Audit-Prozess in den Bereichen Industrieautomation und eingebettete Systeme

18. Juni 2013 | Roadshow Industrial IT Security | Michael Lecheler

"If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology" - Bruce Schneier

SCHUTZWERK

Die SCHUTZWERK GmbH ist ein unabhängiges und international tätiges Beratungsunternehmen.

Unsere Kernkompetenz liegt in der Prüfung sowie in der prozess- und konzeptbezogenen Optimierung der Bereiche IT-Sicherheit, Datenschutz und Unternehmenssicherheit.

Die ganzheitliche Stärkung technischer, organisatorischer und menschlicher Sicherheitsaspekte steht im Vordergrund unserer Dienstleistungen.

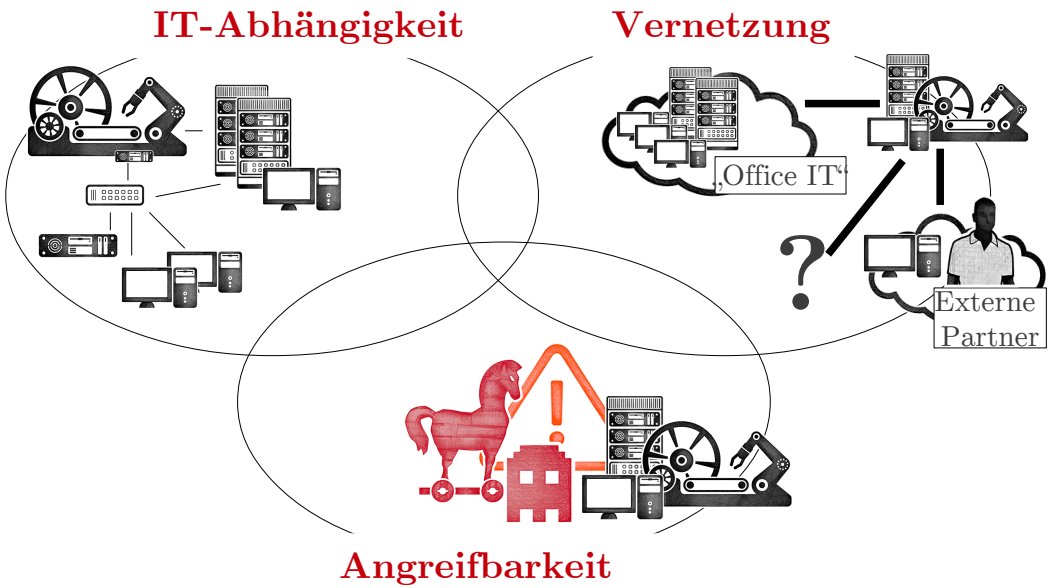
IT-Sicherheit...

... Übersicht erlangen

... Verfügbarkeit gewährleisten

... Verbindungen / Zugriffe reglementieren

... etc.



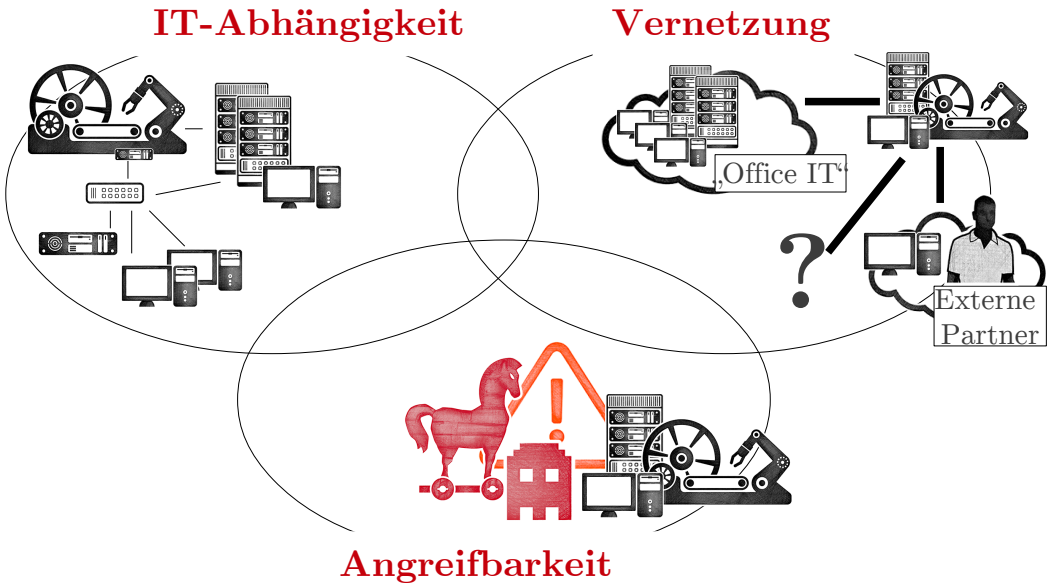
IT-Sicherheitsaudits...

