IT-Security

Mag. Dr. Gerhard Wirth MBA

Zielsetzung

Erkennen und Beurteilen von Risken und deren Behandlung sowie der notwendigen Maßnahmen zur Erhöhung der Sicherheit der IT.

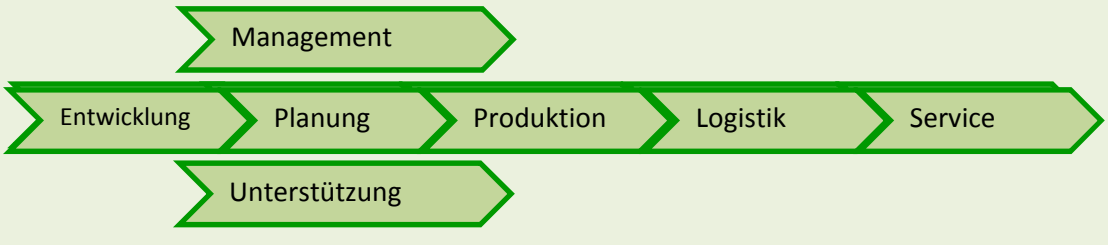
Vorgehen

Untersuchung der Grundlagen und Fakten zur IT-Security des Unternehmens.
Die Vorgaben der ISO 27001 dienen als Leitfaden der Analyse.

Kundennutzen

Grundlage zur Erhöhung der Sicherheit der Unternehmens-IT auf der Grundlage der Norm ISO 27001.
Möglichkeit der Vorbereitung zur Zertifizierung nach ISO 27001.
Beseitigung der wichtigsten Risken im Bereich der IT-Sicherheit.

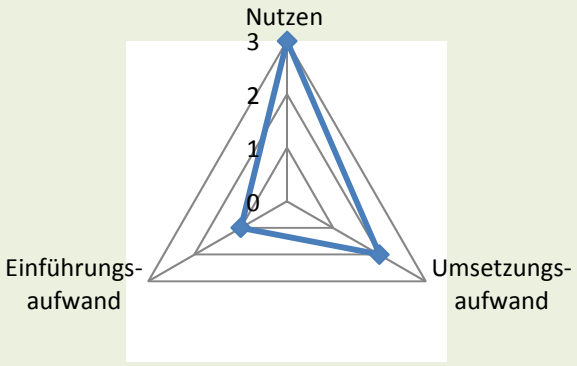
Wirkung auf Kern- und Hauptprozessen



IT-Security

Mag. Dr. Gerhard Wirth MBA

Aufwand-/Nutzenrelation



Ausgewählte Einsatzgebiete

Führung	Produktentwicklung, F&E, Design
Strategie	Beschaffung
Teammanagement	Leistungserbringung, Produktion, Logistik
Mitarbeiterentwicklung	Vertrieb, Auftragsabwicklung
Wissensmanagement	Customer-Relations-Management
Risikomanagement	Qualitätsmanagement
Gesundheits-, Arbeits-, Umweltschutz	Rechnungswesen, Controlling
IT-Prozesse, IT-Security	Unternehmenskommunikation

Quantitative Ergebnisse	Qualitative Ergebnisse
Erkennen der notwendigen Maßnahmen und ggf. Investitionen zur Erreichung einer für das Unternehmen erforderlichen IT-Sicherheit.	Strukturierter Report nach den Anforderungen und Erkenntnissen der ISO 27001.

IT-Security

Mag. Dr. Gerhard Wirth MBA

Hilfmittel und Werkzeuge	Ergänzende Methoden
Alle MS-Office-Produkte. Checklisten. ISO 27001.	5 S von Toyota. 7 Mudas.

Erweiterte Beschreibung der Vorgangsweise

Beschreibung des Umfanges und der Grenzen des IT-Security-Managements-Systems unter Berücksichtigung der Besonderheiten des Business Modells, der Organisation (Diagramm), der Standorte, eingesetzter IT-Komponenten und Technologie und betroffener Stake-Holder, sowie Beschreibung eventuell vorgenommener Ausschließungen.
Beschreibung der Policy des IT-Security-Management-Systems unter Berücksichtigung der Besonderheiten des Business Modells, der Organisation (Diagramm), der Standorte, eingesetzter IT-Komponenten und Technologie.
Berücksichtigung von geschäftlichen und gesetzlichen Anforderungen und von vertraglichen Verpflichtungen zur Frage der Sicherheit der Informationssysteme.
Definition der Risken für die Sicherheit von Geschäftsinformationen, für Einhaltung gesetzlicher Bestimmungen und für die Einhaltung sonstiger Regelungen sowie Beschreibung der Methode, nach der diese Risken überprüft werden.
Definition von Kriterien nach denen Risken überprüft und ggf. akzeptiert werden, sowie die dafür geltenden Grenzwerte.
Die definierten Grenzwerte und die Methode muss gewährleisten, dass innerhalb des Systems vergleichbare und reproduzierbare Ergebnisse erzielt werden können.

Die Norm ISO 27001 fordert für alle Schritte im ISMS (IT-Security-Management-System) ein konsequentes Vorgehen nach dem PDCA-Zyclus nach Deming.

IT-Security

MANAGEMENT services

Mag. Dr. Gerhard Wirth MBA

Darstellungen, Grafiken, Muster, etc.