VORLAGE ZU ABSCHNITT 1.8 DES BANDES 5A

Die Risikoseite des Eigentümers

Eine Seite je Risikoeigentümer, unterschrieben: die Risiken seiner Tätigkeit als Szenarien, seine Entscheidung dazu und die Annahme, die nur ein Mensch mit Befugnis ausfüllen kann.

Kategorie: Arbeitsblatt. Bezug im Buch: Abschnitt 1.8 (Leitfrage, Tabellen 1, 2 und 4); Norm: Klauseln 6.1.2, 6.1.3, 8.2 und 8.3 der ISO/IEC 27001:2022 mit Änderung 1:2024, in den eigenen Worten des Buches. Rechtsstand des Bandes: 27. September 2026.

Risikoeigentümer (Name, Funktion)		**Tätigkeit, die er führt**	
Haus / Standort		**Datum der Seite**	
Beratung durch die IT		**Stand der Beurteilung vom**	

So nutzen Sie diese Vorlage

1. Eine Seite je Risikoeigentümer, mit den Risiken, auf die es für den Betrieb am meisten ankommt: Das Register kommt zur Eigentümerschaft als eine Reihe von Entscheidungen benannter Führungskräfte, nicht als ein Register mit hundertachtzig Zeilen, alle der IT zugewiesen.
2. Schreiben Sie jedes Risiko als Szenario: wer, worüber, mit welcher Folge. So geschrieben, benennt das Risiko seinen eigenen Eigentümer, weil es die Tätigkeit benennt. Das Wort «Phishing» allein ist eine Bedrohung, kein Szenario.
3. Die Spalte «Restrisiko angenommen» füllt nur der Risikoeigentümer aus, mit Name, Datum und Unterschrift. Die IT berät und kann kein Risiko im Namen einer Tätigkeit annehmen, die sie nicht führt.

Spalte «Im Buch»: verlangt = von der Norm verlangt, wie das Buch sie in eigenen Worten wiedergibt (Klausel in Klammern); Methode = Vorgehen dieses Bandes, keine Anforderung.

1 Die Frage an den Eigentümer

Frage	Antwort	Grund (aus dem Band)	Im Buch
Sind Sie befugt, die Tätigkeit zu ändern, aus der die Risiken dieser Seite entstehen?	☐ ja ☐ nein	Lautet die Antwort nein, ist das Register eine Liste, und die Risiken darauf hat niemand angenommen. Ein Risiko gehört dem, der die Tätigkeit ändern kann.	verlangt (6.1.2 c: Verantwortung und Befugnis)
Was nimmt das Haus an? (betroffene Gäste, verlorener Umsatz, gestörte Tage)		Eine kurze Aussage, was das Haus annimmt, ist der mögliche Nachweis der Kriterien; die Punktzahl allein entscheidet nicht.	verlangt (6.1.2 a); Fünf-mal-fünf-Matrix: Methode

2 Die Risiken dieser Tätigkeit

Nr.	Szenario: wer, worüber, mit welcher Folge	Bewertung: Folgen in Gästen, Umsatz und Tagen	Behandlung: was ändert sich in der Tätigkeit	Restrisiko angenommen: Name, Datum, Unterschrift	Überprüfen, wenn sich ändert

Verlangt (6.1.2 c): Risiken für Vertraulichkeit, Integrität und Verfügbarkeit ermittelt, Risikoeigentümer benannt. Verlangt (6.1.3 f): Die Risikoeigentümer genehmigen den Behandlungsplan und nehmen die Restrisiken an; der Satz, der aus einer Analyse eine Entscheidung macht. Verlangt (8.2): Beurteilung in Abständen und bei wesentlichen Änderungen; wer die Änderung macht, muss das wissen. Methode dieses Bandes: Szenarien statt Katalog, Bewertung in Gästen, Umsatz und Tagen, Behandlung als Änderung der Tätigkeit statt allein Sensibilisierung.

