DataGuard

ISO 27001 Implementierung –

So klappt's mit Ihrer Zertifizierung

16. September 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?
- Überblick: ISO 27001
- ISO 27001 Implementierung
- Deep Dive: ISO 27001 Audit
- Key Take Aways & Zeit für Ihre Fragen!

WARUM INFORMATIONSSICHERHEIT?

Feuer im Rechenzentrum

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

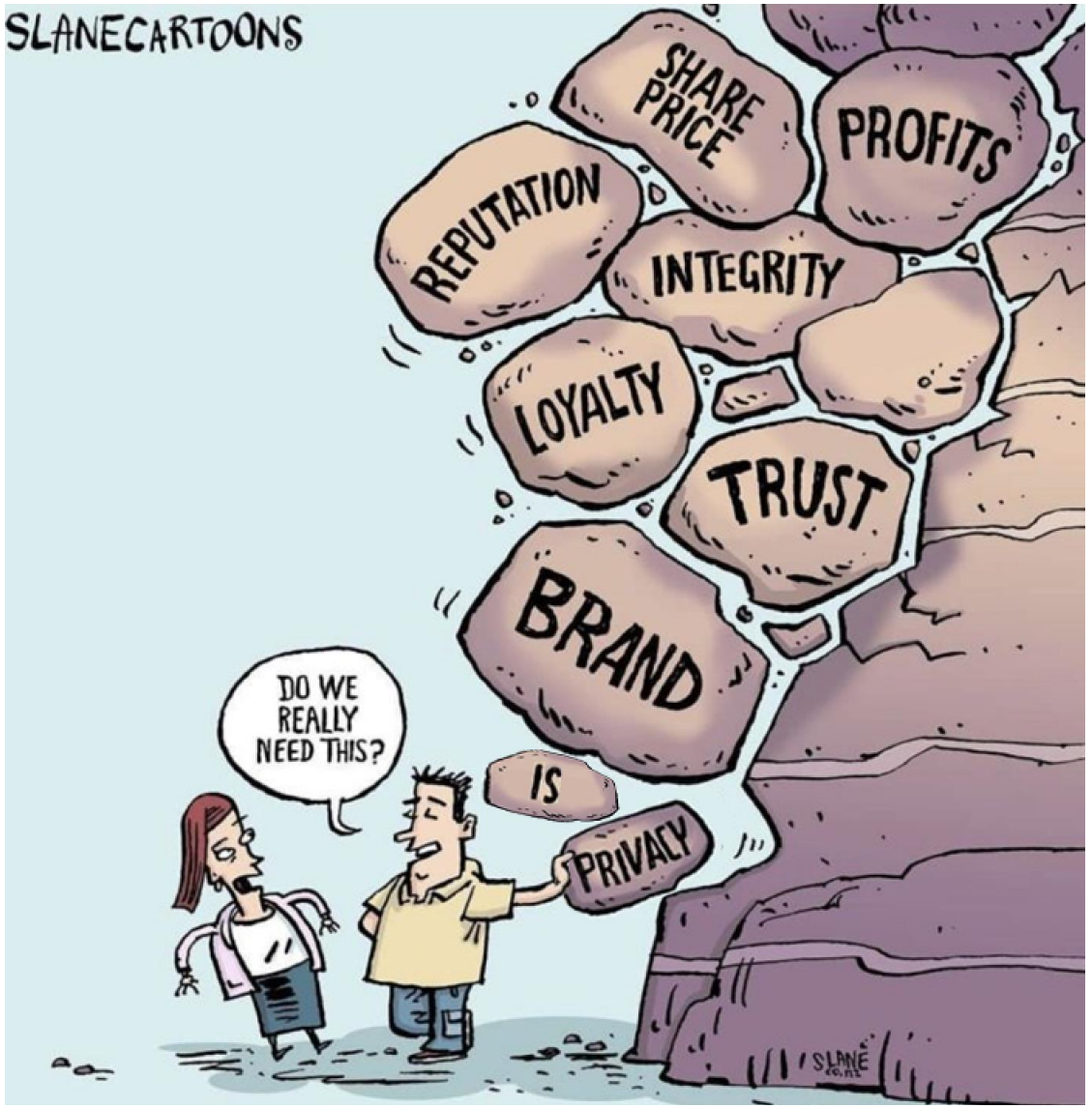
„Nach Angaben des französischen Webzeitung „Le Journal du net“ gab es in dem zerstörten Datenzentrum nur Alarmsysteme, doch keine Sprinkleranlagen oder ähnliche automatische Mittel zur Feuerbekämpfung.“

*Quelle: FAZ online

Warum Informationssicherheit?

