IT-Basis Check: Informationssicherheit

Standortbestimmung und Beurteilung gemäß ISO/IEC 27001

Informationen sind wesentliche Bestandteile erfolgreicher Geschäftsprozesse und **stellen einen großen Wert dar**, für dessen Sicherung und Erhaltung die Leitung des Unternehmens verantwortlich ist.

Die Vertraulichkeit, die Verfügbarkeit, die Richtigkeit und die Vollständigkeit sowie die Verbindlichkeit von Informationen sind unverzichtbare Bestandteile einer erfolgreichen Unternehmensstrategie.

Dabei gewinnen die **Infrastrukturen der Informationstechnologie**, die für die Bereitstellung und Verarbeitung von Informationen genutzt werden, weiterhin an **Bedeutung** und müssen den Anforderungen gerecht werden.

Bisher haben sich Unternehmen nur auf die IT-Sicherheit konzentriert. Die Erfahrungen der letzten Jahre haben jedoch aufgezeigt, dass es notwendig ist „IT-Sicherheit“ umfassender zu betrachten und auf alle in einem Unternehmen existierenden Daten, unabhängig in welcher Form diese existieren, auszudehnen. Aus „Daten“ werden in der Folge „Informationen“ und „ITSicherheit“ wird zu „Informationssicherheit“.

Die **internationale Norm ISO/IEC 27001** berücksichtigt diese Sichtweise und fordert für Informationssicherheit einen eigenen Prozess und definiert zugleich konkrete Maßnahmen. Dieses Information Security Management System (ISMS) entspricht im Wesentlichen einem **Qualitätsmanagement der Sicherheitsanforderungen** von Informationen.

SEC4YOU führt eine **Standortbestimmung** in Bezug auf die Anforderungen der **ISO/IEC 27001** durch, ermittelt die Verbesserungspotenziale und liefert konkrete Lösungsvorschläge.

https://sec4you.com
office@sec4you.com
+43 1 253 17 97

Kernbestandteile & Ergebnisse

Der IT-Basis Check erfolgt gemäß den Vorgaben der ISO/IEC 27001. Hierdurch wird gewährleistet, dass die Standortbestimmung dem aktuellen Stand der Technik entspricht und alle relevanten Prüfbereiche berücksichtigt werden.

Prüffelder der ISO/IEC 27001

- Rahmenbedingungen und Sicherheitsbedürfnis des Unternehmens
- Verantwortung und Engagement der Unternehmensleitung
- Umgang mit Risiken und Chancen
- Unterstützung, Bewusstsein und Kommunikation der Sicherheitsziele
- Messung der Ziele und Verfahren zur Verbesserung
- Richtlinien und Aufbau der Sicherheitsorganisation
- Sicherheitsanforderungen im Personalwesen
- Umgang mit Informationen und Verantwortung
- Zugriffsschutz und Benutzerverwaltung
- Einsatz kryptographischer Maßnahmen
- Physische Sicherheit
- Betriebssicherheit, Virenschutz, Backup und Restore und Monitoring
- Kommunikationsicherheit
- Anschaffung, Entwicklung und Instandhaltung von Systemen
- Sicherheit im Umgang mit Lieferanten
- Umgang mit Sicherheitsvorfällen
- Sicherheitsaspekte im betrieblichen Kontinuitätsmanagement
- Konformität mit gesetzlichen und vertraglichen Anforderungen

Nutzen für das Unternehmen

- Rechtssicherheit durch die Anwendung der international anerkannten ISO/IEC 27001, da Normen im Streitfall als **„Stand der Technik"** gelten
- Beurteilung des IST-Standes durch unabhängige Experten
- Kenntnis möglicher Gefährdungspotenziale und bewusste Auseinandersetzung mit Risiken;
- Erhöhung der Effektivität und Effizienz der eingesetzten Ressourcen für Sicherheit
- Fehlende Sicherheitsmaßnahmen werden ermittelt und können zeitgerecht behoben werden

Im Ergebnis erhalten Sie einen schriftlichen **Bericht**, in dem **vorhandene Schwachstellen** und Risiken aufgezeigt werden und **konkrete Empfehlungen** zur Verminderung der ermittelten Risiken für Ihr Unternehmen beschrieben werden.