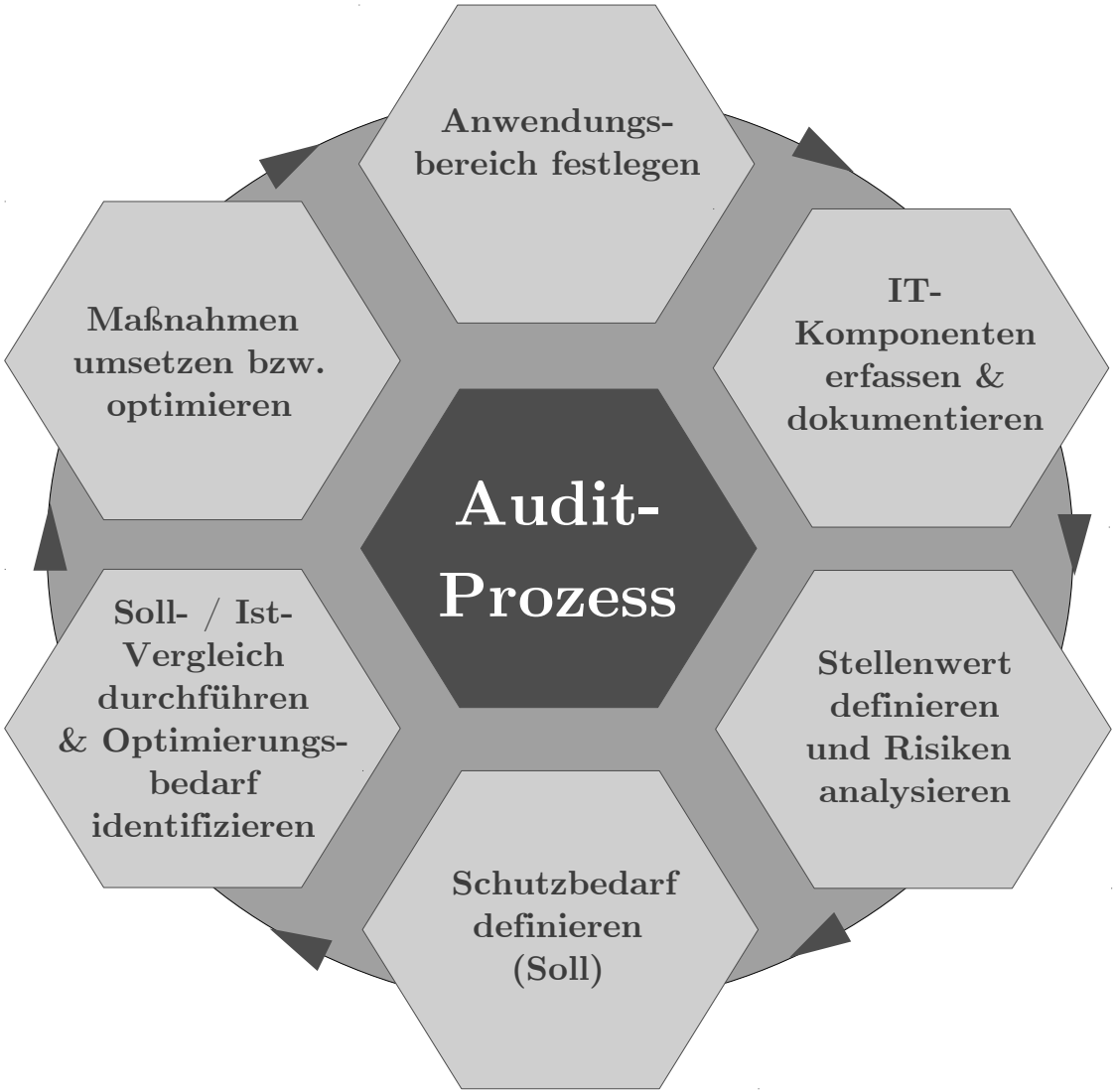
... schaffen die notwendige Transparenz (Soll-/Ist)...

... identifizieren notwendige Maßnahmen...

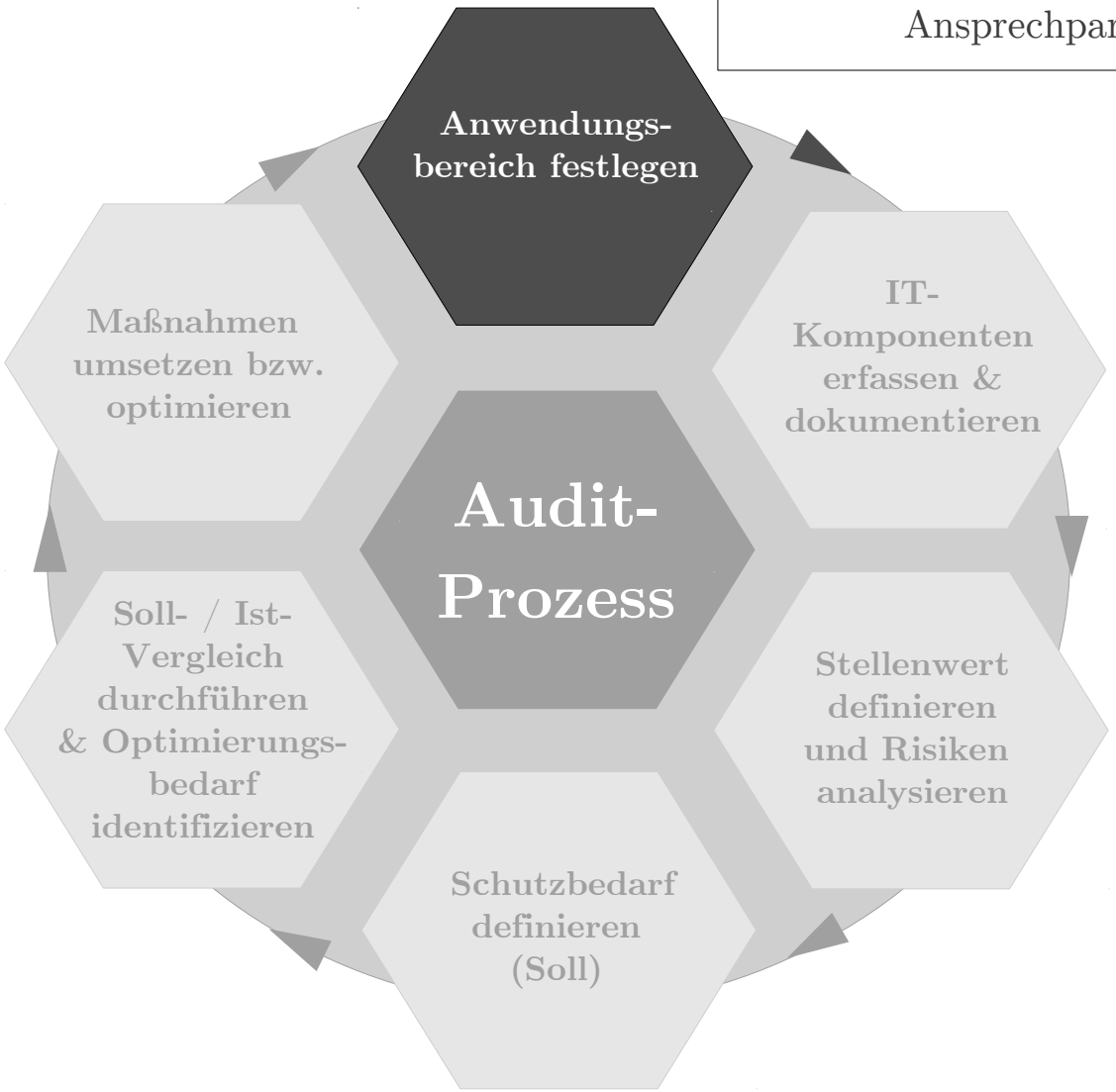
... und ermöglichen die Bewertung deren Angemessenheit!

