SÜD IT
Security & Mittelstand

ISO 27001 Zertifizierung

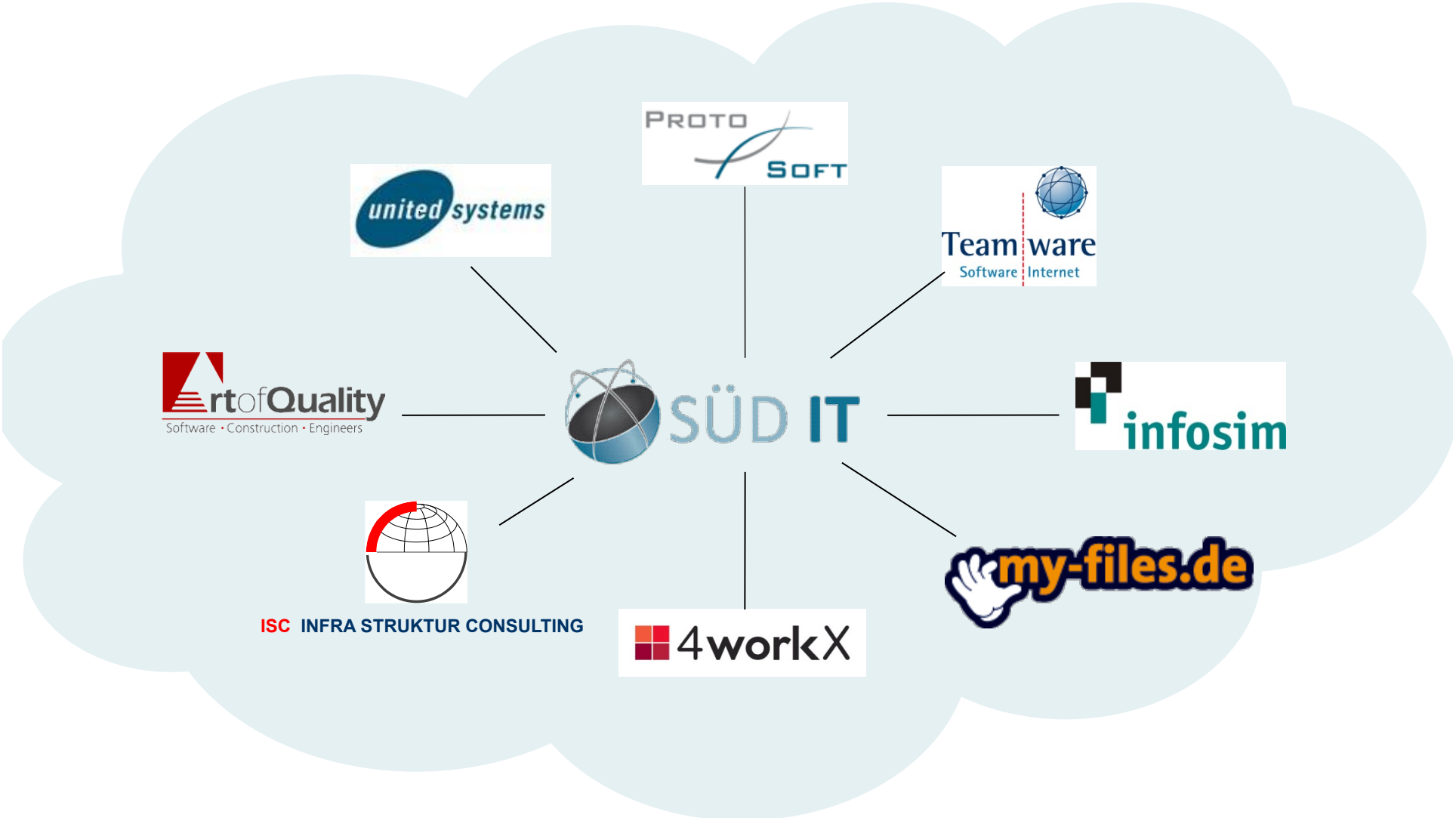
Motivation – Inhalte – Ablauf – Aufwände – Ergebnisse

