ERPvisors
Excellence in IT
a TMG Consultants company

IT-Sicherheitskonzepte als Risikominimierer

ERPvisors-Impulspapier

Wie können Sie Ihre IT-Lücken identifizieren und beheben?

Warum braucht man ein IT-Sicherheitskonzept?

Ohne ganzheitliches Risikokonzept geht in Zukunft nichts mehr

ERPvisors
Excellence in IT
a TMG Consultants company

IT-Sicherheitsstrategie

Konzeption des Informationssicherheitssystems und der -konzepte (ISMS)
z. B.
ISO 27001
TISAX®

Umsetzung der Standards als Fundament

Warum sollte man sich mit einem IT-Sicherheitskonzept beschäftigen?

- Lückenhafte Sicherheitskonzepte führen zu hohem Schaden
- Vielseitige Angriffe auf die IT-Infrastruktur sind identifizierbar
- Frequenz der IT-Angriffe steigt an
- Digitalisierte Geschäftsmodelle haben Konsequenzen auf die IT-Sicherheit
- Ansteigende Sicherheitsregularien
- IT-Sicherheitsstandards schaffen Kostenreduktionen

Zur Bewältigung der zukünftigen Herausforderungen ist ein ganzheitliches Risikokonzept unbedingt erforderlich, das Maßnahmenpläne umsetzbar macht und Transparenz gegenüber IT-Sicherheitslücken schafft.

Vorteile der ISO 27001

Warum ein umfassendes Informationssicherheitssystems essenziell ist

ERPvisors
Excellence in IT
a TMG Consultants company

Portfolio der ERPvisors „P³+M“

Bezugspunkte und Einordnung in das Produktportfolio von ERPvisors

ERPvisors
Excellence in IT
a TMG Consultants company

Plan
Strategien und Ansätze

- Vorstudien/Machbarkeitsstudien
- **IT-Strategie**
- IT-Organisation
- **IT-Sicherheitskonzepte**
- ERP-Einführung & Rollout-Strategie
- ERP-/Systemauswahl
- S/4HANA Setup

Prepare
Prozessberatung

- Vertrieb
- SCM / Operations
- FI/CO
- Einkauf
- Service
- Human Resources
- Master Data Management
- ...

Perform
Implementierungsunterstützung

- SAP Implementierung
- Test Management
- CutOver Management
- Datenbereinigung und -migration
- **Informations- und Datensicherheit**
- Berechtigungsmanagement
- Rollout-Management
- Hypercare

Manage
Programm und Projekt-management

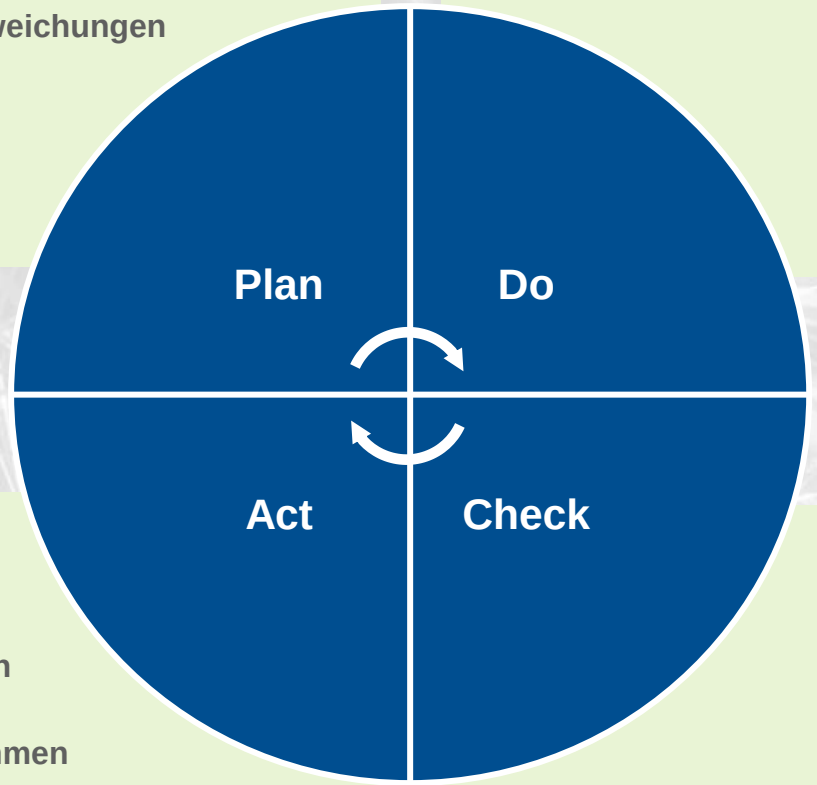
- **Projekt- und Programmleitung**
- **Project Management Office**
- Project Office
- Change Request Management
- Steuerung von Implementierungsressourcen (intern/extern)

