Software EMEA Performance Tour 2013

17.-19 Juni, Berlin

In 12 Schritten zur ISo27001

Tipps & Tricks zur ISO/IEC 27001:27005

Gudula Küsters

Juni 2013

Das ISO Rennen und wie Sie den Halt nicht verlieren

12 Schritte zur ISO 27001

1. Projekt Ziel und Setup
2. TOP Management Awareness
3. Rollen und Verantwortlichkeiten im ISMS
4. Definition des Geltungsbereiches
5. Mitarbeiter Awareness
6. Erstellung einer SOA für den Geltungsbereich
7. GAP Analyse zur Standortbestimmung
8. Einführung Dokumentenmanagement
9. Dokumentationen
10. Notwendige Prozesseinführungen
11. Kontinuierlicher Verbesserungsprozess
12. Audits intern und extern

12 Schritte zur ISO 27001

1. Projekt Ziel und Setup
2. TOP Management Awareness
3. Rollen und Verantwortlichkeiten im ISMS
4. Definition des Geltungsbereiches
5. Mitarbeiter Awareness
6. Erstellung einer SOA für den Geltungsbereich
7. GAP Analyse zur Standortbestimmung
8. Einführung Dokumentenmanagement
9. Dokumentationen
10. Notwendige Prozesseinführungen
11. Kontinuierlicher Verbesserungsprozess
12. Audits intern und extern

Ziel der ISO/IEC 27001

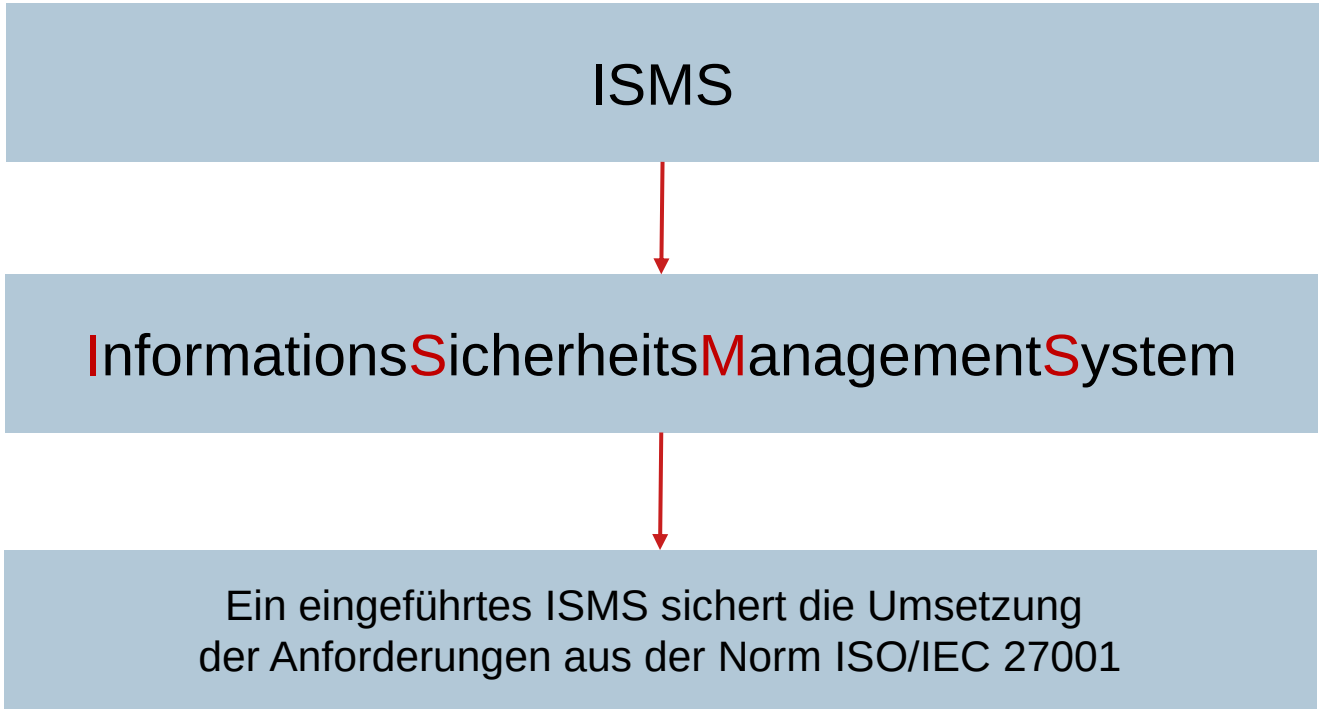
Die ISO/IEC 27001 ist aus dem britischen Standard BS 7799-2 hervorgegangen.

