IT Security Management

ISO 27001 & IT-Grundschutz

Maßnahmen zur Sicherung der unternehmensweiten IT-Infrastruktur sind mittlerweile in vielen Unternehmen implementiert. Doch sind diese Maßnahmen auch ausreichend bzw. angemessen? Die ISO und das Bundesamt für Sicherheit in der Informationstechnik (BSI) stellen mit der Norm ISO 27001 bzw. den IT-Grundschutz-Katalogen jeweils Standardwerke für die geeignete Auswahl von Sicherheitsmaßnahmen für typische IT-Konfigurationen zur Verfügung. Ziel ist es, durch geeignete Anwendung organisatorischer, personeller, infrastruktureller und technischer Standard-Sicherheitsmaßnahmen ein Sicherheitsniveau zu erreichen, das für den normalen Schutzbedarf angemessen und ausreichend ist sowie als Basis für hochschutzbedürftige Systeme und Anwendungen dienen kann. Egal, an welchem Standard Sie sich orientieren – ein erfolgreiches Audit führt Sie zum international anerkannten ISO-27001-Zertifikat.

Ziel

plan42 unterstützt Sie mit eigenen ISO-27001-Auditoren bei der Erstellung eines Sicherheitskonzepts bzw. bei der Umsetzung der Norm ISO 27001/der IT-Grundschutz-Kataloge – auf Wunsch bis hin zum ISO-27001-Zertifikat. Unsere langjährige Erfahrung ist Ihr Vorteil bei der schnellen und kostenoptimalen Durchführung des Projekts.

Durchführung nach IT-Grundschutz

1. **Initiierung des Sicherheitsprozesses** – Wir unterstützen Sie nicht nur bei der Ermittlung der Anforderungen und der Formulierung allgemeiner Sicherheitsziele, sondern auch bei der Erstellung einer Sicherheitsleitlinie sowie beim Aufbau einer Sicherheitsorganisation.
2. **IT-Strukturanalyse** – Der zu untersuchende IT-Ausschnitt wird festgelegt. Anschließend sammeln wir die benötigten Informationen über die dort eingesetzte Informationstechnik.
3. **Schutzbedarfsfestellung** – Wie viel Schutz benötigt Ihre Infrastruktur? Ziel der Schutzbedarfsfeststellung ist es, diese Frage zu klären und damit die Auswahl angemessener Maßnahmen zu ermöglichen.
4. **Modellierung** – Bei der Modellierung werden alle Komponenten des IT-Verbundes mit Hilfe der Bausteine/Controls der ISO 27001 bzw. der IT-Grundschutz-Kataloge nachgebildet.
5. **Basis-Sicherheitscheck** – Die bereits umgesetzten Sicherheitsmaßnahmen werden mit den Empfehlungen der ISO 27001 bzw. der IT-Grundschutz-Kataloge verglichen, um das erreichte IT-Sicherheitsniveau zu identifizieren, Verbesserungsmöglichkeiten aufzuzeigen und ihre Realisierung einzuleiten. Die Sicherheitsmaßnahmen beschränken sich nicht nur auf technische Aspekte, sondern umfassen auch Organisation, Personal und bauliche Infrastruktur.
6. **Ergänzende Sicherheitsanalyse** – Für kritische Komponenten mit besonders hohem Schutzbedarf reichen die Controls der ISO 27001 bzw. der IT-Grundschutz-Kataloge evtl. nicht aus. Ob und ggf. welche zusätzlichen Maßnahmen hier erforderlich sind, wird mit Hilfe einer ergänzenden Sicherheitsanalyse ermittelt.
7. **Umsetzung der Strategie** – Wir unterstützen Sie bei der Realisierung fehlender Sicherheitsmaßnahmen und helfen Ihnen sowohl bei der technischen Umsetzung als auch bei der Erstellung von Sicherheitsrichtlinien und -konzepten.
8. **Audit** – Abschließend bereiten wir die Unterlagen für die Auditierung vor und begleiten Sie auf Wunsch bis zur Zertifizierung.

Ergebnis

Entsprechend den Empfehlungen der ISO 27001 bzw. der IT-Grundschutz-Kataloge werden die Ergebnisse der einzelnen Schritte umfassend dokumentiert. So verfügen Sie über die vom Gesetzgeber geforderten Dokumente für das Risikomanagement und können falls gewünscht eine ISO-27001-Zertifizierung durchführen lassen.

plan42

plan42 ist ein Beratungsunternehmen, das sich auf die Bereiche IT Service Management, IT Security Management & Business Solutions spezialisiert hat. Von der Prozessanalyse über die Beratung und Konzeption bis hin zur Realisierung – plan42 verbindet technische Expertise mit praxisbewährten Konzepten aus den Bereichen IT Service & Security Management.