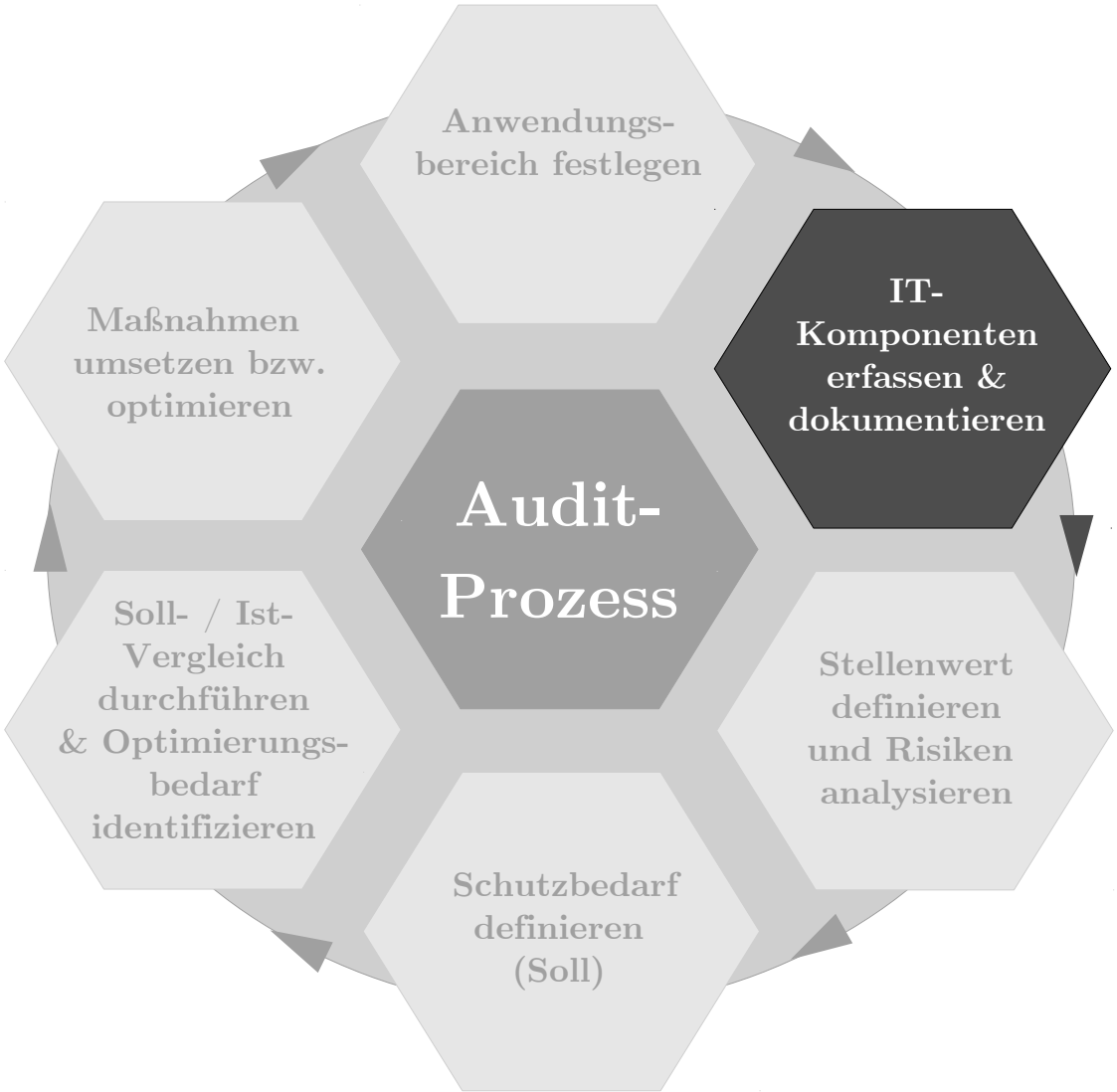
Ziele



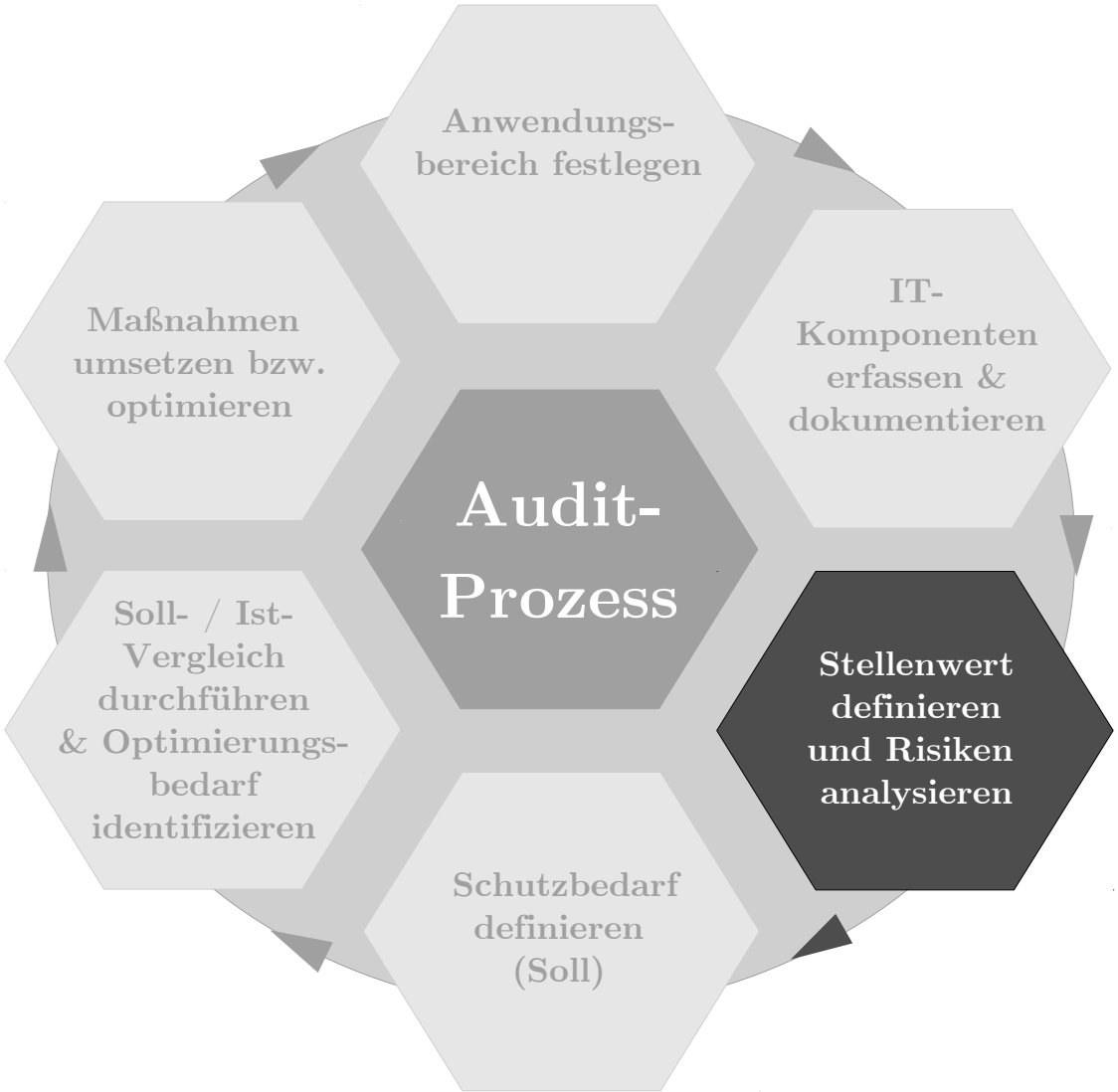

Anwendungs-
bereich festlegen
IT-
Komponenten
erfassen &
dokumentieren
Stellenwert
definieren
und Risiken
analysieren
Schutzbedarf
definieren
(Soll)
Soll- / Ist-
Vergleich
durchführen
& Optimierungs-
bedarf
identifizieren
Maßnahmen
umsetzen bzw.
optimieren
Audit-
Prozess