Dr. Stefan Krempl, ISO 27001 Lead-Auditor, Datenschutzbeauftragter
krempl@sued-it.de

Süd IT AG - Stahlgruberring 11 - 81829 München Tel. 089 / 461 35 05 -12

SÜD IT
Security & Mittelstand

SÜD IT AG - Die Mitglieder sind Spezialisten



SÜD IT
Security & Mittelstand

ISO 27001 Zertifizierung

Motivation – Inhalte – Ablauf – Aufwände – Ergebnisse

SÜD IT
Security & Mittelstand

Motivation - bei Projektbeginn

- Erhöhen der eigenen Sicherheit
- Kundenforderung
- Wettbewerbsvorteil durch TÜV-Zertifizierung als Marketing-Argument
- Erfüllen gesetzlicher Vorschriften (KonTraG, Basel II, KRITIS)

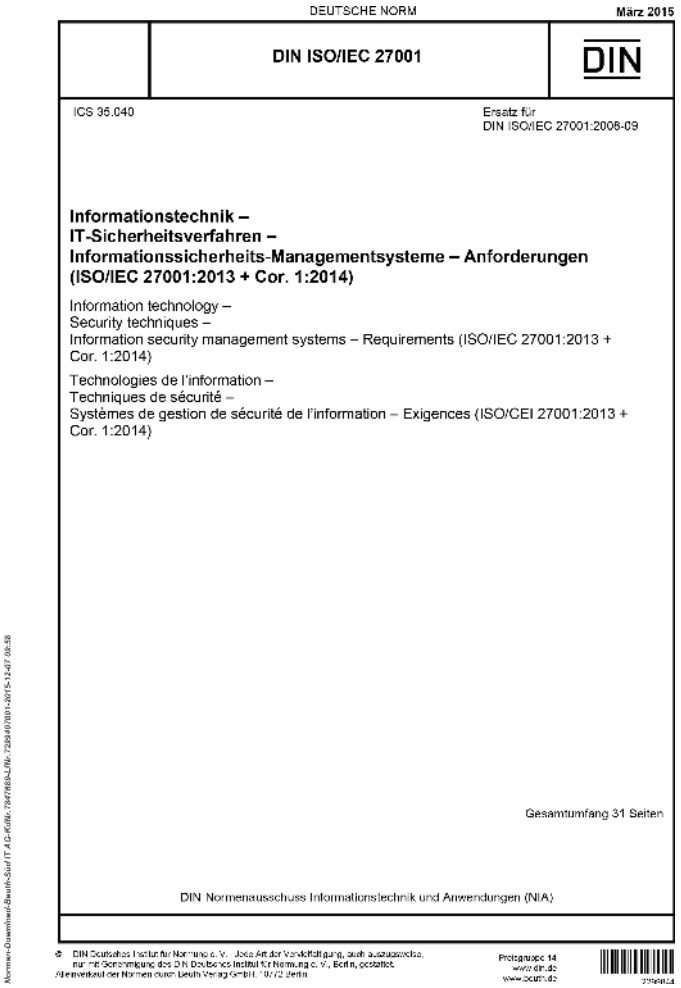
ISO 27001 Zertifizierung

Motivation – **Inhalte** – Ablauf – Aufwände – Ergebnisse

SÜD IT
Security & Mittelstand

Was ist die ISO/ISO27001

- Internationaler Standard nach dem Informationssicherheits-Management-Systeme zertifiziert werden können
- Vergleichbar zur ISO 9001 - jedoch Informationssicherheits- statt Qualitätsmanagement
- Beschreibt notwendige Dokumente, Prozesse und Maßnahmen die für eine Zertifizierung erforderlich sind



DEUTSCHE NORM März 2015

DIN ISO/IEC 27001

DIN

ICS 35.040

Ersatz für
DIN ISO/IEC 27001:2008-09

Informationstechnik –
IT-Sicherheitsverfahren –
Informationssicherheits-Managementsysteme – Anforderungen
(ISO/IEC 27001:2013 + Cor. 1:2014)