Datenschutz als fundamentaler Wert

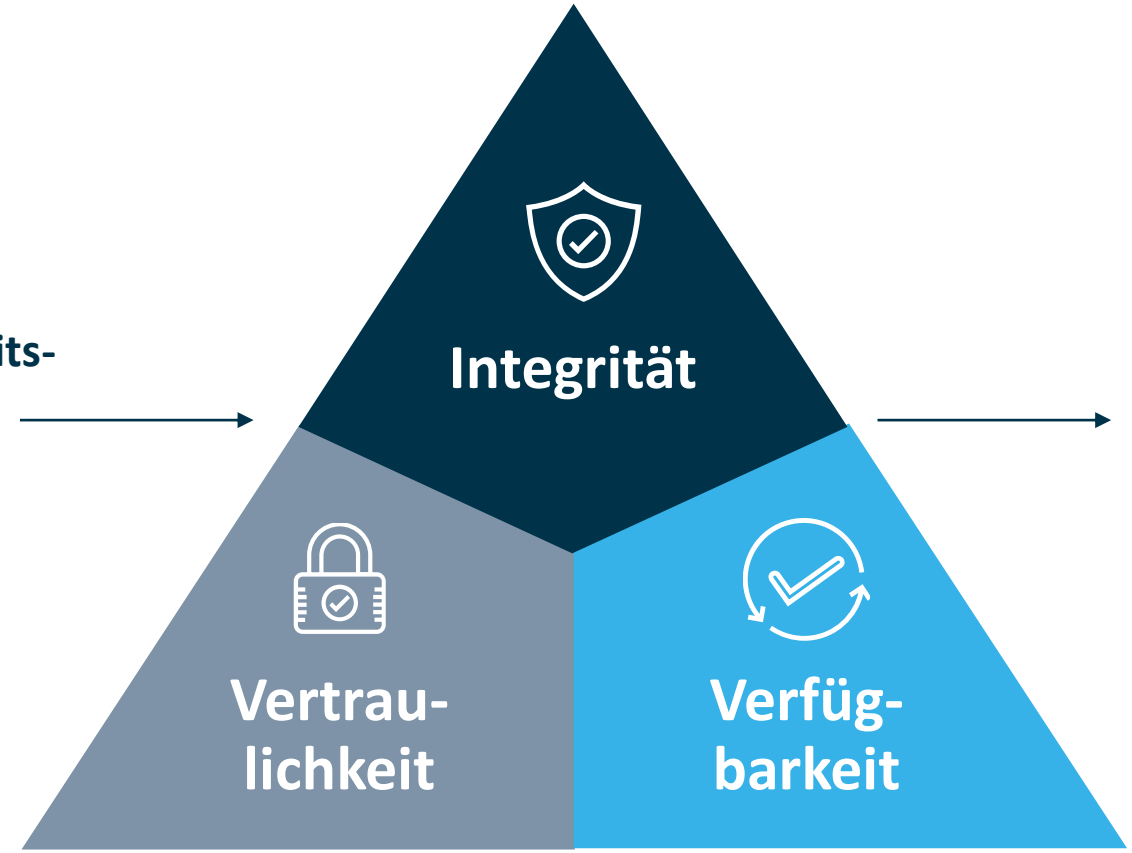
Informationssicherheit als zweiter fundamentaler Wert



ÜBERBLICK:
ISO 27001

Schutz Ihrer Informationswerte

Das Informationssicherheits-Managementsystem schützt die



Ihrer Informationswerte vor Risiken und Schwachstellen

Die ISO 27001 …

- ist der führende internationale Standard für Informationssicherheit
- bietet ein prozess- und risikoorientiertes Framework für den Aufbau eines ISMS (=Informationssicherheits-Managementsystems)
- sieht eine Zertifizierung vor
- kann von allen Unternehmen genutzt werden und ist deshalb
  - individuell auszulegen
  - Konkretere Hinweise zur Implementierung eines ISMS nach ISO 27001 Standard findet sich in der der ISO 27002
- enthält 6 übergreifende Kapitel und 14 Maßnahmen-Kapitel,
  die 114 Maßnahmenziele enthalten

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!

