ISO 27001:2013 - Zertifikat für Managementsysteme für Informationssicherheit

Einführung

Diese Internationale Norm wurde erstellt, um Anforderungen für die Einrichtung, Implementierung, Aufrechterhaltung und kontinuierliche Verbesserung eines Informationssicherheits-Managementsystems bereitzustellen. Die Einführung eines Informationssicherheitsmanagementsystems ist eine strategische Entscheidung für ein Unternehmen. Die Einrichtung und Implementierung des Informationssicherheitsmanagementsystems einer Organisation wird beeinflusst von den Bedürfnissen und Zielen der Organisation, den Sicherheitsanforderungen, den verwendeten organisatorischen Prozessen sowie der Größe und Struktur der Organisation. All diese Einflussfaktoren dürften sich im Laufe der Zeit ändern.

Das Informationssicherheitsmanagementsystem bewahrt die Vertraulichkeit, Integrität und Verfügbarkeit von Informationen durch die Anwendung eines Risikomanagementprozesses und gibt interessierten Parteien das Vertrauen, dass Risiken angemessen gemanagt werden.

Es ist wichtig, dass das Informationssicherheitsmanagementsystem Teil der Prozesse und der gesamten Managementstruktur der Organisation ist und in diese integriert ist und dass die Informationssicherheit bei der Gestaltung von Prozessen, Informationssystemen und Kontrollen berücksichtigt wird. Es wird erwartet, dass die Implementierung eines Informationssicherheitsmanagementsystems in Übereinstimmung mit den Anforderungen der Organisation skaliert wird.

Diese Internationale Norm kann von internen und externen Parteien verwendet werden, um die Fähigkeit der Organisation zu bewerten, die eigenen Informationssicherheitsanforderungen der Organisation zu erfüllen.

Die Reihenfolge, in der Anforderungen in dieser Internationalen Norm dargestellt werden, spiegelt nicht ihre Bedeutung wider oder impliziert die Reihenfolge, in der sie umgesetzt werden sollen. Die Listenelemente werden nur zu Referenzzwecken aufgezählt.

ISO/IEC 27000 beschreibt den Überblick und das Vokabular von Informationssicherheits-Managementsystemen unter Bezugnahme auf die Normenfamilie von Informationssicherheits-Managementsystemen (einschließlich ISO/IEC 27003 [2] , ISO/IEC 27004 [3] und ISO/IEC 27005 [4]) mit verwandten Begriffen und Definitionen.

Anwendungsbereich

Diese Internationale Norm legt die Anforderungen für die Einrichtung, Implementierung, Aufrechterhaltung und kontinuierliche Verbesserung eines Informationssicherheitsmanagementsystems im Kontext der Organisation fest. Diese Internationale Norm enthält auch Anforderungen für die Bewertung und Behandlung von Informationssicherheitsrisiken, die auf die Bedürfnisse der Organisation zugeschnitten sind. Die in dieser Internationalen Norm festgelegten Anforderungen sind generisch und sollen auf alle Organisationen anwendbar sein, unabhängig von Art, Größe oder Art. Der Ausschluss einer der in den Abschnitten 4 bis 10 festgelegten Anforderungen ist nicht akzeptabel, wenn eine Organisation die Konformität mit dieser Internationalen Norm beansprucht.