- Ziel der Norm ISO/IEC 27001 ist die Anforderungen an ein Informationssicherheits-Managementsystem (im folgenden ISMS genannt) im Rahmen eines Prozess-Ansatzes darzustellen.
- Die ISO/IEC 27001 beinhaltet Anforderungen an ein ISMS, das mittelbar zur Informationssicherheit beiträgt.

Informationen
- angemessen
- wirksam
- durchgängig

vor den jeweils identifizierten Bedrohungen zu schützen

Definitionen - ISMS



Projekt Ziel und Setup

...

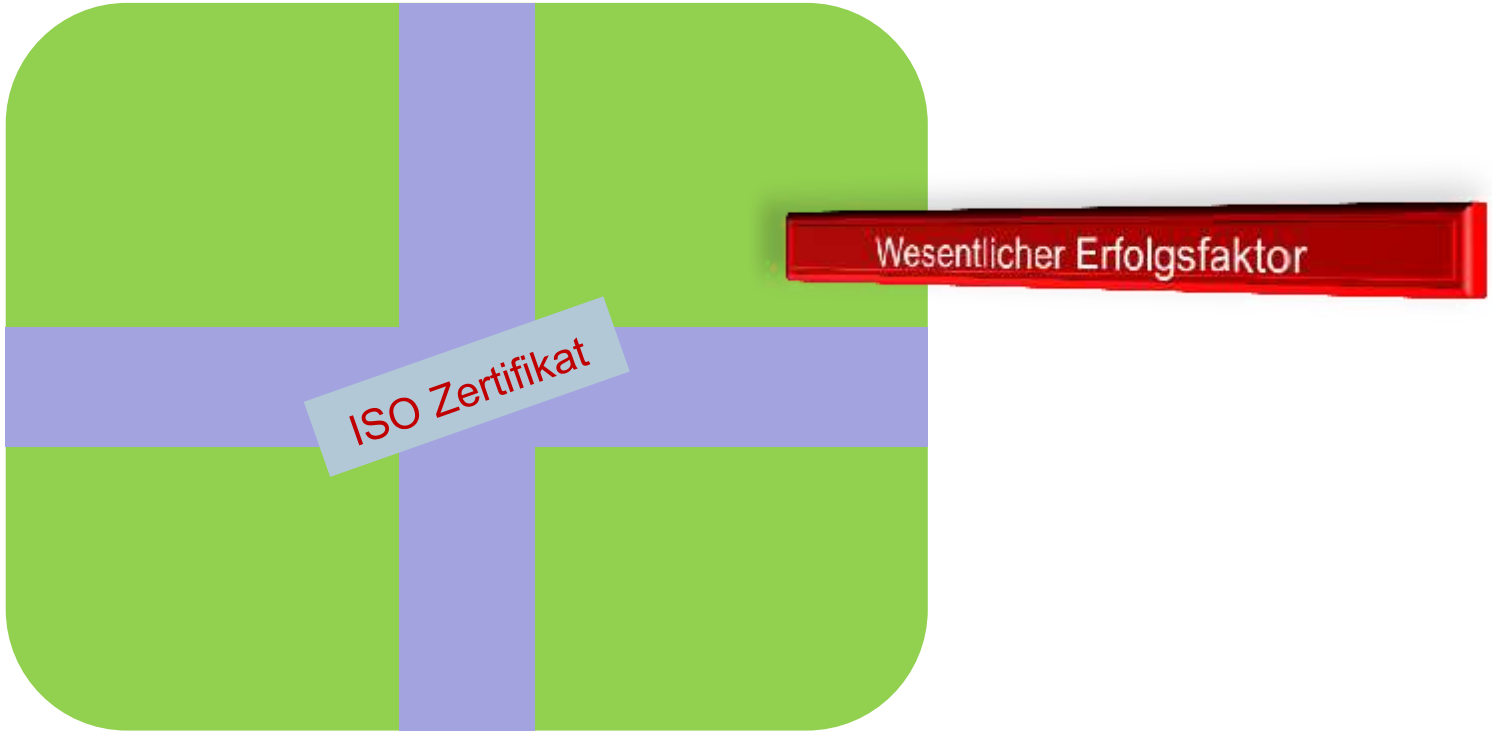
Security

Marketing

Ausschreibungen

Reifegraderhöhung

Projekt Ziel und Setup



12 Schritte zur ISO 27001

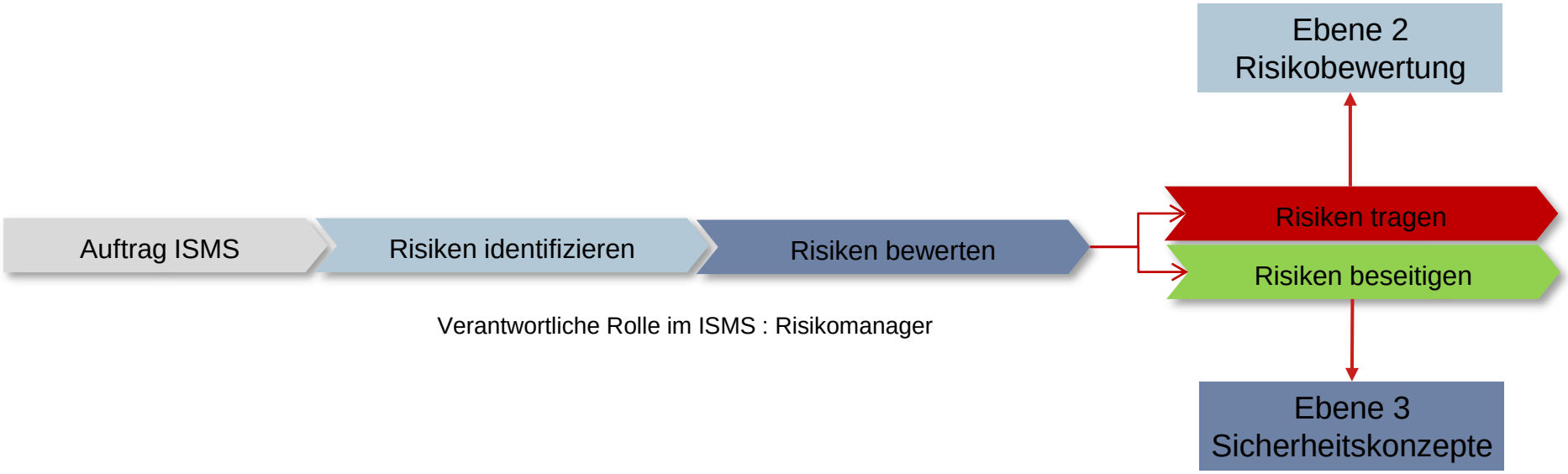
1. Projekt Ziel und Setup
2. TOP Management Awareness
3. Rollen und Verantwortlichkeiten im ISMS
4. Definition des Geltungsbereiches
5. Mitarbeiter Awareness
6. Erstellung einer SOA für den Geltungsbereich
7. GAP Analyse zur Standortbestimmung
8. Einführung Dokumentenmanagement
9. Dokumentationen
10. Notwendige Prozesseinführungen
11. Kontinuierlicher Verbesserungsprozess
12. Audits intern und extern

TOP Management Arwareness

12 Schritte zur ISO 27001