ISO 27001 Implementierung

Schritt 1: Zusammenstellung Ihres Teams

- ✓ Auswahl eines Projektmanagers/Projekttreibers
- ✓ Diese Person stellt das passende Team zusammen
- ✓ Gemeinsame Definition der Ziele, Vision und des gewünschten zeitlichen Rahmens des Projekts
- ✓ Festlegen der Rollen und Verantwortlichkeiten (z. B. anhand RACI-Matrix) („*responsible, accountable, consulted, informed*“)
- ✓ Festlegen der Stakeholder, die miteinbezogen werden müssen

---

Ergebnisse: **Verantwortlichkeitsmatrix des Projektteams, Entwurf der Erklärung zur Anwendbarkeit und der Dokumentation zum Anwendungsbereich**

Schritt 2: Zusammenstellung Ihres Teams

- ✓ Rückhalt und Commitment des Management einholen (v.a. mit Blick auf Ressourcen)
- ✓ Definition des ISMS-Anwendungsbereichs (z. B. Gesamtunternehmen vs. nur Entwicklung)
- ✓ Informationssicherheitsrichtlinie: Was will das Team erreichen, und wie?
- ✓ Dokumentation Ihrer Herangehensweise an die Informationssicherheit

---

Ergebnisse: Informationssicherheitsrichtlinie, Schulungsplan für Mitarbeiter, Entwurf von Aufzeichnungen, um die Effektivität Ihrer Maßnahmen zu verfolgen

Schritt 3: Risiken identifizieren und minimieren

- ✓ Definition von Regeln zur Bewertung Ihrer Risiken,
- ✓ … der Auswirkung der Risiken auf Ihr Geschäftsmodell sowie
- ✓ … der jeweiligen Eintrittswahrscheinlichkeit
- ✓ Festlegen des akzeptablen Risikoniveaus (hängt stark von der Art Ihres Unternehmens und Ihrer Risikotoleranz ab)

Ergebnisse: Prozesse für Risikomanagement, Pläne für Risikobewertung und -behandlung sowie Bewertung der Fehler in den Schritten zur Informationssicherheit

Schritt 4: Implementierung Ihrer Prozesse

- ✓ Start der konkreten Umsetzung Ihrer Prozesse zum Schutz Ihrer Informationswerte
- ✓ Eine wichtige Rolle spielen dabei auch Mitarbeitersensibilisierung, z. B. durch Schulung
- ✓ Definition von Überprüfungsschritten und verpflichtenden Verfahren
- ✓ Erweiterung und/oder Anpassung Ihrer Dokumentation: Im Rahmen der tatsächlichen Implementierung Ihrer Prozesse erlangen Sie mehr Klarheit und ggf. neue Erkenntnisse

---

Ergebnisse: Handbuch zum Informationssicherheits-Managementsystem (ISMS), neue Richtlinien zur Informationssicherheit, aktualisierter Audit-Plan für die interne Informationssicherheit, aktualisierte Pläne für die Risikobewertung und –behandlung

Schritt 5: Messen, überwachen, überprüfen

- ✓ Überprüfung Ihres Informationssicherheits-Managementsystems
- ✓ Durchführung interner Audits und ggf. Ableitung geeigneter Maßnahmen
- ✓ Definition Ihrer Leistungskennzahlen (KPIs)
- ✓ Erstellung Ihres Jahresberichts und einer Präsentation für Ihre Stakeholder
- ✓ ISMS mindestens einmal pro Jahr auf den Prüfstand durch Management und interne Audits stellen ➔ neue Gegebenheiten, neue Risiken, neue Bedrohungen zeitnah adressieren