Der PDCA-Cycle als Grundstruktur

Leitplanken für die Einführung eines ISMS

ERPvisors
Excellence in IT
a TMG Consultants company

- Ersteinschätzung der Ist-Situation
- Planfestlegung und Identifikation von Plan-Ist-Abweichungen
- Erstellung eines Fahrplans mit den Kernfragen
- Planalternativen aufsetzen und priorisieren



- Verwirklichung der ausgewählten Planalternative
- Durchführung von Szenarioanalysen
- Diskursive Betrachtung der Ergebnisse
- Bereitstellung der notwendigen Ressourcen

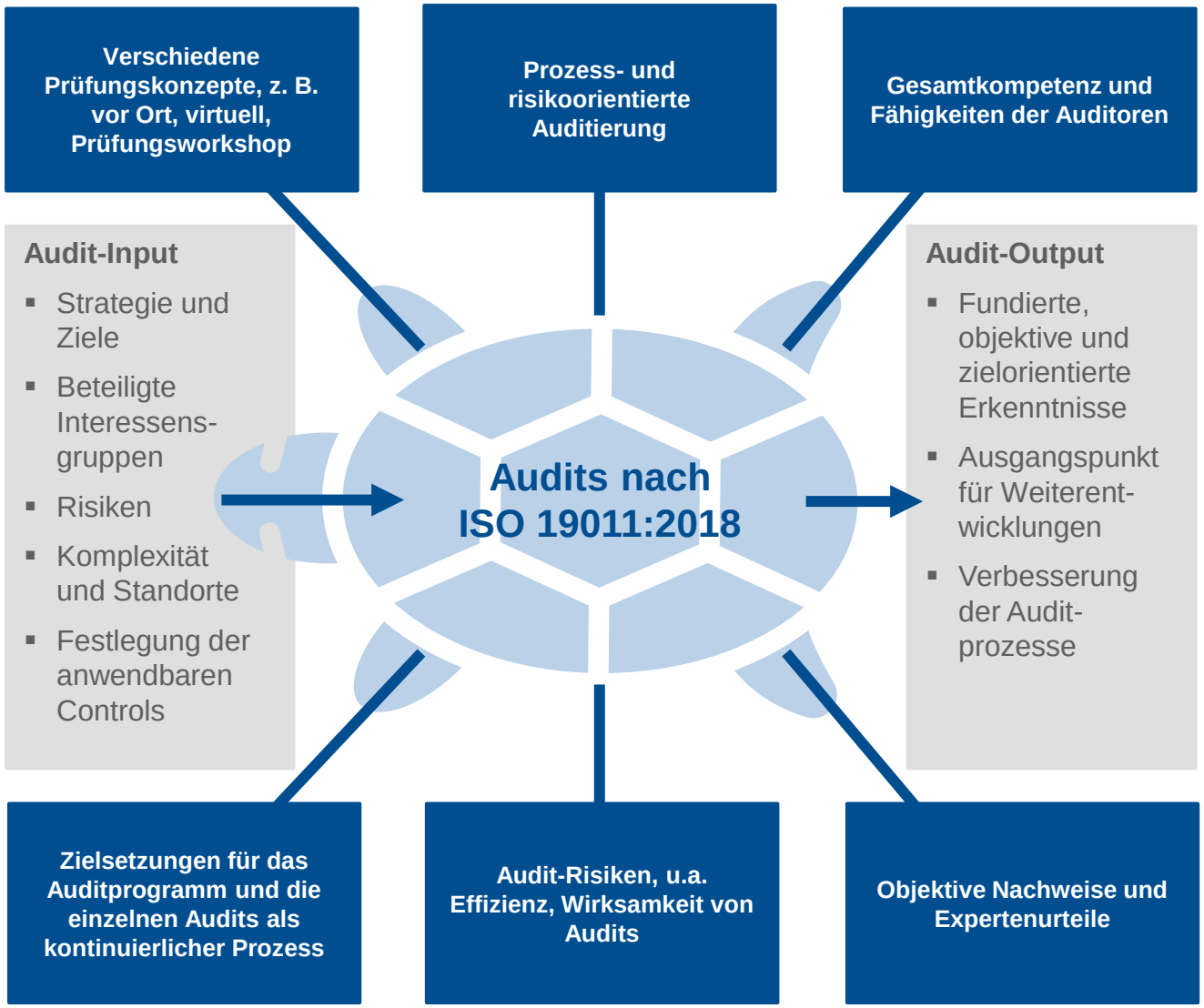
- Übertragung der Erkenntnisse auf das Gesamtprojekt
- Frühzeitige Anpassungen fördern und unterstützen
- Reflexion und Evaluierung der realisierten Maßnahmen und Vorgehensweisen
- Identifikation und Bewertung von Optimierungen