1. Projekt Ziel und Setup
2. TOP Management Awareness
3. Rollen und Verantwortlichkeiten im ISMS
4. Definition des Geltungsbereiches
5. Mitarbeiter Awareness
6. Erstellung einer SOA für den Geltungsbereich
7. GAP Analyse zur Standortbestimmung
8. Einführung Dokumentenmanagement
9. Dokumentationen
10. Notwendige Prozesseinführungen
11. Kontinuierlicher Verbesserungsprozess
12. Audits intern und extern

Risikomanagement



Verantwortliche Rolle im ISMS : Risikomanager

Mögliche Rollen in einem ISMS

- ISMS Security Board
  - Bericht des Risk Manager an das TOP Management, Risiken akzeptieren und tragen, Maßnahme Katalog genehmigen
- CISO
  - Chief Information Security Officer
  - Einhaltung, Durchführung, Umsetzung des ISMS
  - Prüfung und Überwachung des Maßnahme Kataloges
- Informationssicherheitsbeauftragter
  - Ist mit definierten Tätigkeiten im Rahmen des ISMS betraut (z.B. Audits, Monitoring)
- Risk Manager
  - Risiko Management
  - Bestimmt den Schutzbedarf (Risikoklassifizierung, Bedrohungsszenario, Risikobewertung, Erstellung und Pflege des Maßnahme Kataloges)
- etc. …