Information technology –
Security techniques –
Information security management systems – Requirements (ISO/IEC 27001:2013 + Cor. 1:2014)

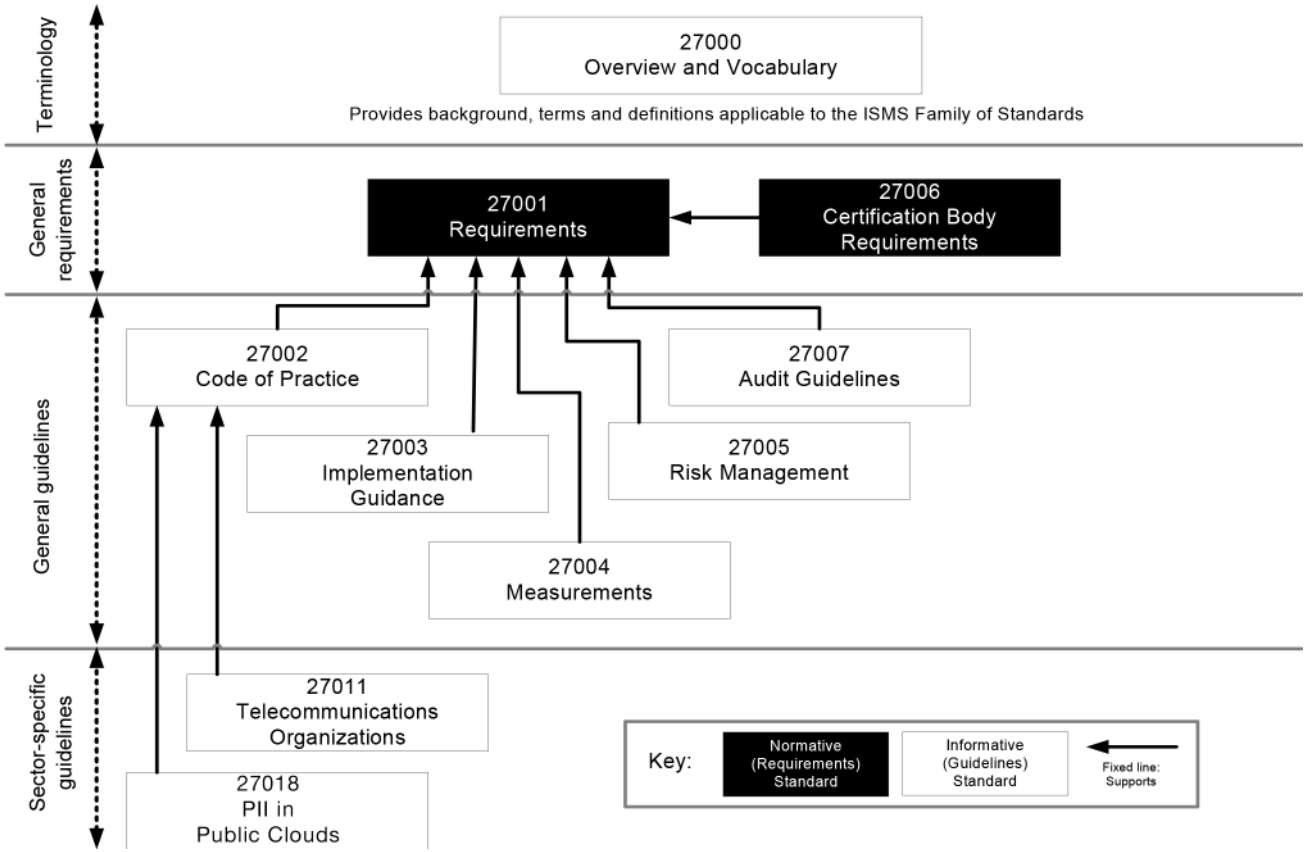
Technologies de l'information –
Techniques de sécurité –
Systèmes de gestion de sécurité de l'information – Exigences (ISO/CEI 27001:2013 + Cor. 1:2014)

Gesamtumfang 31 Seiten

DIN Normenausschuss Informationstechnik und Anwendungen (NIA)