Untersuchungsobjekt definieren/ abgrenzen sowie Verantwortlichkeiten und Ansprechpartner festlegen

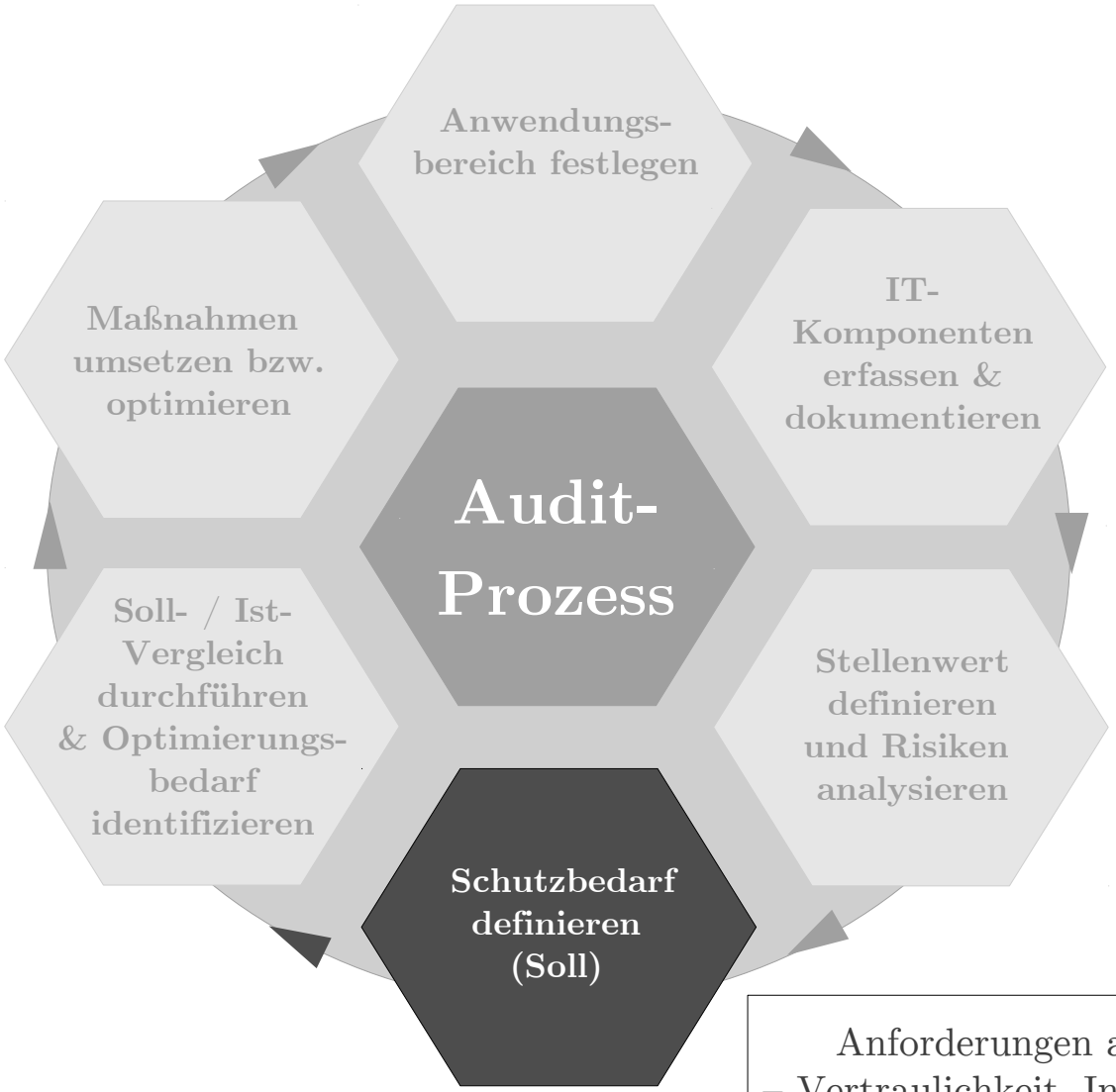




Zentrale Gesamtübersicht zu allen relevanten IT-Komponenten schaffen (Hard- und Software