12 Schritte zur ISO 27001

1. Projekt Ziel und Setup
2. TOP Management Awareness
3. Rollen und Verantwortlichkeiten im ISMS
4. Definition des Geltungsbereiches
5. Mitarbeiter Awareness
6. Erstellung einer SOA für den Geltungsbereich
7. GAP Analyse zur Standortbestimmung
8. Einführung Dokumentenmanagement
9. Dokumentationen
10. Notwendige Prozesseinführungen
11. Kontinuierlicher Verbesserungsprozess
12. Audits intern und extern

Scope – Definition des Scope eines ISMS

- Kapitel 4 Punkt 4.2.1 fordert die Definition des Anwendungsbereiches und der Grenzen des Informationssicherheitsmanagementsystems (ISMS), unter Berücksichtigung der Eigenschaften des Geschäfts, der Organisation, ihres Standortes, ihrer Werte (Assets) und ihrer Technologie, einschließlich der Details über und Rechtfertigung von jeglichen Ausschlüssen aus dem Anwendungsbereich.

12 Schritte zur ISO 27001

1. Projekt Ziel und Setup
2. TOP Management Awareness
3. Rollen und Verantwortlichkeiten im ISMS
4. Definition des Geltungsbereiches
5. Mitarbeiter Awareness
6. Erstellung einer SOA für den Geltungsbereich
7. GAP Analyse zur Standortbestimmung
8. Einführung Dokumentenmanagement
9. Dokumentationen
10. Notwendige Prozesseinführungen
11. Kontinuierlicher Verbesserungsprozess
12. Audits intern und extern

Scope – Mitarbeiter in Scope

- Alle Mitarbeiter, die beteiligt sind an der Erbringung der definierten Services sind sogenannte „Mitarbeiter in Scope“
- Der ISMS Verantwortliche meldet alle beteiligten Mitarbeiter für einen Audit an
- Jeder betroffene Mitarbeiter sollte zumindest grundlegenden Fragen zum ISMS im Rahmen eines Auditprozesses beantworten können

12 Schritte zur ISO 27001

1. Projekt Ziel und Setup
2. TOP Management Awareness
3. Rollen und Verantwortlichkeiten im ISMS
4. Definition des Geltungsbereiches
5. Mitarbeiter Awareness
6. Erstellung einer SOA für den Geltungsbereich
7. GAP Analyse zur Standortbestimmung
8. Einführung Dokumentenmanagement
9. Dokumentationen
10. Notwendige Prozesseinführungen
11. Kontinuierlicher Verbesserungsprozess
12. Audits intern und extern

Controlls ISO/IEC 27001

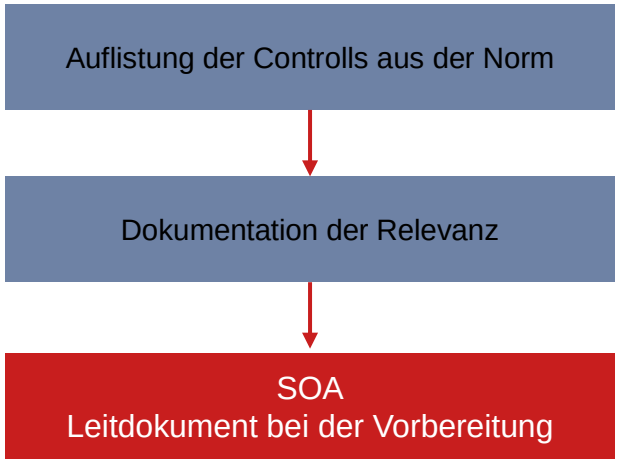
Segmente	
A.5 Sicherheitsleitlinie	A.11 Zugangskontrolle
A.6 Organisation der Informationssicherheit	A.12 Beschaffung, Entwicklung und Wartung von Informationssystemen
A.7 Management von organisationseigenen Werten	A.13 Umgang mit Informationssicherheitsvorfällen
A.8 Personelle Sicherheit	A.14 Sicherstellung des Geschäftsbetriebs (Business Continuity Management)
A.9 Physische und umgebungsbezogene Sicherheit	A.15 Einhaltung von Vorgaben (Compliance)
A.10 Betriebs- und Kommunikationsmanagement	

...

SOA – Statement of Applicability

- The statement of applicability is a document which identifies the controls chosen for your environment, and explains how and why they are appropriate.

Das bedeutet:



...