SÜD IT
Security & Mittelstand

Standard Familie



SÜD IT
Security & Mittelstand

ISO/IEC 27001:2013 – Haupt-Teil

1. Anwendungsbereich
2. Normative Verweisungen
3. Begriffe
4. Kontext der Organisation
5. Führung
6. Planung (incl. Risikomanagement)
7. Unterstützung
8. Betrieb
9. Bewertung der Leistung
10. Verbesserung

SÜD IT
Security & Mittelstand

ISO/IEC 27001:2013 - Anhang A

115 Maßnahmenziele bzw. Controls in 14 Abschnitten

- A.5 Informationssicherheitsrichtlinien
- A.6 Organisation der Informationssicherheit
- A.7 Personalsicherheit
- A.8 Verwaltung der Werte
- A.9 Zugangssteuerung
- A.10 Kryptographie
- A.11 Physische und umgebungsbezogene Sicherheit
- A.12 Betriebssicherheit
- A.13 Kommunikationssicherheit
- A.14 Anschaffung, Entwicklung und Instandhalten von Systemen
- A.15 Lieferantenbeziehungen
- A.16 Handhabung von Informationssicherheitsvorfällen
- A.17 Informationssicherheitsaspekte beim Business Continuity Management
- A.18 Compliance

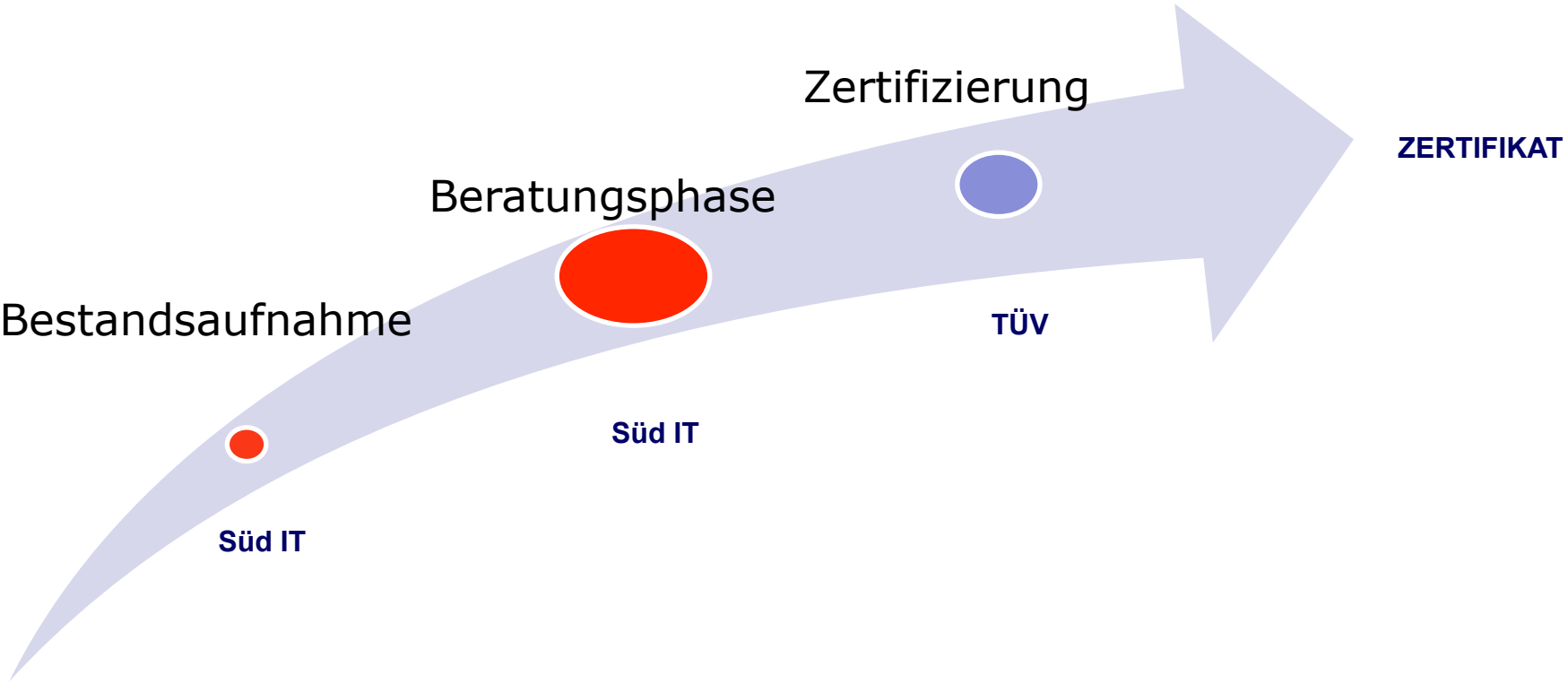
SÜD IT
Security & Mittelstand

ISO 27001 Zertifizierung

Motivation – Inhalte – **Ablauf** – Aufwände – Ergebnisse

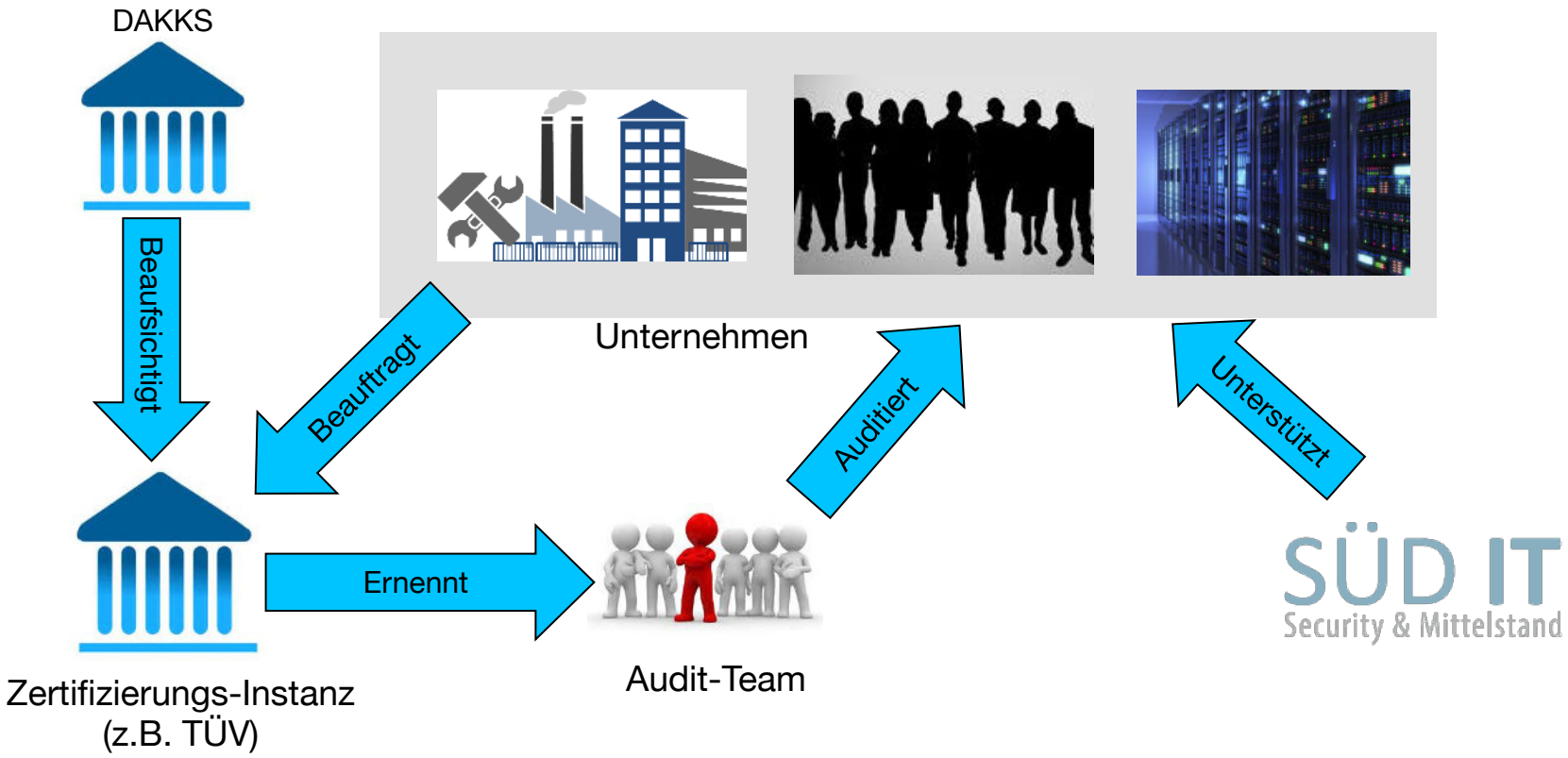
SÜD IT
Security & Mittelstand

Der Weg zur ISO27001 Zertifizierung



SÜD IT
Security & Mittelstand