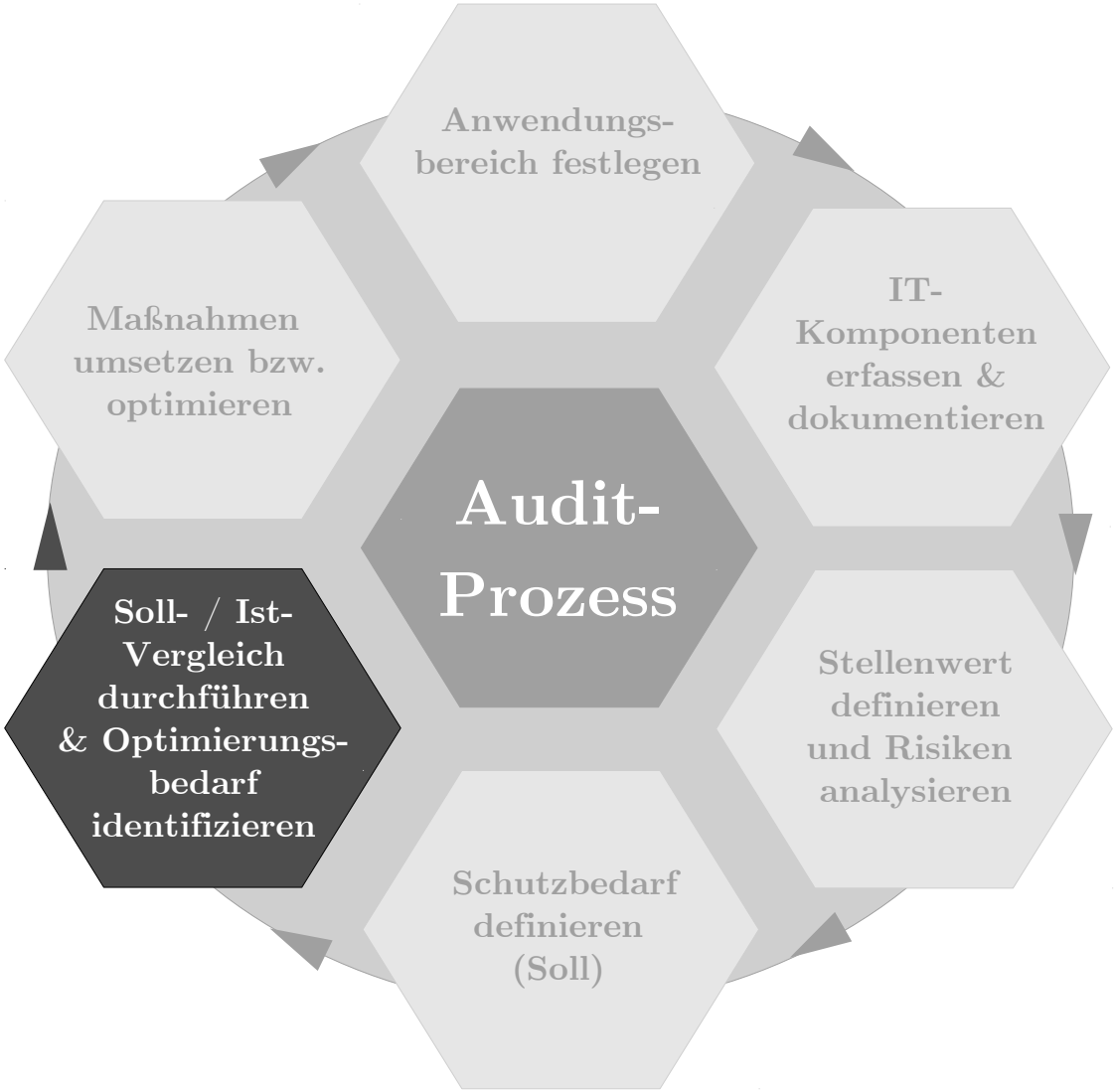


Stellenwert des Untersuchungsobjekts für die Geschäfts-prozesse und den Unternehmenserfolg ermitteln, Bedrohung erfassen und Risiken ableiten

