ISMS Risk Assessment Matrix

Risikomatrix gemäß ISO 27001

Tomas Jakobs

09.03.2026

Inhaltsverzeichnis

Versionsstand & Änderungsverzeichnis

Versionshistorie und Änderungsnachverfolgung dieses Dokuments erfolgt durch das Versionskontrollsystem der Organisation.[1] Die jeweils gültige Fassung ist durch das Deckblatt und das im Seitenkopf angegebene Dokumentdatum gekennzeichnet.

Datum	Autor	Änderung
09.03.2026	Tomas Jakobs	added pre-processor and snippet git_document_history
08.03.2026	Tomas Jakobs	Update after huge feedback: - pdfcpu post-processor - 2nd document - Support for custom .tex overrides - Support for autogenerating pdf-forms - more frontmatter settings
06.03.2026	Tomas Jakobs	Initial Commit

[1] https://codeberg.org/tomas-jakobs/isms-risk-assessment-matrix

ISMS Risk Assessment Matrix

Risiken werden in der ISMS-Methodik definiert als:

> **Risiko = Wahrscheinlichkeit × Schadenshöhe**

Dieses Dokument stellt eine semiquantitative Risikomatrix zur Bewertung von Informationssicherheitsrisiken in einer Organisation dar.[2] Die Risikobewertung ist Teil eines Informationssicherheitsmanagementsystems (ISMS) und erfolgt gemäß den Anforderungen der ISO/IEC 27001.[3]

Die Organisation adressiert Informationssicherheitsrisiken im Rahmen des ISMS gemäß den Anforderungen zur Behandlung von Risiken und Chancen.[4] Dieses Dokument definiert Kriterien zur Bewertung der Eintrittswahrscheinlichkeit und der Auswirkungen von Informationssicherheitsrisiken.

Die Risikobewertung wird regelmäßig sowie bei wesentlichen Änderungen der organisatorischen oder technischen Rahmenbedingungen überprüft und aktualisiert.[5]

Dieses Dokument ist zur besseren Lesbarkeit im Querformat.

---

[2] gemäß ISO/IEC 27001:2022 Abschnitt 6.1.2 (Information security risk assessment)

[3] gemäß ISO/IEC 27001:2022 Abschnitt 4.4 (Establishing, implementing, maintaining and continually improving an information security management system)

[4] gemäß ISO/IEC 27001:2022 Abschnitt 6.1.2 (Information security risk assessment – identification, analysis and evaluation of information security risks)

[5] gemäß ISO/IEC 27001:2022 Abschnitt 6.1.2 sowie Abschnitt 9.1 und 9.3 (Monitoring, measurement, analysis and evaluation sowie Management review)

Wahrscheinlichkeit

Bestimmung der Eintrittswahrscheinlichkeit eines Ereignisses im Rahmen der Risikobewertung.[6]

Wert	Robustheit	Erfahrungswert	Einschätzung	Rahmenbedingungen
1 (unwahrscheinlich)	Das System arbeitet aktiv gegen den Eintritt des Ereignisses	In der Vergangenheit ist das Ereignis gar nicht oder nur sehr selten aufgetreten	Der Eintritt des Ereignisses im betrachteten Zeitraum wäre eine Überraschung	Das Ereignis kann nur eintreten, wenn spezielle Rahmenbedingungen gegeben sind, die sehr selten sind
2 (möglich)	Das System ist vor dem Eintritt geschützt, allerdings ist dieser Schutz nicht zuverlässig	In der Vergangenheit ist das Ereignis schon aufgetreten	Der Eintritt des Ereignisses wäre keine Überraschung	Die Rahmenbedingungen können in der Praxis vorkommen
4 (wahrscheinlich)	Das System verhindert den Eintritt des Ereignisses nicht	Das Ereignis ist schon häufig aufgetreten	Das Ereignis wird im betrachteten Zeitraum erwartet	Die Bedingungen für den Eintritt sind häufig gegeben
8 (sehr wahrscheinlich)	Das System entwickelt sich zwangsläufig auf den Eintritt des Ereignisses zu	Das Ereignis ist wiederholt aufgetreten oder tritt regelmäßig auf	Das Ereignis wird im betrachteten Zeitraum eintreten	Die Rahmenbedingungen sind permanent gegeben

[6] gemäß ISO/IEC 27001:2022 Abschnitt 6.1.2 a, d und e (Definition von Bewertungskriterien sowie Analyse und Bewertung von Informationssicherheitsrisiken)