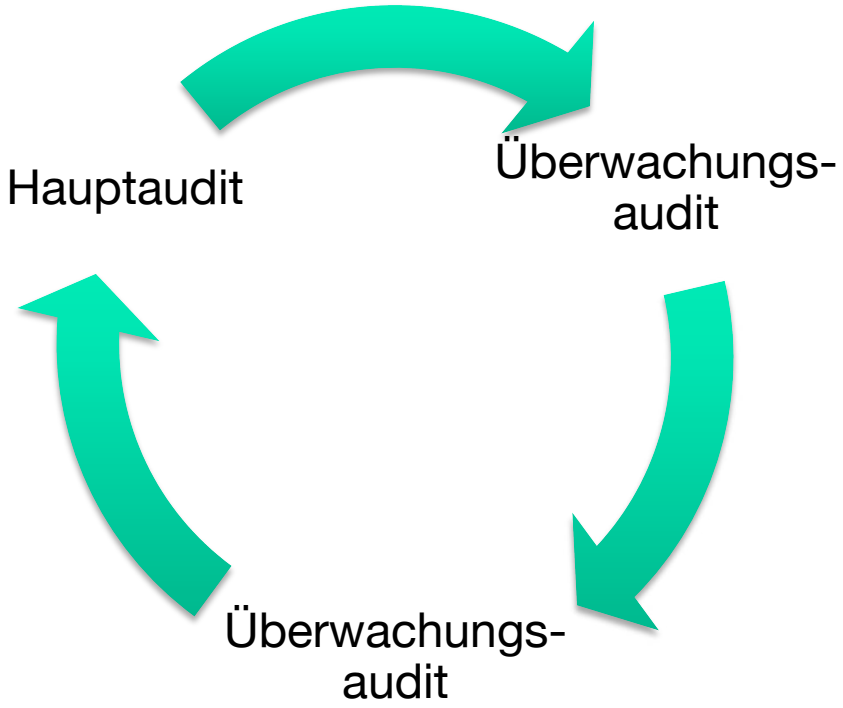
Beteiligte am Zertifizierungsprozess



SÜD IT
Security & Mittelstand

SÜD IT
Security & Mittelstand

3-jährlicher Zertifizierungszyklus



SÜD IT
Security & Mittelstand

Schritt 1 – Workshop Kompaktanalyse

Die Kompaktanalyse erfolgt durch Interviews und Dokumentenprüfungen anhand von Checklisten und einer Besichtigung der Infrastruktur.

Als Ergebnis der Kompaktanalyse erhalten Sie

- Beurteilung der Informationssicherheit Ihres Unternehmens
- Liste der Abweichungen gegenüber der Forderungen der Norm.
- Abschätzung der zu erwartenden Aufwände bis zu einer Zertifizierung.