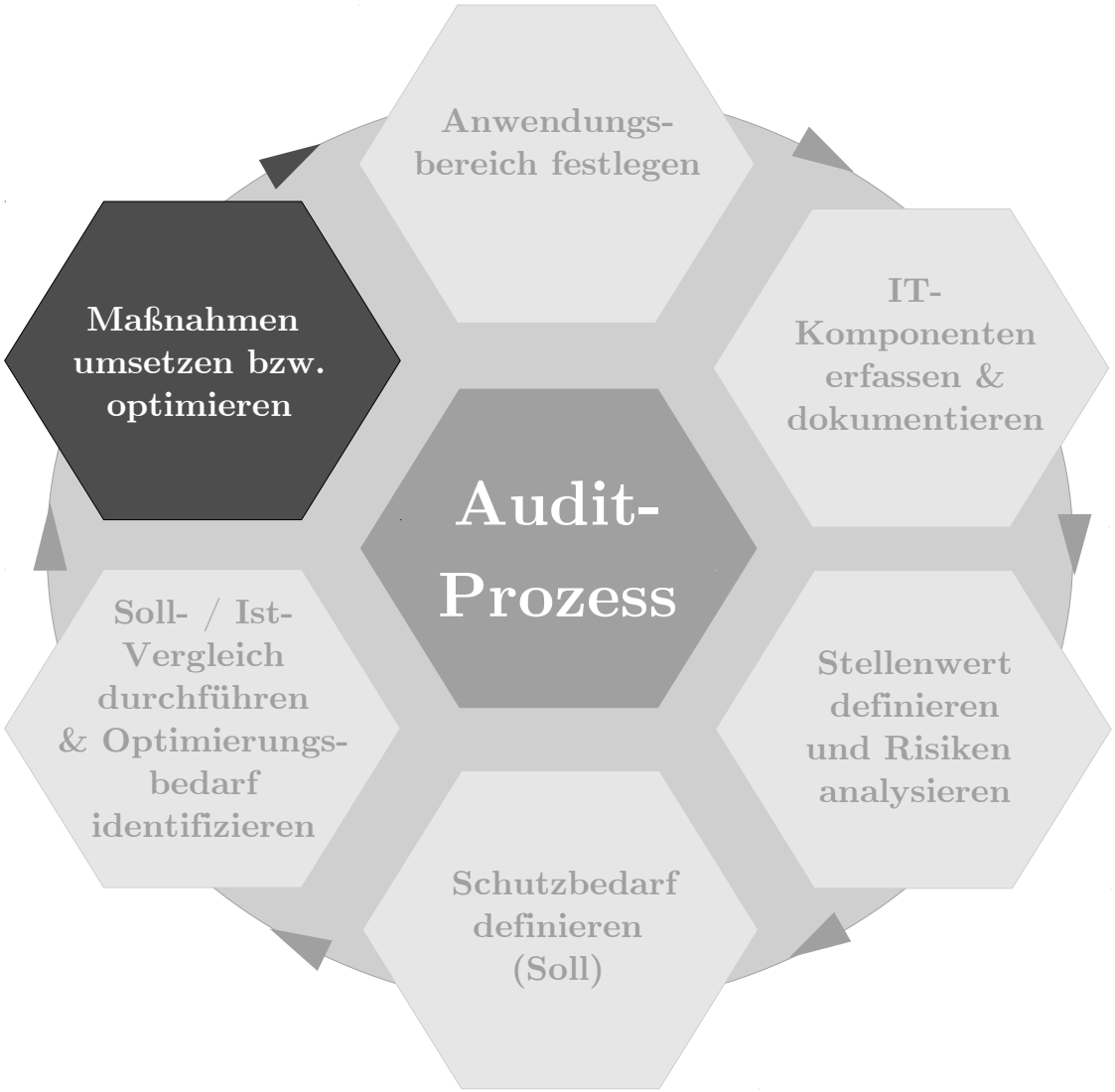


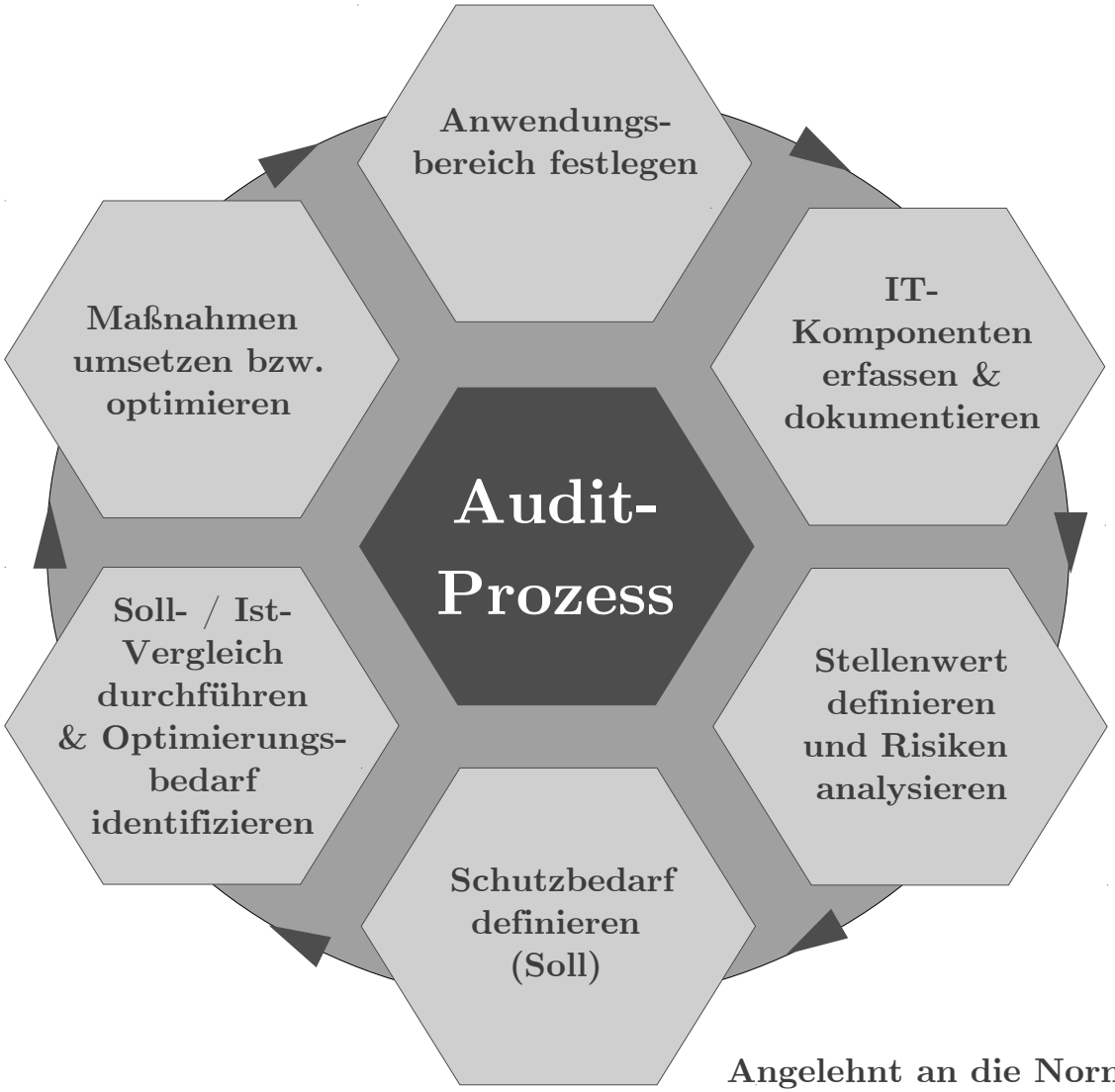
Anforderungen an die IT-Grundwerte
– Vertraulichkeit, Integrität, Verfügbarkeit –
festlegen

Ist-Zustand der IT-Sicherheit technisch und konzeptbezogen prüfen, um notwendige Optimierungs-maßnahmen zu identifzieren (Abgleich mit Soll-Anforderungen)



Bestehende Maßnahmen optimieren bzw. zusätzliche Maßnahmen umsetzen

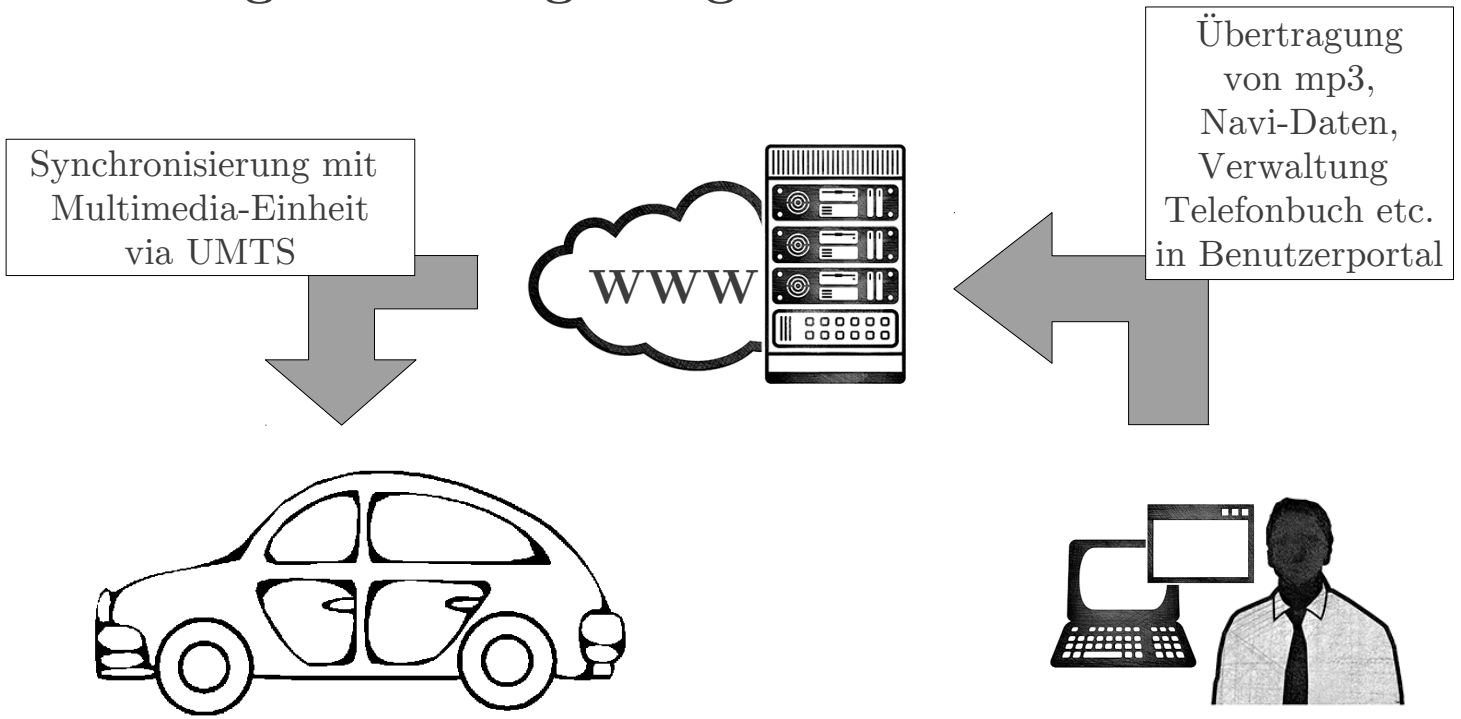




Angelehnt an die Normen ISO/IEC 27001 (ISMS) und ISO/IEC 27005 (IT-Risikomanagement)

