0800 400 510 1

AKTUELLE INFORMATION RISIKOANALYSE UND -REDUZIERUNG MIT ISO 27001

Prozessmanagement - Nr. 06/2021

Prozessmanagement

Wir entlasten Führungskräfte und schützen Mitarbeiter. Seit 1997.

Risikoanalyse und -reduzierung mit Hilfe der ISO 27001

Die Risikoanalyse in der DIN ISO 27001 ist der Ansatz von Unternehmen, mögliche Risiken der Informationssicherheit frühzeitig zu erkennen, diese zu bewerten und durch Sicherheitsmaßnahmen das Gesamtrisiko zu reduzieren. Die Einschätzung der bestehenden Sicherheitsrisiken ist dabei eine wesentliche Voraussetzung für ein erfolgreiches Management der Informationssicherheit. Auch in der Norm ISO IEC 27001 ist die Festlegung eines Prozesses zur Informationssicherheitsrisikobeurteilung gefordert. Ziel einer ISMS Risikoanalyse ist es, diese Risiken zu identifizieren, zu bewerten und so das Gesamtrisiko zu ermitteln.

Welche Methoden gibt es zur Risikoanalyse?

Die Auswahl der Methode ist für das Unternehmen frei wählbar. Eine Vorgabe der ISO 27001 gibt es nicht. Die Methodik muss nachvollziehbar und dokumentiert sein. Entsprechend dem Ziel und Zweck können dabei unterschiedliche Risikoanalysen oder Standards mehr oder weniger sinnvoll sein. Mögliche Methoden zur Risikoanalyse finden sich im Standard 100-3 des Bundesamtes für Sicherheit und Informationstechnik (BSI). Weitere Orientierung bietet zum Risikomanagement die Norm ISO 31000. Speziell für informationslastige und IT-basierte Umgebungen eignet sich jedoch die Vorgehensweise nach der ISO IEC 27005 sehr gut. Hier findet man Empfehlungen für Umsetzung des Risikomanagements. Zudem ist die ISO 27005 mit der ISO 31000 abgestimmt. Hier stellen wir Ihnen eine Vorgehensweise mit der Ausrichtung an den formellen Anforderungen des Standards ISO IEC 27005 vor.

Start der Risikoanalyse mit Ermittlung der Bedrohungen

Zunächst sollten Sie für eine ISMS Risikoanalyse die Gefahrenquellen bzw. Bedrohungen ermitteln. Unter einer Gefahrenquelle versteht man hierbei jeden Umstand oder Ereignis, welches einen potenziellen Schaden an einem Informationswert

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 RISIKOANALYSE UND -REDUZIERUNG MIT ISO 27001

Prozessmanagement - Nr. 06/2021

Prozessmanagement

verursachen kann. Ursachen der Bedrohungen können dabei natürlicher, menschlicher Art oder durch Umgebungsbedingungen herbeigeführte Ursachen sein. Als Ergebnis sollte hierbei eine Aufstellung mit möglichen Gefahrenquellen entstehen, welche vorhandene Schwachstellen im System ausnutzen können.

Schwachstellenermittlung

Es folgt eine Ermittlung der Schwachstellen der aktuellen Informationswerte. Unter einer Schwachstelle versteht man hierbei eine Sicherheitsschwäche in geltenden Verfahren der Verarbeitung von Informationen, im Design eines IT-Systems, bei dessen Implementierung oder beim Ausführen interner Kontrollen. Diese können dabei absichtlich oder unabsichtlich ausgenutzt werden. Allgemein ermittelt man sie durch Befragen der verantwortlichen Personen sowie der Administratoren oder anhand offizieller Quellen. Weitere Möglichkeiten, um (insbesondere technische) Schwachstellen festzustellen, sind automatisierte Scanning-Tools oder Penetrationstests (oftmals durch externe Experten durchgeführt, um Informationssysteme und Netzwerkkomponenten auf Schwachstellen zu prüfen). Die ermittelten Bedrohungen und zugehöriger Schwachstellen bilden die Basis für die Schutzbedarfsfeststellung und dadurch ermittelten Anforderungen. Dies dient dann als Grundlage für die Risikobewertung.

Prüfung der bereits vorhandenen Schutzmaßnahmen

Bereits existierende oder geplante Sicherheitsmaßnahmen sind hierbei zu berücksichtigen, um unnötige Kosten oder Aufwände zu vermeiden. Hierbei sind auch bereits umgesetzte Maßnahmen zu bewerten. Geplante neue Sicherheitsmaßnahmen müssen mit den existierenden kompatibel sein und eine wirtschaftlich sowie technisch sinnvolle Ergänzung darstellen.

Welche Schritte folgen bei der Risikoanalyse gem. ISO 27001?

Nach der Ermittlung der möglichen Bedrohungen, erfolgt als nächstes eine Risikobewertung. Basierend auf dem Bedrohungspotenzial folgt eine Einschätzung, wie erforderlich Sicherheitsmaßnahmen durchzuführen sind. Neben der Angemessenheit der geplanten oder bereits bestehenden Maßnahmen sind auch das Ausmaß eines Risikos von zwei weiteren Faktoren abhängig:

1. **Wahrscheinlichkeit des Eintretens**
2. **Folgen bzw. die zu erwartenden Auswirkungen**

Die Risikobewertung erfolgt dabei oftmals mithilfe einer Risikomatrix nach Nohl.

