0800 400 510 1

AKTUELLE INFORMATION RISIKEN IN DER INFORMATIONSSICHERHEIT

Prozessmanagement - Nr. 09/2021

Prozessmanagement

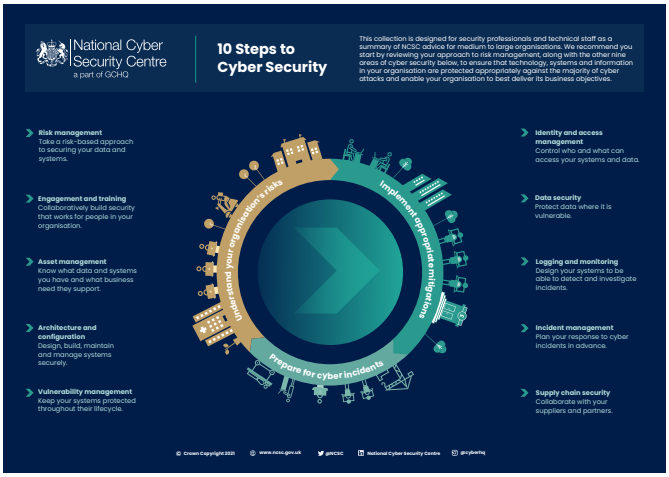
Wir entlasten Führungskräfte und schützen Mitarbeiter. Seit 1997.

Risiken in der Informationssicherheit - Wie kann die DIN ISO/IEC 27001 zur Minimierung beitragen?

Informationen stellen heutzutage eine der wertvollsten und kritischsten Ressourcen in einem Unternehmen dar. Diese sind aufgrund der weltweit immer stärker zunehmenden Vernetzung großen Bedrohungen und Cyberangriffen ausgesetzt. **Diese Bedrohungen werden immer ausgeklügelter und die Schäden, welche sie hervorrufen, immer größer.** Diese zusammen mit Datenschutzverletzungen gehören mit zu den fünf wahrscheinlichsten Risken der **TOP 10 der Risiken für Unternehmen** mit dem größten Effekt auf das Unternehmen (Weltwirtschaftsforum, Global Risks Report 2018). Die Häufigkeit nimmt hier genauso zu wie das schädigende Potenzial. Auch ist zu beobachten, dass die finanziellen Kosten zur Abwehr solcher Cyberangriffe dazu stetig steigen.

Eine Strategie in der Informationssicherheit ist daher wichtiger denn je!

Bereits 2016 erkannte man in der britischen Regierung welche Bedrohungen Cyberangriffe darstellten und man konzipierte die ***10 Steps to Cybersecurity***. Dieses Konzept sollte als Leitfaden zur Orientierung für Führungskräfte dienen, mit dem Ziel die Cybersicherheit zu verbessern und Informationen im Unternehmen besser zu schützen. Dies unabhängig von Standort, Größe oder der Branche (NCSC, 10 Steps to cybersecurity).



Leistungsangebot Prozessmanagement

AKTUELL & WICHTIG!

Krisenmanagement- und Prozessmanagement Beratung

Potentiale identifizieren & analysieren

Strukturen entwickeln & gestalten

Prozesse festlegen & zielgerichtet steuern

Lifecycle & nachhaltige Entwicklung

Managementsysteme - QHSE

WIE KÖNNEN WIR IHNEN HELFEN?

FKC CONSULT GmbH
Eschenburgstr. 5
23568 Lübeck
www.fkc-gmbh.de

prozessmanagementanfrage@fkc-gmbh.de

0800 400 510 1

AKTUELLE INFORMATION RISIKEN IN DER INFORMATIONSSICHERHEIT

Prozessmanagement - Nr. 09/2021

Prozessmanagement

Kernelement dieses Leitfadens ist es, ein effektives Informationssicherheitsmanagement zu integrieren, welches sowohl von der Geschäftsführung unterstützt wird aber auch mit Subunternehmern vereinbart werden kann. **Wichtig ist hier die laufende Beteiligung des leitenden Managements.** Dies soll der Garant für ein fortlaufenden starken Fokus sowie die Zurverfügungstellung der erforderlichen Ressourcen bedingt durch eine dynamische Risikenverschiebung darstellen.

Wie hängt nun dieser Leitfaden mit der ISO 27001 zusammen?

Auch in der ISO 27001 erfolgt eine Ermittlung Ihrer wertvollsten Ressourcen mit dem Versuch diese zu schützen. Dieses können personenbezogene Daten, Kundendaten, Informationen finanzieller Natur oder auch anderer Art sein.

Hat ein Unternehmen ein **Informationssicherheitsmanagementsystem (ISMS) gem. ISO 27001 implementiert** hat es folgende Phasen durchlaufen:

- **1. Ermittlung der Ressourcen**
- **2. Analyse der Sicherheitsrisiken sowie der Bedrohungen**
- **3. Bestimmung des erforderlichen Risiko- und Behandlungsniveaus**
- **4. Einführung von Kontrollen zur Beseitigung oder Minimierung der Sicherheitsrisiken**

Hier findet man dann auch die enge Verbindung zwischen den ***10 Steps to Cybersecurity*** und der ISO 27001. Die ***10 Steps to Cybersecurity*** stellen hierbei den ersten Ansatz zur Beratung dar, während die ISO 27001 dann für das leitende Management ein Mittel zur praktischen Umsetzung darstellt. Hierbei geht es dann im Speziellen um die die Selektion und Entwicklung von Maßnahmen zur Kontrolle basierend auf der Risikobereitschaft des Unternehmens. Hierbei kommt es also sehr auf die Abstimmung von Risiko und Kontrolle an.

