

Lizenzbestimmungen

- Diese Materialien sind lizenziert für @USERINFONAME@.
- Die Materialien dürfen **ausschließlich** für die Implementation, Verbesserung oder den Betrieb von Sicherheitsmaßnahmen innerhalb der genannten Organisation genutzt werden.
- Hierfür dürfen die Materialien beliebig verändert, ergänzt oder neu gestaltet werden.
- Für alle anderen Einsatzzwecke - insbesondere für die Veröffentlichung der Materialien und deren Einsatz für Kunden des Lizenznehmers - muss im Vorfeld eine schriftliche Genehmigung der 3473 Gurus GbR eingeholt bzw. eine entsprechende Lizenz erworben werden.

Diese Vorgabe definiert Maßnahmen der Kategorie „B“. Maßnahmen der Kategorie „B“ müssen behandelt werden. Sie sind prinzipiell verpflichtend (Schlüsselworte MUSS/MÜSSEN, DARF NICHT/DÜRFEN NICHT/DÜRFEN KEINE, siehe [Abschnitt 1.2 T3](#)) und ihre Behandlung wird bei einem Audit geprüft.

Für Maßnahmen der Kategorie „B“ besteht die Möglichkeit, in Eigenverantwortung geeignete, verhältnismäßige und wirksame (siehe [§30 Abs. 1 Satz 1 BISO n.F.](#)) Formen der Umsetzung zu entwickeln:

- Die Organisation kann sich bei jeder einzelnen Maßnahme dieser Kategorie dazu entscheiden, sie nicht oder nicht vollständig umzusetzen.
- Sie muss ihre Entscheidung nicht begründen.
- Wenn sie eine Maßnahme nicht oder nicht vollständig umsetzt wird ist die Organisation dazu verpflichtet, eine Risikoidentifizierung, -analyse und -behandlung gem. [Anhang A.2](#) zu etablieren. Dabei muss die nicht oder nicht vollständig umgesetzte Maßnahme als Schwachstelle betrachtet werden. Die zu untersuchende Fragestellung lautet: „Welche Risiken entstehen weil die Maßnahme X nicht bzw. nicht vollständig umgesetzt wird?“ Durch die Risikoidentifizierung und -analyse wird systematisch ermittelt, welche Risiken die Organisation durch ihre Entscheidung in Kauf nimmt. Im Zuge der Risikobehandlung muss sie „geeignete, verhältnismäßige und wirksame Maßnahmen zur Vermeidung, Reduzierung oder Übertragung der Risiken“ definieren, dokumentieren und umsetzen (siehe [Anhang A.2.5 A2](#)). Es besteht die Möglichkeit, Risiken zu akzeptieren, wenn ihre Schadenhöhen und/oder Eintrittswahrscheinlichkeiten unterhalb der Risikoakzeptanzgrenze liegen (siehe [Anhang A.2.5 E3](#)) oder wenn dies vom Topmanagement gewollt ist (siehe [Anhang A.2.5 A5](#)).
- Alle Maßnahmen dieser Kategorie sind in der ersten Spalte der Tabellen mit dem Buchstaben „B“ gekennzeichnet (z. B. „B1“ oder „B2.5“).