Bewertung der Eintrittswahrscheinlichkeit

Hierunter versteht man die erwartete Wahrscheinlichkeit, dass eine Gefahr wirksam wird. In diesem Kontext wird die Einschätzung des Eigners verwendet, mit der ein bestimmtes Ereignis in einem bestimmten Zeitraum auftritt. Bei dieser Bewertung ist besonders auf folgende Faktoren zu achten:

- Gefahrenquelle der Motivation und Leistungsfähigkeit
- Art der Gefährdung
- Existenz und Wirksamkeit der vorhandenen Maßnahmen

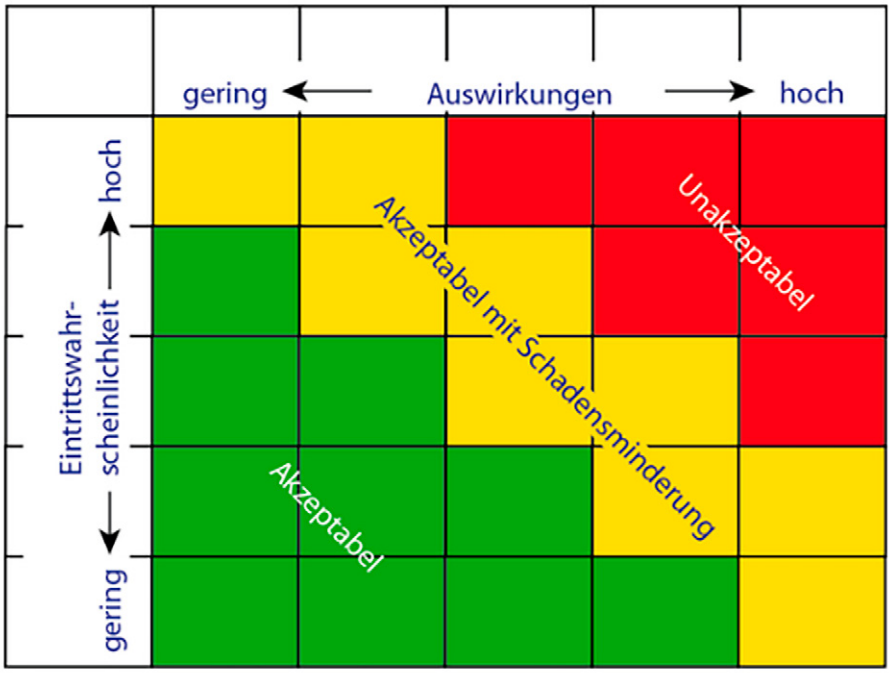
0800 400 510 1

AKTUELLE INFORMATION
RISIKOANALYSE UND -REDUZIERUNG MIT ISO 27001

Prozessmanagement - Nr. 06/2021

Prozessmanagement

Bestimmung und Analyse von Auswirkungen



Um die Höhe des Risikos festzustellen, werden die negativen Konsequenzen der Schadensereignisse hinsichtlich der existierenden Schwachstellen und des zu erwartenden Schadens bewertet.

Wie kann das Risiko einer Gefährdung reduziert werden?

Durch die Festlegung geeigneter Sicherheitsmaßnahmen können Sie die ermittelten Risiken anschließend mindern. Unter Risikomaßnahmen versteht man hierbei Handlungen zur Minderung, Vermeidung, Übertragung oder Akzeptanz von Risiken. Dabei können Maßnahmen in ursachenbezogene sowie wirkungsbezogene Maßnahmen unterteilt werden:
Ursachenbezogene Maßnahmen beziehen sich auf die Verringerung der Wahrscheinlichkeit des Eintretens und die Reduzierung der Anzahl von Schadensereignissen.
Wirkungsbezogene Maßnahmen sollen das Ausmaß möglicher negativer Auswirkungen von Ereignissen minimieren.

Für jedes bei der ISMS Risikoanalyse ermittelte und priorisierte Risiko wird an dieser Stelle geklärt, mit welchen Maßnahmen die Risiken behandelt werden können. Grundsätzlich sollten hierbei die Maßnahmen auf Basis der Risikobewertung, den zu erwartenden Kosten für die Umsetzung sowie dem Nutzen ausgewählt werden. Die Unternehmensleitung sollte Risiken mit geringer Eintrittswahrscheinlichkeit aber hohem Ausmaß gesondert betrachten. Sind in solchen Fällen die Maßnahmen aus wirtschaftlicher Sicht nicht zu rechtfertigen, könnte die Umsetzung dennoch sinnvoll sein.

Sie haben noch Fragen zum Risikobehandlung? Gerne stehen unsere Experten Ihnen mit Rat und Tat zur Verfügung!

Bilder von Canva.

prozessmanagementanfrage@fkc-gmbh.de