---

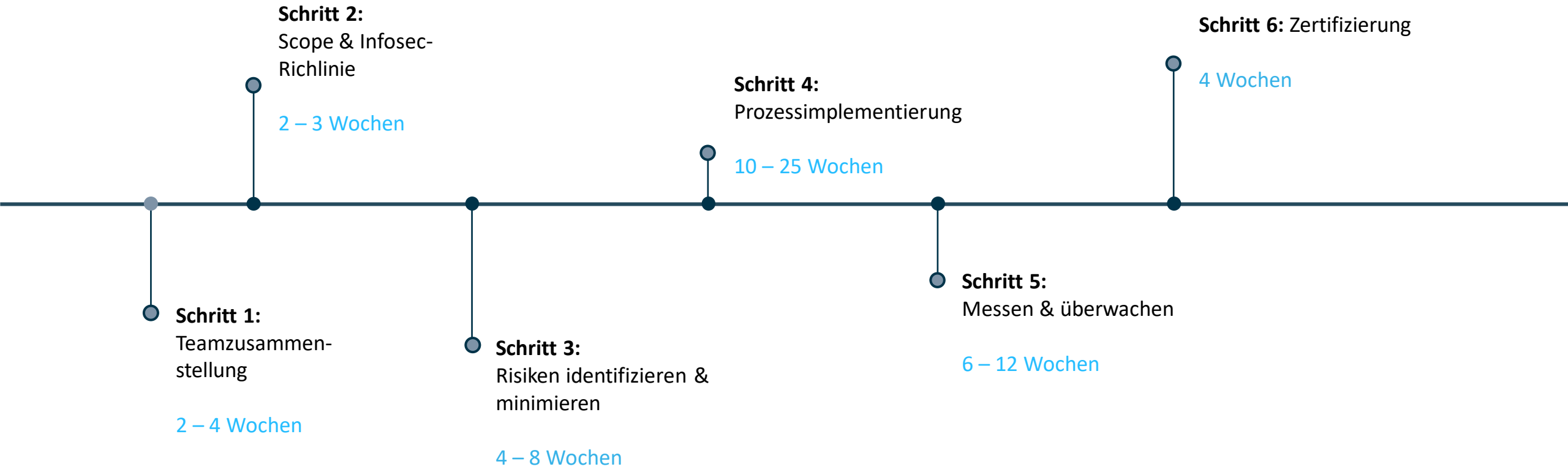
Ergebnisse: Messgrößen & Leistungskennzahlen (KPIs), internes Audit und -bericht, Jahresberichts und Präsentation für wichtige Stakeholder, Plan bzw. Pläne für Korrekturmaßnahmen und kontinuierliche Verbesserungen

Schritt 6: Zertifizierung

- ✓ Auswahl Ihres Auditors
- ✓ Vor dem Audit sollten Sie sicher sein, dass Sie Ihre Prozesse auch leben können.
  ➔ Audit-Kosten fallen so oder so an!
- ✓ Audit: Stufe 1: Nur Dokumentation – Stufe 2: Vor Ort

Ergebnisse: Vorbereitungsplan für das Zertifizierungs-Audit, Aktionspläne zur Behebung von Nichtkonformitäten

Timeline: Der Weg zur ISO 27001-Zertifizierung



DEEP DIVE:
ISO 27001 AUDIT

ISO 27001 Zertifizierungsaudit – Stufe 1

Ist Ihr Managementsystem zertifizierungsfähig?

- Sammeln von notwendigen Informationen zum Geltungsbereich.
- Prüfen Ihrer Dokumentation auf Konformität und Vollständigkeit.
- 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.