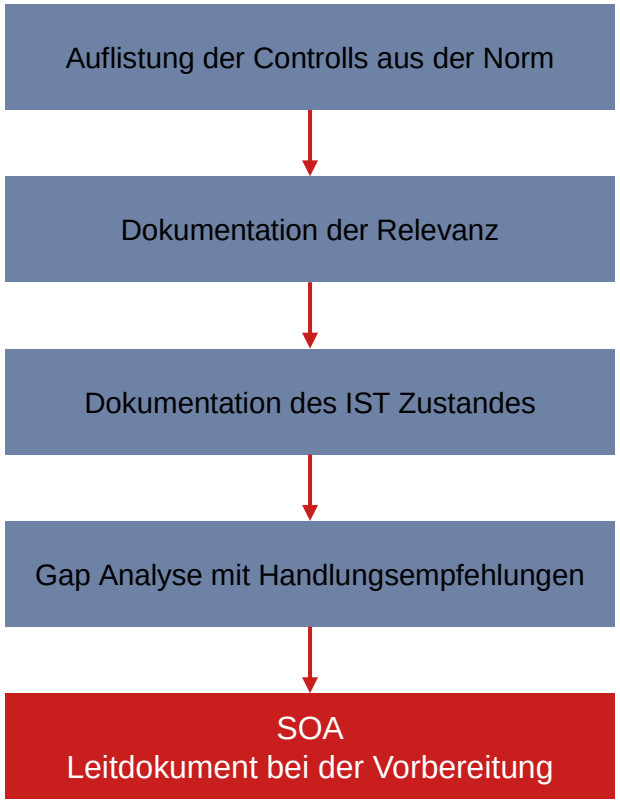
12 Schritte zur ISO 27001

1. Projekt Ziel und Setup
2. TOP Management Awareness
3. Rollen und Verantwortlichkeiten im ISMS
4. Definition des Geltungsbereiches
5. Mitarbeiter Awareness
6. Erstellung einer SOA für den Geltungsbereich
7. GAP Analyse zur Standortbestimmung
8. Einführung Dokumentenmanagement
9. Dokumentationen
10. Notwendige Prozesseinführungen
11. Kontinuierlicher Verbesserungsprozess
12. Audits intern und extern

SOA – Statement of Applicability

- The statement of applicability is a document which identifies the controls chosen for your environment, and explains how and why they are appropriate.

Das bedeutet:



...

12 Schritte zur ISO 27001

1. Projekt Ziel und Setup
2. TOP Management Awareness
3. Rollen und Verantwortlichkeiten im ISMS
4. Definition des Geltungsbereiches
5. Mitarbeiter Awareness
6. Erstellung einer SOA für den Geltungsbereich
7. GAP Analyse zur Standortbestimmung
8. Einführung Dokumentenmanagement
9. Dokumentationen
10. Notwendige Prozesseinführungen
11. Kontinuierlicher Verbesserungsprozess
12. Audits intern und extern

Dokumentenmanagement - Dokumente

- müssen geschützt und gelenkt werden
- dokumentierte Verfahren z.B. Dokumentationsrichtlinie einführen
- erstellen oder aktualisieren
- prüfen
- genehmigen
- kontrollierte und dokumentierte Verteilung
- alle diese Schritte nachvollziehbar dokumentieren
- Änderungen und Überarbeitungsstatus kennzeichnen
- Verfügbarkeit sicherstellen
- lesbar und leicht erkennbar
- Kennzeichnen gemäß Klassifizierungsrichtlinie
- ordnungsgemäße Entsorgung
- …

12 Schritte zur ISO 27001

1. Projekt Ziel und Setup
2. TOP Management Awareness
3. Rollen und Verantwortlichkeiten im ISMS
4. Definition des Geltungsbereiches
5. Mitarbeiter Awareness
6. Erstellung einer SOA für den Geltungsbereich
7. GAP Analyse zur Standortbestimmung
8. Einführung Dokumentenmanagement
9. Dokumentationen
10. Notwendige Prozesseinführungen
11. Kontinuierlicher Verbesserungsprozess
12. Audits intern und extern

Dokumentenmanagement - Aufzeichnungen

- erstellen und Instand halten
- schützen und kontrollieren
- gesetzliche oder amtliche Anforderungen
  und vertragliche Verpflichtungen beachten
- lesbar, leicht erkennbar und wieder auffindbar
- einhalten von Kennzeichnung, Aufbewahrung, Schutz, Wiederauffindbarkeit,
  Aufbewahrungsfrist und Benutzung der Aufzeichnungen
- nicht nur Prozessabläufe, sondern auch Nachweise über die Prozessaktivitätsdurchläufe
  dokumentieren
- …