- Überprüfung der Maßnahmen und Abgleich mit dem Meilensteinplan
- Abweichungsanalysen durchführen
- Ableitung von Korrekturmaßnahmen und Früherkennungssystemen
- Durchführung interner Audits

Leitfaden zur Auditierung von Managementsystemen

Wir unterstützen Sie mit bewährten und fundierten Konzepten und Methodiken

ERPvisors
Excellence in IT
a TMG Consultants company



Ausmaß der Zusammenarbeit zwischen dem Prüfer und der geprüften Stelle	Standort des Auditors	
	Vor Ort	Remote
Mit menschlicher Interaktion	Durchführen von Interviews Ausfüllen von Checklisten und Fragebögen unter Beteiligung der zu auditierenden Organisation Durchführung einer Dokumentenprüfung (Stichprobenerhebung)	Über interaktive Kommunikationsmittel: ▪ Durchführung von Interviews ▪ Ausfüllen von Checklisten und Fragebögen ▪ Durchsicht von Dokumenten unter Beteiligung der geprüften Person
Ohne menschliche Interaktion	Überprüfung von Dokumenten (z. B. Aufzeichnungen, Daten-analyse) Beobachtung der durchge-führten Arbeiten (Screening) Ausfüllen von Checklisten Stichprobenerhebung (z. B. von Produkte)	Überprüfung von Dokumenten (z. B. Aufzeichnungen, Datenanalyse) Beobachtung der geleisteten Arbeit durch Überwachungs-maßnahmen unter Berücksichtigung sozialer und rechtlicher Anforderungen Analyse von Daten

Vor-Ort-Prüfungen werden am Standort der geprüften Stelle durchgeführt. Remote-Audittätigkeiten werden, ungeachtet der Entfernung, an jedem beliebigen Standort durchgeführt, außer an dem zu auditierenden Standort. Interaktive Audittätigkeiten schließen die Interaktion zwischen dem Personal der zu auditierenden Organisation und dem Auditteam ein. Nicht-interaktive Audittätigkeiten schließen keine menschliche Interaktion mit ein, sondern nur die Kommunikation zwischen den vorhandenen Systemen.

Phasen des ISO-Zertifizierungsprozesses

ERPvisors unterstützt Sie in allen Projektphasen der ISO-Zertifizierung

ERPvisors
Excellence in IT
a TMG Consultants company

Vorbereitungs-phasen

1 Gap-Analyse

- Welche Gaps lassen sich prinzipiell in Ihrer IT identifizieren?
- Wie sind die Gaps zu systematisieren?

2 Gap-Disclosure

- Wie lassen sich die identifizierten IT-Lücken schließen?
- Welche Maßnahmen sind in welcher Priorisierungsklasse durchzuführen?

3 Initialisierung der Zertifizierung

- Welche Abstimmungsprozesse sind mit der Zertifizierungsstelle vorzunehmen?
- Welche Themenfelder sind noch vor dem Zertifizierungsprozess zu klären?

4 Erst-Zertifizierung

- Welche Phasen werden in der Erstzertifizierung unterschieden?
- Welche Ressourcen werden für die Erstzertifizierung benötigt?