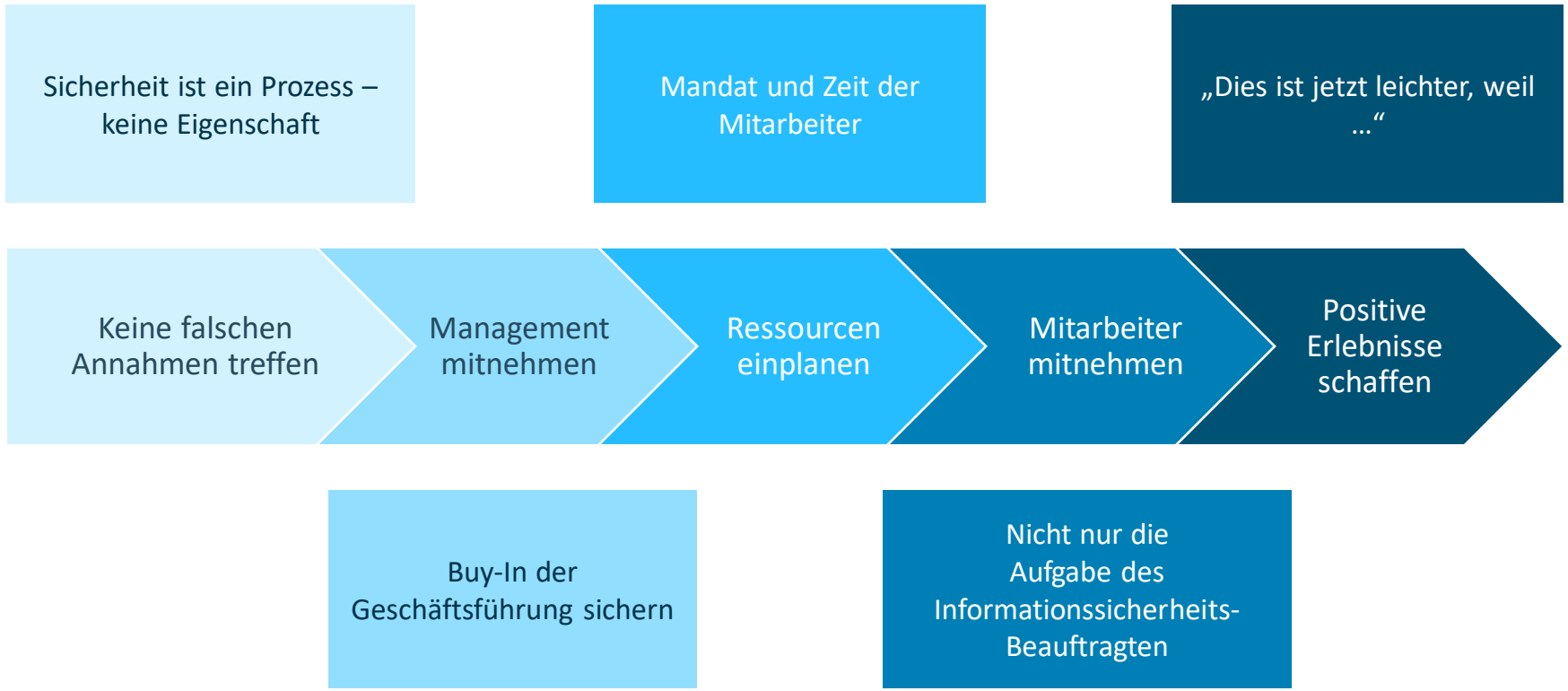
ISO 27001 Zertifizierungsaudit – Stufe 2

Ist Ihr Managementsystem wirksam?

- Stichproben zu allen Anforderungen und
- in allen Prozessen bzw. Abteilungen innerhalb des Geltungsbereichs
- basierend auf:
  - Forderungen der Norm
  - Dokumenten der Organisation
  - Grundlagen (z.B. Gesetze, weiterführende, branchenspezifische, erforderliche Normierungen)
- Abschlussgespräch: Bewertung der Ergebnisse, erstes Auditergebnis sowie ggf. Mitteilung von Mängeln / Abweichungen.
- Ggf. Festlegen von Korrekturmaßnahmen.
- Nachfolgend: Verifizierung der Ursachenanalyse und der nachgewiesenen Maßnahmen durch das Auditteam.

ZUSAMMENFASSUNG

Top 5 Takeaways zum erfolgreichen ISO 27001-Audit



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/