Schadenshöhe

Bewertung der Auswirkungen eines Ereignisses auf Organisation, Vermögenswerte und betroffene Personen.[7]

Wert	Geschäftsprozesse	Unternehmenswerte	Gefahr für Leib und Leben	Verstoß gegen Gesetze oder Verträge	Wiederherstellung
1 (vernachlässigbar)	Zentrale Geschäftsprozesse werden nicht gestört	Unternehmenswerte gehen nur in einem geringen Umfang verloren	Es besteht keine Gefahr für Leib und Leben	Es liegen keine Verstöße gegen Gesetze oder Verträge vor	Eine Wiederaufnahme kann im Rahmen des normalen Geschäftsbetriebes geleistet werden
2 (spürbar)	Zentrale Geschäftsprozesse werden zwar gestört, die Störung ist jedoch nicht wesentlich	Unternehmenswerte gehen nicht in einem wesentlichen Umfang verloren	Es besteht keine Gefahr für Leib und Leben	Es liegt ein Verstoß gegen Gesetze oder Normen vor. Die daraus resultierende Haftung ist gering	Der Schaden ist behebbar ohne dass wesentliche Mittel des Unternehmens eingesetzt werden müssen
4 (schmerzhaft)	Der Schaden stört zentrale Geschäftsprozesse empfindlich oder bringt diese zum Erliegen	Es gehen wesentliche Unternehmenswerte verloren	Es können Menschen verletzt werden	Es liegt ein Verstoß gegen Gesetze oder Verträge vor. Die resultierende Haftung ist beträchtlich, jedoch nicht ruinös	Der Schaden kann mit den Mitteln des Unternehmens behoben werden
8 (katastrophal)	Zentrale Geschäftsprozesse werden zum Erliegen gebracht	Es gehen wesentliche Unternehmenswerte verloren oder werden zerstört	Es können Menschen schwer verletzt werden oder ums Leben kommen	Gesetze und Verträge werden gebrochen und die Haftung ist ruinös	Der Schaden kann mit den Mitteln des Unternehmens nicht wieder behoben werden

[7] gemäß ISO/IEC 27001:2022 Abschnitt 6.1.2 a, d und e (Definition von Bewertungskriterien sowie Analyse und Bewertung von Informationssicherheitsrisiken)

Risikobewertung und -behandlung

Einstufung identifizierter Risiken auf Basis der Risikobewertung der vorhergehenden Tabellen.[8]
Zugleich Grundlage zur Priorisierung der Behandlungsreihenfolge.[9]

Wert	Behandlung	Aufwand
1	Risiko akzeptieren	Behandlung nur bei sehr geringem Aufwand
2–4	Risiko kann akzeptiert werden	Behandlung nur bei geringem Aufwand
8	Risiko sollte behandelt werden	Behandlung mit moderatem Aufwand
16–32	Risiko muss behandelt werden	Behandlung auch bei hohem Aufwand notwendig
64	Risiko muss sofort behandelt werden	Behandlung auch bei sehr hohem Aufwand notwendig

[8] gemäß ISO/IEC 27001:2022 Abschnitt 6.1.3 (Information security risk treatment)

[9] gemäß ISO/IEC 27001:2022 Abschnitt 6.1.2 a, d und e (Definition von Bewertungskriterien sowie Analyse und Bewertung von Informationssicherheitsrisiken)

Risiko-Matrix

Darstellung der Risikobewertung als Kombination aus Eintrittswahrscheinlichkeit und Schadenshöhe.[10][11]

	vernachlässigbar (1)	spürbar (2)	schmerzhaft (4)	katastrophal (8)
sehr wahrscheinlich (8)	mittel (8)	hoch (16)	hoch (32)	sehr hoch (64)
wahrscheinlich (4)	gering (4)	mittel (8)	hoch (16)	hoch (32)
möglich (2)	gering (2)	gering (4)	mittel (8)	hoch (16)
unwahrscheinlich (1)	sehr gering (1)	gering (2)	gering (4)	mittel (8)

[10] gemäß ISO/IEC 27001:2022 Abschnitt 6.1.2 a, d und e (Definition von Bewertungskriterien sowie Analyse und Bewertung von Informationssicherheitsrisiken)

[11] gemäß ISO/IEC 27001:2022 Abschnitt 6.1.2 b (Risk acceptance criteria)