- **Beispiel Fahrzeugelektronik (stark proprietär):**
  - > Zunehmende Vernetzung der Fahrzeuge (intern + extern)
  - > Innovative Funktionen (Multimedia, Internet, offene Ethernet-Schnittstelle)
  - > Daten können ins Fahrzeug „eingebracht“ werden, z.B. mp3-Downloads, Navi-Daten

- **Audit folgender Umgebung:**



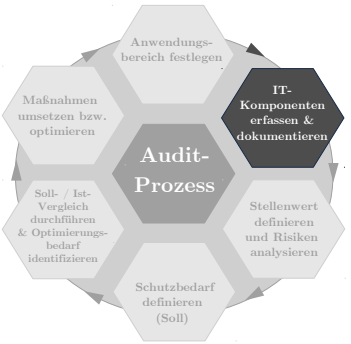
▶ Untersuchungsobjekt / Verantwortlichkeiten :

> **Fahrzeugelektronik mit Internet- und Multimedia-Schnittstellen (Anwendungsbereich):** Übertragung von mp3-Playlists und Navi-Daten, Telefonbuchverwaltung (etc.) via Nutzerportal zum Fahrzeug

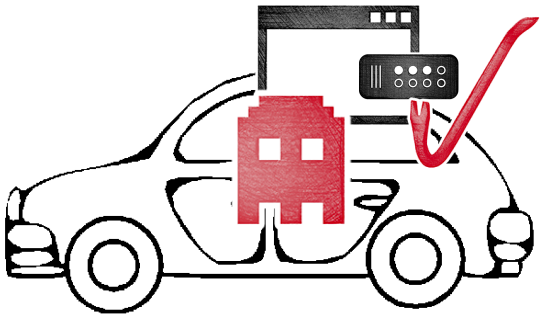
> **Komponenten im Fahrzeug:** Multimedia-Einheit, Internet-Gateway, Bedieneinheit (in Verbindung mit sicherheitsrelevanten Komponenten, z.B. Motorsteuerung)

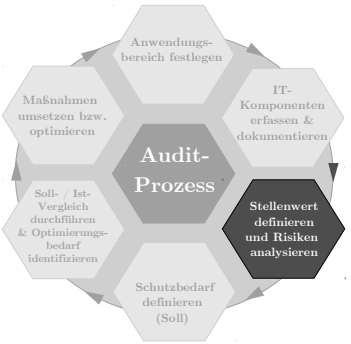
> **„Klassische“ IT-Komponenten:** Server und Kommunikationsverbindungen (VPN via UMTS), Web-Frontend des Portals

> **Projektansprechpartner:** Entwicklungsabteilung des Automobilkonzerns, Lieferant Mulitmedia-Komponente, Entwickler und Betreiber der Server-Systeme / des Web-Frontends



- **Stellenwert:** Entscheidende Innovationstechnologie des Automobilkonzerns um wettbewerbsfähig zu bleiben
- **Wesentliche Bedrohungen:**
  - > Manipulation des Systems durch „Angreifer“
  - > Infektion des Fahrzeugs mit Schadprogrammen (Gefahr von Fehlfunktionen)
  - > Diebstahl von Know-how durch Reverse Engineering von Software-Komponenten
- **Konkrete Risiken:**
  - > Störung des Fahrzeugs bis hinein in sicherheitskritische Komponenten (direkte Gefahr für Fahrer)
  - > Verlust des Marktvorsprungs
  - > Imageschaden





▶ IT-Grundwerte:

> Hohe Anforderungen an die Verfügbarkeit: Manipulationsschutz bzgl. Ausfall Multimedia

> Sehr hohe Anforderungen an die Verfügbarkeit: Auswirkungen auf Fahrzeugsteuerung (Ausfall)

> Sehr hohe Anforderung an die Integrität: Manipulationsschutz bzgl. Veränderungen (z.B. Lautstärke hochregeln, Tachoanzeige manipulieren)

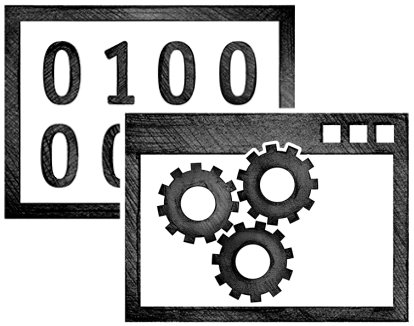
> Sehr hohe Anforderungen an die Vertraulichkeit: Reverse Engineering der Software

> Unter diesen Gesichtspunkten wurde auch die Server-Umgebung und das Benutzerportal betrachtet (z.B. Verfügbarkeit und Angreifbarkeit Web-Frontend)

▶ Angewandte Audit-Methoden:

- > **Konzeptionelles Audit** (fragebogenbasiert) und **Penetrationstests** des Benutzerportals
- > **Audit der Kommunikationsverbindung** (mitlesen und verändern der Daten)
- > **Audit der Schnittstellen am Fahrzeug** (UMTS / IP-Verbindung / USB (direkt), bzgl. direkte Zugriffsmöglichkeiten auf das System, Möglichkeit der Einspielung manipulierter Dateien
- > **Audit bezüglich Ausbruchmöglichkeiten aus der Multimediaeinheit** in Richtung Fahrzeugsteuerung (z.B. via CAN-BUS)
- > Weitere angewendete Methoden: **Fuzzing** zum Test der Robustheit (Einspielen diverser veränderter und ergänzter Dateien – z.B. mp3 mit verschiedenst veränderten Metadaten)

- **Entwicklung spezieller Tools notwendig:**
  - > Automatisierung von Tests (Simulation von Benutzereingaben, wie z.B. wiederholtes Laden und Ansteuern von mp3-Dateien)
  - > Überwachung der Ergebnisse (Untersuchungsobjekte teilweise „Black-Boxes“)



▶ Erzielte Ergebnisse:

> Implementierungs- und Betriebsmängel des Benutzerportal (Web-Frontend angreifbar, mangelhafte Redundanz von Systemkomponenten etc.)