Schritt 2 – Planung und Umsetzung eines ISMS

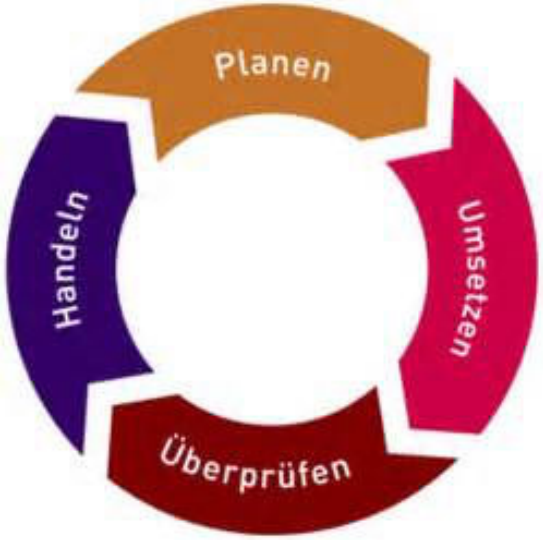
Ein ISO/IEC 27001 konformes **I**nformation **S**ecurity **M**anagement **S**ystem (ISMS) besteht aus

- Prozessen,
- Verfahren und Regeln,
- Infrastrukturmaßnahmen sowie
- Dokumenten und Aufzeichnungen.

Als erfahrene Auditoren wissen wir genau worauf es ankommt. Wir zeigen Ihnen als "Bergführer" den besten Weg und tragen als "Sherpa" einen Teil der Last. Dabei stellen wir sicher, dass die Forderungen der Norm ohne unnötigen Ballast erfüllt werden.

Schritt 3 – Pflege und Verbesserung

- Die ISO/IEC 27001:2013 erfordert ein gelebtes ISMS. D.h. der minimale Umsetzungszeitraum bis zur Zertifizierung beträgt mindestens 9 Monate.
- Die kontinuierliche Pflege und Verbesserung erfolgt nach der Einführung im Rahmen des täglichen Geschäftes.
- Wir unterstützen Sie bei der Planung und Umsetzung eines kontinuierlichen Verbesserungsprozesses oder unterstützen Sie auch kontinuierlich mit kompetenten Mitarbeitern.



Schritt 4 – Interne Audits

Die geplante Durchführung von internen Audits ist Teil der Norm-Forderungen und soll durch externe Mitarbeiter erfolgen. Unabhängig von den vorhergegangenen Schritten führen wir bei Ihnen interne Audits durch, mit denen Sie optimal auf eine Zertifizierung vorbereitet werden.

Schritt 5 – Begleitung bei der Zertifizierung

Die Zertifizierung erfolgt durch eine unabhängige Zertifizierungsinstanz, wie z.B. TÜV, DQS oder DEKRA. Sie erfolgt für jeweils 3 Jahre mit jährlichen Überwachungsaudits.

Die Mitarbeiter der SÜD IT sind selbst erfahrene Auditoren und teilweise für den TÜV tätig. Sie unterstützen Sie bei der Auswahl eines geeigneten Zertifizierers und begleitet Sie sicher durch den Haupt- oder Überwachungsaudit.