5 Jährliches Überwachungs-audit 1 & 2

- Wann finden die Überwachungsaudits statt?
- Welche Regulatorien haben sich geändert?
- Sind ggf. Feinjustierungen notwendig?

6 Re-Zertifizierung

- Ab welchem Zeitpunkt ist eine Rezertifizierung erforderlich?
- Erscheint eine Rezertifizierung überhaupt sinnvoll? Welchen Mehrwert stiftet sie?

Um den zweiten Teil des Zertifizierungsprozesses zielorientiert zu gestalten, ist eine professionelle und strukturierte Vorbereitung notwendig. Ziel dieser Vorbereitungsphasen muss es sein, alle relevanten Lücken zu schließen.

Vorgehen bei der Phase I: Gap-Analyse

Ein effizientes Verfahren für eine strukturierte Lückenanalyse

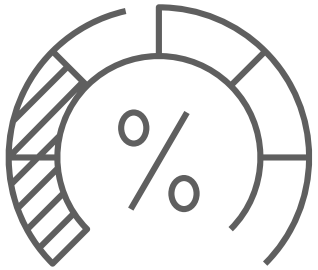
ERPvisors
Excellence in IT
a TMG Consultants company

Auszug

Strukturierte Ist-Analyse

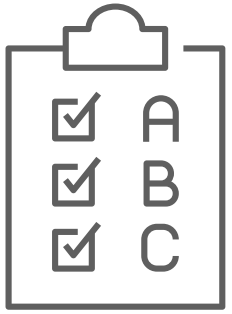
- Überprüfung der bisherigen Vorlagen, Fragebögen und Dokumentationen
- Gezielte Fragestellungen auf Basis von Projekterfahrungen
- Zusammenstellung aller relevanten Projektparameter
- Plausibilitätsprüfung
- Dokumentation der Ergebnisse

Kundenadjustierte Optimierung der Gap-Analyse



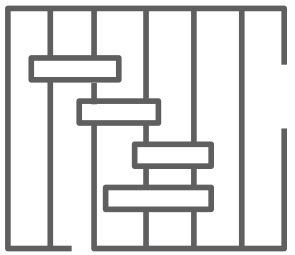
- Erstellung und Optimierung der verfügbaren Gap-Analyse-Templates
- Prüfung möglicher Ver-besserungen: Best-Practice- vs. Trade-off-Lösungen (Abwägung zwischen Kosten und Nutzen sowie obliga-torisch und optional)
- Schaffung von Transparenz
- Dokumentation d. Ergebnisse

Durchführung der Gap-Analyse



- Durchführung der Bewertung mithilfe von Analyse-Tools
- Umsetzung der zuvor entwickelten Schritte mit Kategorisierung
- Priorisierung der Ergebnisse: Quick Wins und Langläufer (insb. vor dem Hintergrund der Timeline)
- Dokumentation der Ergebnisse

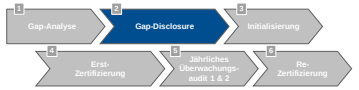
Ausarbeitung eines Umsetzungsplans für die nächsten Projektphasen



- Erstellung einer Roadmap für die Maßnahmen unter Berücksichtigung von:
  - Zeit
  - Ressourcen & Kosten
  - Qualität
- Abstimmung mit dem Gesamt-plan und den Gesamtzielen
- Priorisierung zwischen obligatorischen und optionalen Handlungsfeldern
- Dokumentation d. Ergebnisse

Vorgehen in der Phase II: Gap-Disclosure

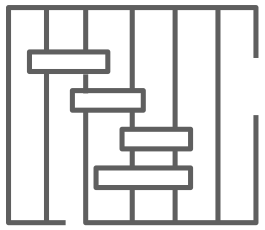
Effizienter Ansatz für eine strukturierte Offenlegung von Lücken