> Absturz Multimedia-Einheit beim Einspielen bestimmter Dateien (überlange Dateinamen etc.) mit Auswirkung auf andere Komponenten (z.B. Navigationssystem)

> etc.

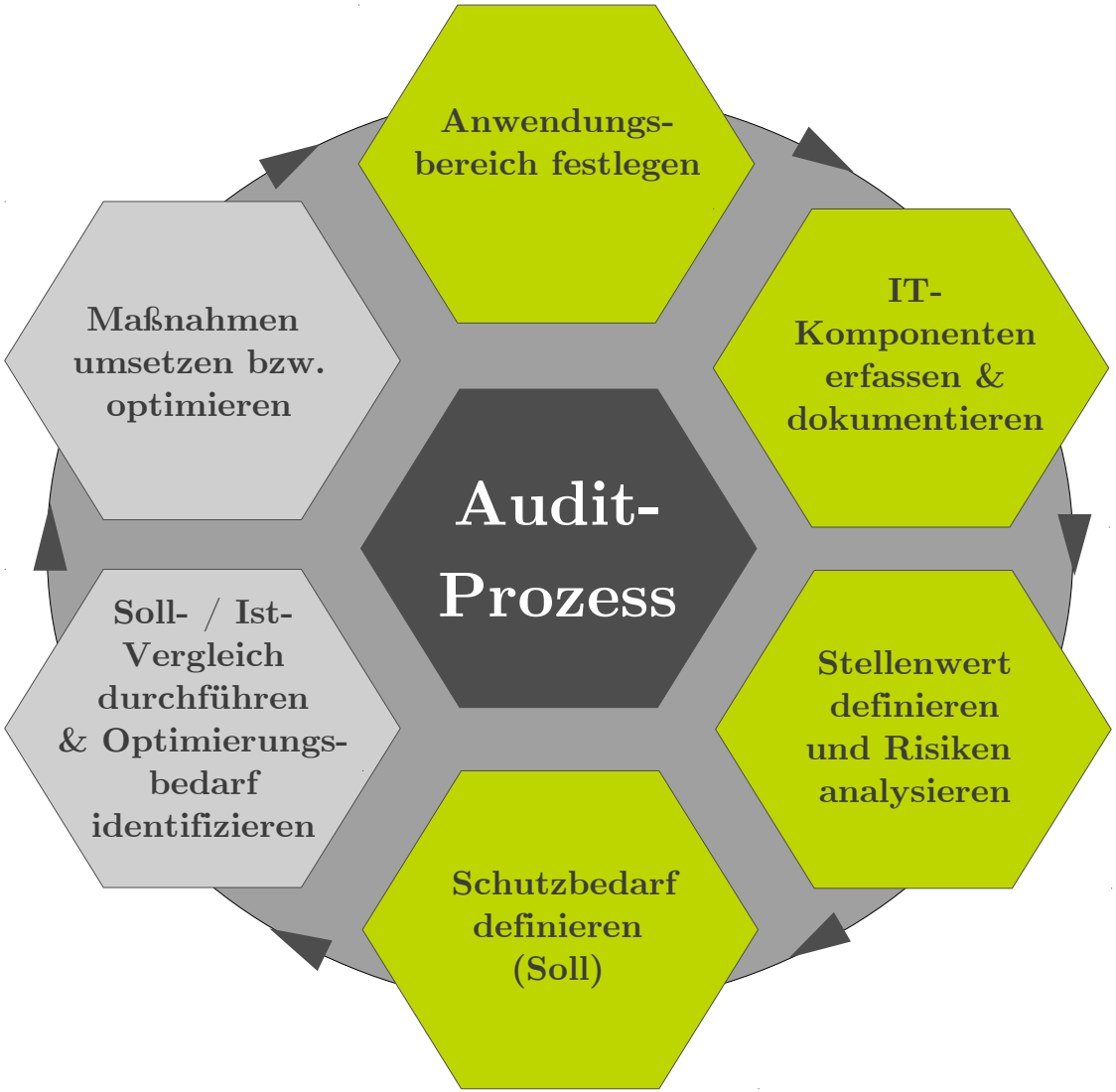
▶ Notwendige Maßnahmen:

> Generelle Optimierung des Benutzerportals (Behebung von Programmiermängeln, wie z.B. Cross-Site-Scripting, redundante Auslegung wichtiger Systemkomponenten etc.)

> Optimierung Mulitmedia-Einheit: Überarbeitung der Software durch den Lieferanten etc.

- Fahrzeugelektronik gestaltet sich im Audit-Prozess besonders schwierig – proprietär / Black-Box-Charakter
- Was dort im Audit funktioniert, funktioniert auch mit anderen Systemen:
  - > Prozess-IT / Leitstandtechnik (Maschinen- und Anlagensteuerung, SCADA)
  - > Consumerprodukte (Router, Multimediasysteme, Kopierer, Drucker)
  - > Gebäudesteuerung
  - > etc.

- IT-Systeme haben inzwischen alle Unternehmensbereiche (und unser Privatleben) durchdrungen, in Verbindung mit deren umfassenden Vernetzung
- Daraus resultiert eine erhebliche IT-Abhängigkeit, welche zwingend IT-Sicherheit bedingt (Vertraulichkeit, Integrität, Verfügbarkeit)
- Eine getrennte Betrachtung der „klassischen IT“ (Office IT etc.) und den Bereichen Industrieautomation / eingebettete Systeme ist künftig nicht mehr möglich
- Ohne strukturierte Prüfungen (Audit-Prozess in 6 Schritten) können IT-Sicherheitsmaßnahmen aber nicht zielgerichtet und umfassend realisiert werden
  - > Schaffung der Übersicht (Systeme, Verantwortlichkeiten)
  - > Schaffung von Transparenz (Anforderungen an das Sicherheitsniveau und Ist-Zustand)
  - > Bewertung der Angemessenheit / Vermeidung des „Gießkannenprinzips“ (Wirtschaftlichkeit)
  - > Die ersten 4 Schritte spielen dabei eine tragende Rolle


Anwendungs-
bereich festlegen
IT-
Komponenten
erfassen &
dokumentieren
Stellenwert
definieren
und Risiken
analysieren
Schutzbedarf
definieren
(Soll)
Soll- / Ist-
Vergleich
durchführen
& Optimierungs-
bedarf
identifizieren
Maßnahmen
umsetzen bzw.
optimieren
Audit-
Prozess

SCHUTZWERK

SCHUTZWERK GmbH
Pfarrer-Weiß-Weg 12
89077 Ulm

Phone +49 731 977 191 0
Fax +49 731 977 191 99

www.schutzwerk.com
info@schutzwerk.com

Für Fragen stehen wir Ihnen gerne zur Verfügung