SÜD IT
Security & Mittelstand

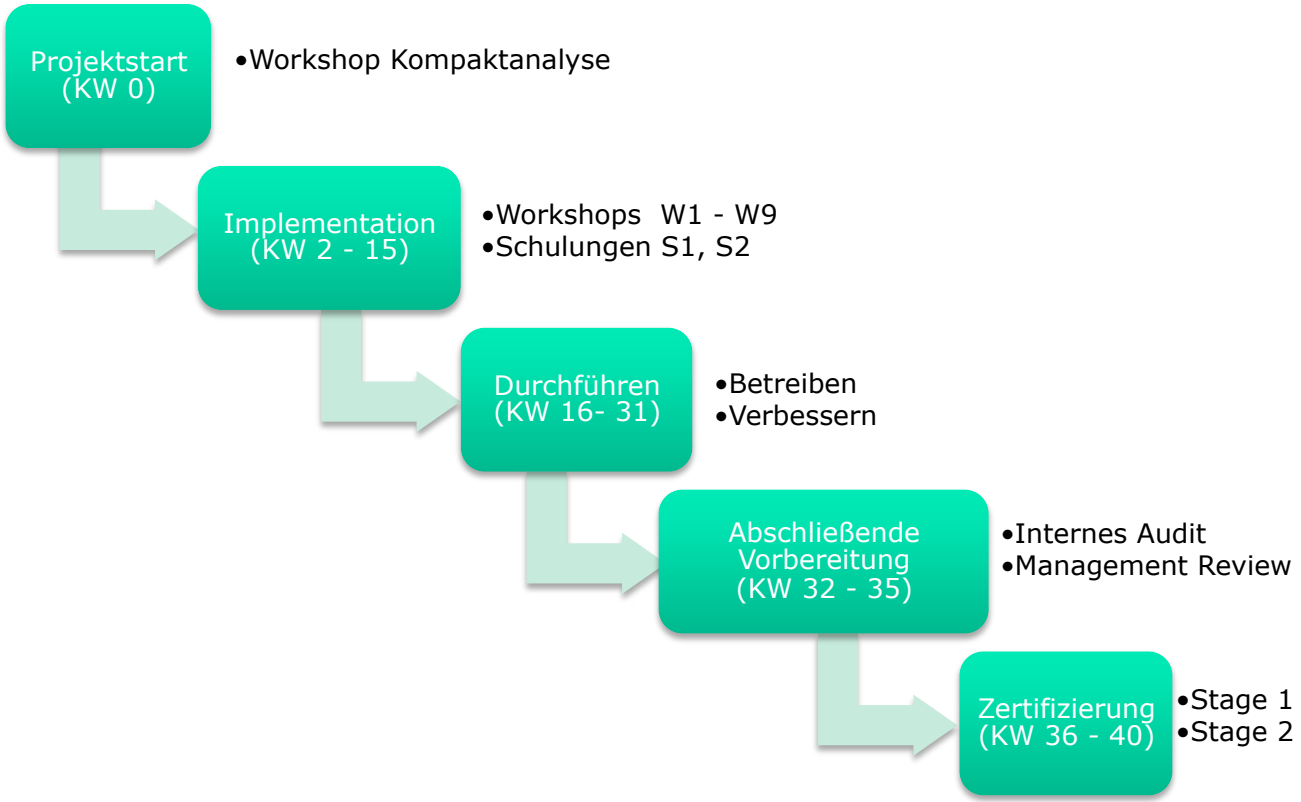
SÜD IT AG – Security & Mittelstand

ISO 27001 Zertifizierung

Motivation – Inhalte – Ablauf – **Aufwände** – Ergebnisse

SÜD IT
Security & Mittelstand

Projektplan



SÜD IT
Security & Mittelstand

Typische Aufwände

- Interne Aufwände
  - 20 – 200 Tage
- Beratungsaufwand
  - 10 – 80 Tage
  - 1 Beratungstag für ca. 2 – 3 interne Tage
  - Die meisten Projekte liegen zwischen 20 und 30 Beratungstagen
- TÜV / Zertifizierer
  - Stage 1 + Stage 2 ab 1,5 Tage abhängig von der Anzahl der Beschäftigten im Geltungsbereich

SÜD IT
Security & Mittelstand

ISO 27001 Zertifizierung

Motivation – Inhalte – Ablauf – Aufwände – **Ergebnisse**

SÜD IT
Security & Mittelstand

Interne Ergebnisse

- Transparenz der Risiken
- Transparenz von (IT-)Prozessen
- Erhöhtes Sicherheitsbewusstsein bei allen Mitarbeitern

SÜD IT
Security & Mittelstand

Externe Ergebnisse

- Erfüllen von Kundenanforderungen
- Marketinginstrument
- Vereinfachte Beauftragung bei Auftragsdatenverarbeitung (§11 BDSG)

SÜD IT
Security & Mittelstand

Referenzen

Vielen Dank für Ihre Aufmerksamkeit!

Dr. Stefan Krempl

Vorstand Süd-IT AG,

ISO 27001 Lead-Auditor, Datenschutzbeauftragter

Tel.: 0175 221 4287
Email: krempl@sued-it.de

Süd IT AG
Stahlgruberring 11
81829 München