12 Schritte zur ISO 27001

1. Projekt Ziel und Setup
2. TOP Management Awareness
3. Rollen und Verantwortlichkeiten im ISMS
4. Definition des Geltungsbereiches
5. Mitarbeiter Awareness
6. Erstellung einer SOA für den Geltungsbereich
7. GAP Analyse zur Standortbestimmun
8. Einführung Dokumentenmanagement
9. Dokumentationen
10. Notwendige Prozesseinführungen
11. Kontinuierlicher Verbesserungsprozess
12. Audits intern und extern

ITSM Prozesse

Service Strategy

Service Design

Service Transition

Service Operation

CSI

12 Schritte zur ISO 27001

1. Projekt Ziel und Setup
2. TOP Management Awareness
3. Rollen und Verantwortlichkeiten im ISMS
4. Definition des Geltungsbereiches
5. Mitarbeiter Awareness
6. Erstellung einer SOA für den Geltungsbereich
7. GAP Analyse zur Standortbestimmun
8. Einführung Dokumentenmanagement
9. Dokumentationen
10. Notwendige Prozesseinführungen
11. Kontinuierlicher Verbesserungsprozess
12. Audits intern und extern

PDCA Cycle

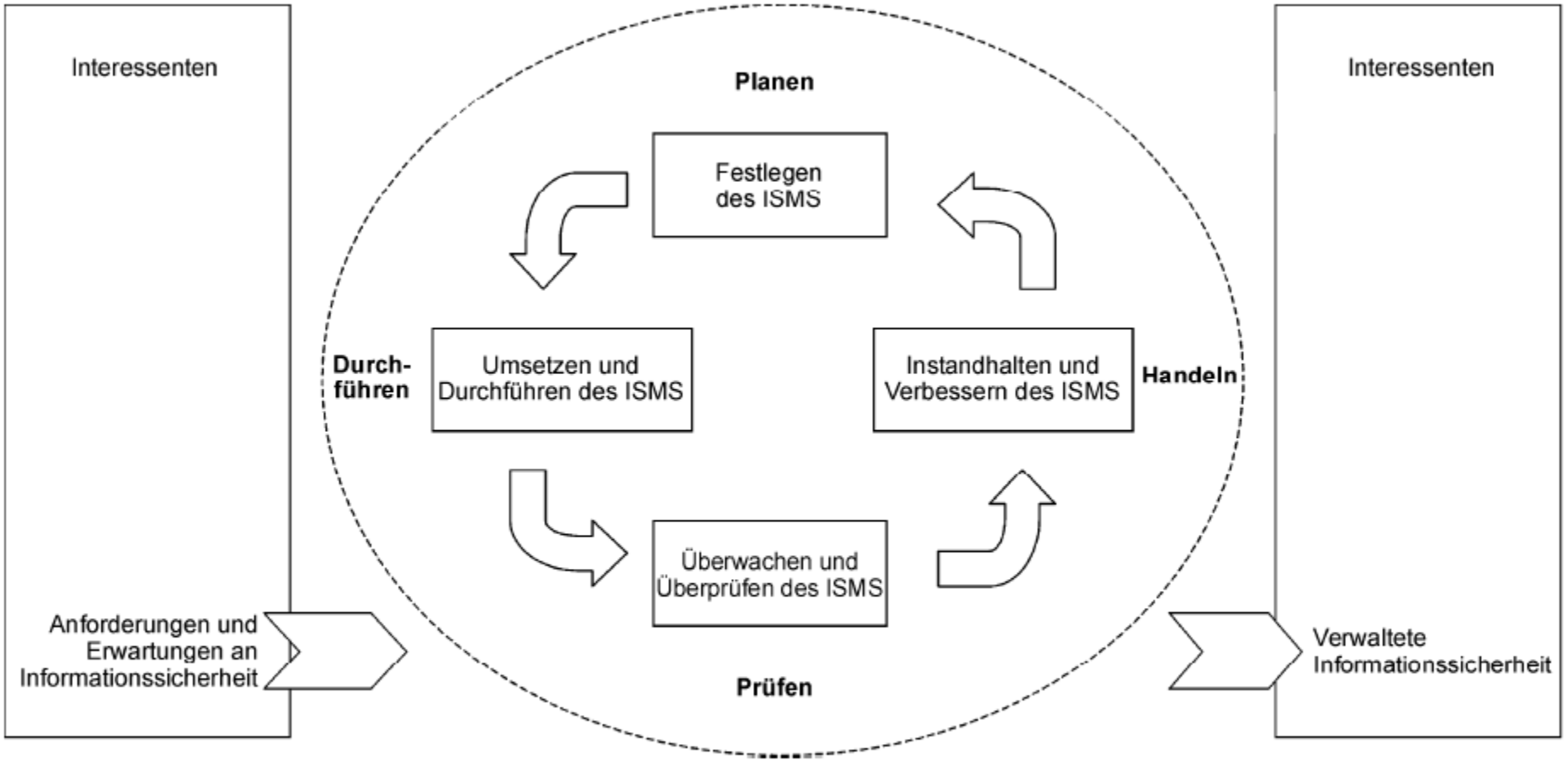


Bild 1 — Auf die ISMS-Prozesse angewandtes PDCA-Modell

12 Schritte zur ISO 27001

1. Projekt Ziel und Setup
2. TOP Management Awareness
3. Rollen und Verantwortlichkeiten im ISMS
4. Definition des Geltungsbereiches
5. Mitarbeiter Awareness
6. Erstellung einer SOA für den Geltungsbereich
7. GAP Analyse zur Standortbestimmun
8. Einführung Dokumentenmanagement
9. Dokumentationen
10. Notwendige Prozesseinführungen
11. Kontinuierlicher Verbesserungsprozess
12. Audits intern und extern

