dataguard.de

LinkedIn

https://www.linkedin.com/in/christiantaube/