

## Risikoanalyse

<b>Schadensausmass</b>	hoch	5	10	15	20	25
		4	8	12	16	20
	mittel	3	6	9	12	15
		2	4	6	8	10
	tief	1	2	3	4	5
		tief		mittel		hoch
		<b>Eintrittswahrscheinlichkeit</b>				

Risikobeschrieb	Auswirkung	Risiko	Massnahmen	Risiko
Schäden durch höhere Gewalt (z.B. Feuer, Wasserschaden)	IT-Systeme können teilweise oder ganz zerstört werden, sodass die Daten nicht mehr abgerufen werden können	8	Feuer- und Wassermelder in Gebäude installieren	4
Stromausfall (partiell oder Totalausfall)	Teil- oder Totalausfall des Systems. Es kann nicht mehr auf die Daten zugegriffen werden	16	Kontrolle/Abnahme Strominstallationen, Notstromaggregate	6
Administratoren haben vollen Zugriff auf alle Systeme.	Administratoren können die Daten manipulieren	10	Vieraugenprinzip, Verschlüsselung der Daten	4
Fehlerhafte Nutzung des Systems	Arbeitsabläufe verzögern sich	6	Geregelte Einarbeitung der Mitarbeiter, Benutzerhandbücher	2
Übertragung falscher Daten	Patienten bekommen falsche Diagnosen und Behandlungen	10	Bessere Einweisung der Mitarbeiter	4
Verlust von gespeicherten Daten	Daten gehen verloren	15	Regelmässige Backups des Systems	6
Das System wird von einem Virus befallen	Datenverlust, Komplettausfall des Systems	20	Regelmässiger Sicherheitscheck des Systems, regelmässiger Einsatz von Viren-Suchprogramme	6
Unzureichende Dokumentation des Systems	Schwierig, das System zu verbessern, da es zu unübersichtlich ist	20	Die Dokumentation besser führen	4
Unabsichtliches Löschen von Daten	Datenverlust	15	Die Rechte werden so vergeben, dass man nicht einfach Daten löschen kann	4
Diebstahl von Daten	Daten kommen in falsche Hände	15	Geräte so platzieren, dass eine unbefugte Kenntnisnahme von Daten durch Besucher ausgeschlossen wird. Sichere Passwörter für das System	3