Umgang mit Auditoren

Auditoren

Klare Vorgehensweise

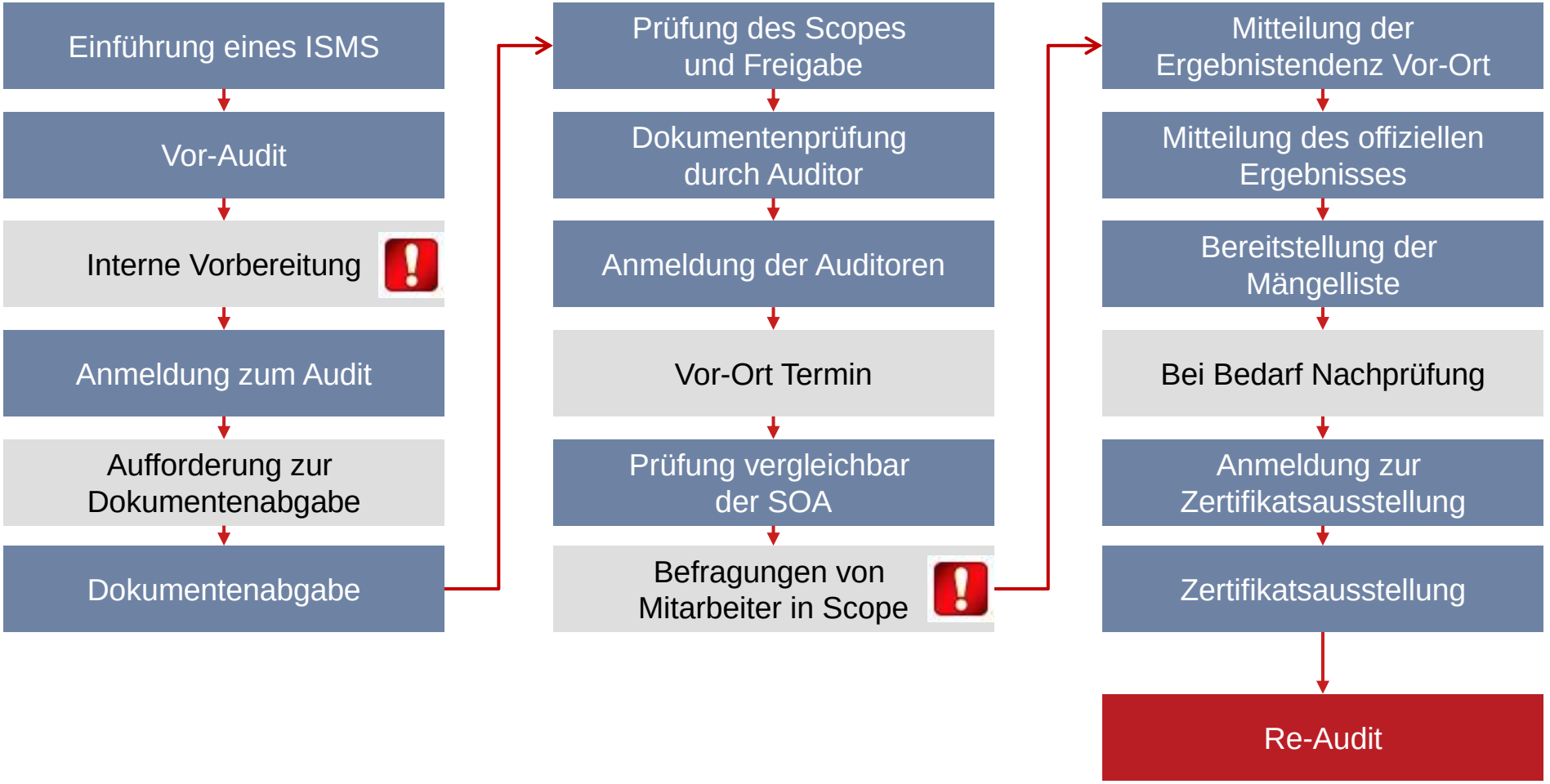
Messerscharfer Verstand

Wir

Gewisse Gelassenheit

Der Auditor hat Recht ☺ IMMER!

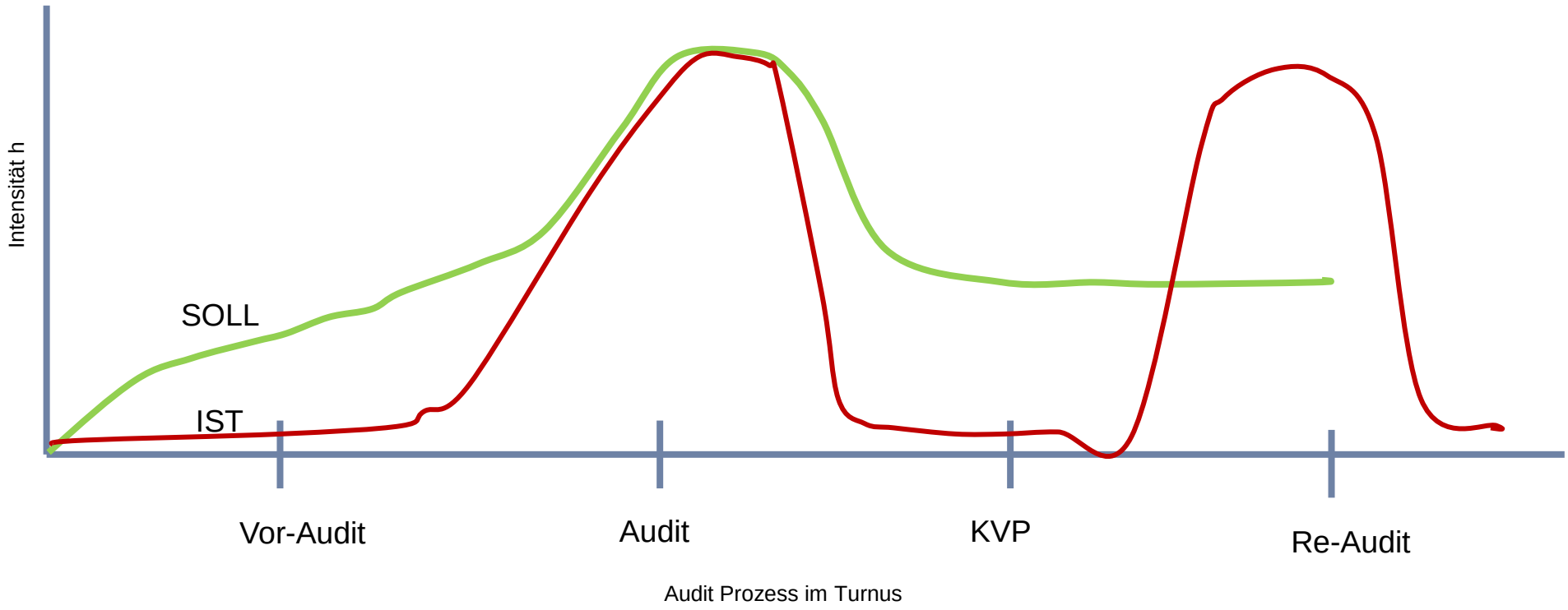
Der Ablauf eines Audit



* Legende= Team involviert

Wodurch entsteht Zeitstress ?

Kein gelebtes, kontinuierliches ISMS → Zeitstress



Weiterer Austausch später gerne in der Pause …

Viel Erfolg!

Gudula Küsters

Telefon: +49 171 4778600
E-Mail: gudula.kuesters@ITunlimited.de

IT unlimited AG
Otto-Lilienthal-Straße 36
71034 Böblingen
www.ITunlimited.de