ERPvisors
Excellence in IT
a TMG Consultants company

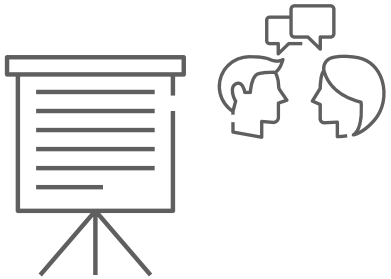
Auszug

Strukturierung und Präzisierung der Handlungsfelder



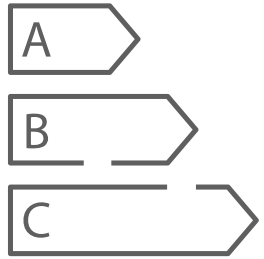
- Ausgangspunkt sind die Ergebnisse aus der Gap-Analyse
- Aufstellung eines Detailplans für die Gap-Disclosure-Phase, unterstützt mit Tools, z. B. JIRA
- Einhaltung und Umsetzung der Priorisierung von Einzelmaßnahmen: obligatorisch vs. optional

Koordinierung und Terminplanung mit dem Produktverantwortlichen



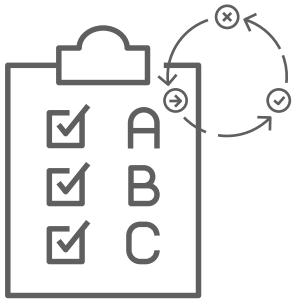
- Koordination der Maßnahmen mit dem Product Owner
- Verwendung unterschiedlicher Projektmanagement-methoden, z. B. SCRUM und KANBAN
- Transparenz und Commitment etablieren
- Dokumentation der Ergebnisse

Umsetzung der Maßnahmen



- Umsetzung des Maßnahmenplans
- Regelmäßige Abstimmung mit den Product Ownern
- Etablierung von Regel-terminen
- Anwendung von Früherkennungsmehtoden
- Dokumentation der Ergebnisse

Nachweise und Berechtigungskonzepte



- Inspektion und Abnahme der Umsetzung
- Falls erforderlich: Zusätzliche Verbesserungen veranlassen, um die Anforderungen rechtzeitig zu erfüllen
- Dokumentation der Ergebnisse
- Verbesserungspotenziale für künftige Zertifizierungs-projekte erarbeiten

Erstbeurteilung durch einen IT-Security Scan

Identifikation der Handlungsfelder zur Verbesserung der IT-Security

ERPvisors
Excellence in IT
a TMG Consultants company

Vorbereitung

Vorbereitung und Bereitstellung der relevanten Informationen zu den relevanten Themenfeldern

Woche 1

Montag	Dienstag	Mittwoch	Donnerstag	Freitag
Kick-off	Status-quo-Analyse Interviews	Status-quo-Analyse Interviews / Sichtung von Unterlagen	Reflektion Ergebnisse Vortag	Reflektion Ergebnisse Vortag
			Status-quo-Analyse Workshop	Feedback der Erstauswertung Workshop
Interviews Geschäftsführung und -leitung	Konsolidierung Ergebnisse			
		Konsolidierung Ergebnisse	Konsolidierung Ergebnisse	Konsolidierung Ergebnisse

Woche 2

Montag	Dienstag	Mittwoch	Donnerstag	Freitag
Reflektion Ergebnisse Vortag	Reflektion Ergebnisse Vortag	Reflektion Ergebnisse Vortag	Reflektion Ergebnisse Vortag	Ergebnis-präsentation
Potenzialanalyse Interviews	Potenzialanalyse Workshop	Erarbeitung eines Aktionsplans Workshop	Konsolidierung und Aufbau Präsentation und des Projektabschlusses	Management Debriefing
Konsolidierung Ergebnisse	Konsolidierung Ergebnisse	Konsolidierung Ergebnisse		

Nachbereitung

Erstellung des Management-Reports und Ableitung weiterer Schritte.

Eine transparente Erstbeurteilung hilft, frühzeitig wichtige Handlungsfelder in der IT-Security zu identifizieren, um einen reibungslosen Zertifizierungsprozess sicherstellen zu können.

Ihr Kontakt

Dipl.-Ing.

Darya van de Sandt-Nassehi

Geschäftsführer

E-Mail: darya.nassehi@tmg.com
Mobil: +49 172 9 79 05 67

M.Sc.

Wojciech Bolesta

Geschäftsführer

E-Mail: wojciech.bolesta@erpvisors.com
Mobil: +49 172 2 85 34 72

www.erpvisors.com

ERPvisors GmbH

Königsallee 27 | 40212 Düsseldorf | Germany
Telefon +49 211 23855-213