3 Unterschrift

Der Risikoeigentümer bestätigt	Name, Funktion	Datum	Unterschrift
Ich habe die Risiken meiner Tätigkeit gesehen, den Behandlungsplan genehmigt und die Restrisiken angenommen, die in Teil 2 mit meiner Unterschrift stehen.			
Zur Kenntnis genommen von der Eigentümerschaft oder der Direktion.			

Mögliche Nachweise laut Band (Tabelle 4): Unterschrift jedes Eigentümers unter die Risiken seiner Tätigkeit, mit Datum; Änderungen bei Plattformen, Lieferanten oder Abläufen lösen eine Überprüfung durch den betroffenen Eigentümer aus. Methode, keine Anforderung: ein förmlicher Ausschuss für die Risikoannahme.

4 Beispiel aus Abschnitt 1.8 (Tabelle 1): Risiko 117, wie es hätte stehen müssen

Merkmal	Beispiel aus Abschnitt 1.8: als Szenario
Beschreibung	Angreifer erlangt Zugangsdaten der Reservierung zum Extranet einer Plattform und schreibt Gästen mit Zahlungslinks
Eigentümer	Revenue-Managerin, die über Konten und Nachrichten bestimmt
Bewertung	Folgen in Gästen, Umsatz und Tagen: Hunderte Gäste betroffen, Sperre des Hauptvertriebswegs in der Hochsaison
Behandlung	zweiter Faktor, persönliche Konten, keine gespeicherten Passwörter, keine Zahlungen über Plattformnachrichten
Angenommen von	Revenue-Managerin, unterschrieben, mit Datum
Überprüft bei Änderung	ja, als die Anzahlungen auf das Nachrichtensystem verlegt wurden

Im Register des Falles stand dasselbe Risiko als «Phishing», Eigentümer «IT», 3 × 3 = 9, behandelt durch eine jährliche Sensibilisierungsschulung, angenommen von niemandem. Wem Risiken typischerweise gehören (Tabelle 2): Vertrieb über Plattformen dem Revenue Management; Meldung und Ausweise der Empfangsleitung; Zahlungen der Leitung Finanzen; Spa und Gesundheitsangaben der Spa-Leitung; Personal der Personalleitung; Lieferanten mit Zugang dem, der den Vertrag unterschreibt, mit der IT; Netz, Server, Sicherungen der IT.

Rechtlicher Rahmen laut Buch (Tabelle 5): Meldung einer Verletzung in Deutschland und Österreich unverzüglich und möglichst binnen 72 Stunden ab Kenntnis, außer bei voraussichtlich unwahrscheinlichem Risiko, Benachrichtigung der Gäste unverzüglich bei voraussichtlich hohem Risiko (Art. 33, 34 DSGVO); in der Schweiz an den Eidgenössischen Datenschutzbeauftragten so rasch als möglich bei voraussichtlich hohem Risiko (revDSG). Maßstab der Sicherheit: geeignete Maßnahmen unter Berücksichtigung des Stands der Technik (Art. 32 DSGVO), in der Schweiz angemessene Datensicherheit nach dem Risiko. Für die Zugangsdaten des eigenen Personals ist in allen drei Ländern das Haus verantwortlich, nicht die Plattform. Die Protokollierung persönlicher Konten ist in Deutschland mitbestimmt (BetrVG § 87 Abs. 1 Nr. 6), in Österreich zustimmungspflichtig (ArbVG § 96a), in der Schweiz gilt das Verbot der Verhaltensüberwachung (ArGV 3 Art. 26). Rechtsstand des Bandes: 27. September 2026.

Was diese Vorlage nicht ist

Diese Vorlage ist kein Rechtsrat und ersetzt weder die ISO/IEC 27001 noch die Risikobeurteilung des Hauses: Sie verlangt keine Software, keinen Katalog und keine bestimmte Bewertungsmethode, und sie führt nicht jede denkbare Bedrohung auf. Sie fragt nach den Risiken, auf die es ankommt, und nach der Entscheidung dessen, der befugt ist. Die Unterschrift macht aus einer Zeile keine Maßnahme. Ein ausgefülltes und unterschriebenes Blatt ist kein Nachweis, solange der Behandlungsplan nicht umgesetzt und bei wesentlichen Änderungen nicht überprüft wird.