Auf den nächsten Seiten finden Sie eine Gegenüberstellung der ***10 Steps to Cybersecurity*** zu den Anforderungen aus der Norm ISO 27001.

0800 400 510 1

AKTUELLE INFORMATION RISIKEN IN DER INFORMATIONSSICHERHEIT

Prozessmanagement - Nr. 09/2021

Prozessmanagement

10 Steps to Cybersecurity	Kontrolle der Klausel nach ISO 27001	Bemerkungen
1. Arbeiten zu Hause und mobil	A 6.2	Eine sichere Aufbewahrung ist auch dann wichtig, wenn ein Mitarbeiter von zu Hause aus, beim Kunden oder unterwegs arbeitet.
2. Benutzerschulung und Sensibilisierung	A 7.3.2	Alle Mitarbeiter und Subkontraktoren müssen die wichtigsten Risiken kennen und wissen, wie Vorfälle gemeldet werden. Dies kann man durch Sicherheits-unterweisungen als ein Teil des Onboardings neuer Mitarbeiter erreicht werden. Eine regelmäßige Fortführung ist hierbei notwendig.
3. Vorfallmanagement	A. 16	Es ist immens bedeutend das ein Unternehmen nach einem Informationssicherheitsereignis die Fähigkeit besitzt, einen Vorfall einzudämmen und dann so schnell wie möglich wieder in den normalen Geschäftsbetrieb zurückzukehren. Nach ISO 27001 müssen Unternehmen Informationssicherheit in ihre Managementprozesse integrieren. Dies erleichtert auch, den Nachweis der Einhaltung der ‚Datenschutz-Grundverordnung (DSGVO).
4. Informationsrisikomanagement	A 6.1 + 8.2	Das ISMS muss vom leitenden Management ernstgenommen werden, dies trägt erheblich zur Schaffung einer risikobewussten Kultur im gesamten Unternehmen bei. Hier finden wir in der ISO 27001 die Forderung, dass das leitende Management seine Unterstützung anbietet und eine klare Ausrichtung vorgibt.
5. Verwalten von Benutzerrechten	A 9.2	Benutzer von IT-Systemen stellen hier unter Umständen eine wichtige Quelle von Informationslecks dar. Nur die rollenbasierte Zuweisung von Zugriffsrechten reduziert Fehler und unterstützt die Verantwortung des Benutzers, sicherzustellen, dass er gute Sicherheitspraktiken befolgt.
6. Kontrollen für Wechselmedien	A 8.3.1	Es steigt die Verfügbarkeit von Speichersticks und anderen tragbaren Geräten. Für Unternehmen ist es daher von entscheidender Bedeutung, über Verfahren zu deren Verwendung zu verfügen, auch sollte hier die sichere Entsorgung von Medien nicht übersehen werden.

0800 400 510 1

AKTUELLE INFORMATION RISIKEN IN DER INFORMATIONSSICHERHEIT

Prozessmanagement - Nr. 09/2021

Prozessmanagement

7. Überwachung	A 12.7 + 12.4	Der Fokus auf unerwartete Aktivitäten zu richten, ist für Unternehmen in geschäftlicher Hinsicht sehr sinnvoll. Die Protokollierung der Überwachung von Benutzeraktivitäten liefert wertvolle Hinweise im Fall einer Verletzung und kann bei zukünftigen Untersuchungen hilfreich sein.
8. Sichere Konfiguration	A 12.1.2+14.2.2+ 14.2.3+14.2.4 +8.1	Das Verständnis der IT-Systeme und die Kontrolle der Änderungen an diesen Systemen trägt dazu bei, deren Integrität zu wahren und sicherzustellen, dass sie angemessen geschützt sind.
9. Malwareschutz	A 12.2	Stellen Sie sicher, dass Ihre Systeme aktualisiert sind, damit nicht bekannte Sicherheitslücken von schädlichen oder mobilen Codes ausgenutzt werden können.
10. Netzwerksicherheit	A 13.1	Das Risiko eines unbefugten Zugriffs durch einzelne oder Geräte wird verringert durch das Wissen wer über Netzwerkzugriff verfügt und wofür dieser genutzt wird.

Die ISO 27001 als Fundament Ihrer Informationssicherheitsstrategie

Unabhängig von der Größe Ihres Unternehmens oder der Branche, in der Sie tätig sind, bietet die ISO 27001 einen Rahmen für die beste Praxis, um Kontrollen zur Verwaltung von Informationssicherheitsrisiken und zum Schutz geschäftskritischer Daten zu ermitteln, zu analysieren und zu implementieren. **Die unabhängige Zertifizierung nach ISO 27001 zeigt, dass Ihr Unternehmen Informationssicherheit ernst nimmt, und bietet einen Wettbewerbsvorteil, um neue Geschäfte zu gewinnen und bestehende Kunden zu binden.**

Gerne unterstützen wir Sie in den Phasen

- **1. Ermittlung der Ressourcen**
- **2. Analyse der Sicherheitsrisiken sowie der Bedrohungen**
- **3. Bestimmung des erforderlichen Risiko- und Behandlungsniveaus**
- **4. Einführung von Kontrollen zur Beseitigung oder Minimierung der Sicherheitsrisiken**

Sprechen Sie uns und unsere Berater gerne darauf an. Zusammen mit Ihnen entwickeln wir hier die für Sie passende Informationssicherheitsstrategie und setzen sie zusammen mit Ihnen in Ihrem Unternehmen um.

prozessmanagementanfrage@fkc-gmbh.de

Bilder von Canva.