

Aufbau eines Information Security Management Systems

Heute sind alle Ihre Geschäftsprozesse in Applikationen abgebildet und sämtliche Daten sind elektronisch gespeichert. Ein kontinuierlicher Geschäftsbetrieb ist ohne Zugriff auf diese Informationen nicht möglich. Informationssicherheit rückt damit immer mehr in den Fokus von Wirtschaftsprüfern und Revisionsabteilungen und fließt in Testate ein.

Doch wie können Sie nachweisen, dass Sie alle notwendigen Maßnahmen ergriffen haben und die relevanten Gesetze und Vorschriften befolgen?

Hier hilft Ihnen ein Information Security Management System (ISMS). Sie müssen sich nicht zwingend nach ISO 27001 oder BSI Grundsicherheitsrichtlinie zertifizieren lassen, um ein Testat zu erreichen, ein dokumentiertes ISMS reicht in der Regel aus.

BDG unterstützt Sie bei der Etablierung des ISMS Prozesses, erstellt gemeinsam mit Ihnen die notwendigen Dokumente und führt IT-Security Assessments und Risikoanalysen durch.

Einem ISMS liegen Leitlinien zugrunde, die auf grundlegenden gesetzlichen Anforderungen oder allgemein anerkannten besten Praktiken (Best Practise) basieren.

ISMS Prozessansatz

Die Einrichtung und Verwaltung eines ISMS erfordert dieselbe Vorgehensweise wie bei anderen Managementsystemen. Das PDCA Prozessmodell aus dem britischen Standard (plan, do, check and act) beschreibt eine Abfolge von sich wiederholenden Aktivitäten: Planen, Durchführen, Prüfen und Handeln.

>>>

In dem Prozessschritt **PLANEN** werden die Sicherheitsziele festgelegt und die Prozesse und Verfahren bestimmt, die für das Risikomanagement und die Verbesserung der Informationssicherheit relevant sind, um die entsprechenden Ergebnisse im Rahmen der Gesamtpolitik einer Organisation zu erreichen.

In dem Prozessschritt **DURCHFÜHREN** werden die Policies, Maßnahmen, Prozesse und Verfahren umgesetzt und durchgeführt. Hierzu zählt die Implementierung der Sicherheitspolitik, die Umsetzung von Kontrollmechanismen und die Integration von Prozessen.

In dem Prozessschritt **PRÜFEN** wird die Einhaltung des ISMS anhand der Sicherheitspolitik, der Sicherheitsziele und von praktischen Erfahrungen überwacht und gemessen sowie eine Berichterstattung über die Ergebnisse an das Management zwecks Überprüfung durchgeführt. Hierzu gehören Prozess-Monitoring, Reviews und Audits sowie die Identifizierung potenzieller Nichtkonformitäten und deren Ursachen sowie veränderte Risiken.

In dem Prozessschritt **HANDELN** werden Korrektur- und Vorbeugemaßnahmen ergriffen, die auf den Ergebnissen der Überprüfung aus der Prüfungsphase basieren. Hierdurch soll eine kontinuierliche Verbesserung des ISMS sichergestellt werden.

Die Zertifizierung nach ISO 27001 oder BSI IT-GSHD kann nur von akkreditierten Zertifizierungsstellen vorgenommen werden. Hierbei wird streng nach Auditoren, die Unternehmen im Zertifizierungsprozess begleiten (Lead Auditoren) und akkreditierten Auditoren, die Zertifizierungen durchführen (Certification Bodies) unterschieden.

BDG verfügt über mehrere Lead Auditoren und unterstützt Sie im Rahmen von Compliance Audits im Zertifizierungsprozess.

Bei der Vorbereitung auf ein Zertifizierungsaudit wird untersucht, ob eine angestrebte Zertifizierung nach ISO 27001 oder BSI Grundsatz sinnvoll ist. Dabei wird ein realer Zertifizierungsprozess simuliert. Angefangen von einem Review des dokumentierten Sicherheitsniveaus, um festzustellen, ob zertifiziert werden kann, bis hin zu einer Delta-Analyse, werden alle nicht konformen Elemente identifiziert.

Wir schlagen Ihnen konkrete Maßnahmen vor, um eine angestrebte Zertifizierung erfolgreich zu bestehen, unterbreiten Ihnen Verbesserungsvorschläge und setzen diese auf Wunsch gemeinsam mit Ihnen um. Durch eine zielgerichtete Betreuung während der Vorbereitungsphase auf das Zertifizierungsaudit können Sie Zeit und Kosten sparen.