SiKoSH
SICHERHEIT FÜR KOMMUNEN
IN SCHLESWIG-HOLSTEIN

SiKoSH Leitfaden - Vorgehensweise zur Erstellung eines Sicherheitskonzepts nach SiKoSH

Version:	1.0.0
Datum:	08.03.2018
Kontakt:	KomFIT e.V. Kiel sikosh@KomFIT.de https://www.sikosh.de

Inhalt

1 Allgemeine Hinweise

1.1 Über diese Vorgehensweise zur Erstellung eines Sicherheitskonzepts

Die Erstellung eines Sicherheitskonzepts erfolgt innerhalb einer Institution, wie z.B. einer kommunalen Einrichtung, in der Regel im Anschluss an den Aufbau und der Implementierung der grundlegenden ISMS Einführungsprozesse. Wie ein solches Einstiegs-ISMS effizient eingeführt werden kann, beschreibt der *SiKoSH Standard - Vorgehensweise zur Einführung eines ISMS nach SiKoSH.* In diesem Dokument sind auch alle grundlegenden Erläuterungen zu den Grundlagen der Anwendung von SiKoSH beschrieben.

Es empfiehlt sich den SiKoSH Standard zunächst sorgfältig durchzuarbeiten, bevor mit der Erstellung eines Sicherheitskonzepts begonnen wird. Innerhalb des SiKoSH-Standards sind die für die Erstellung eines Sicherheitskonzepts relevanten Inhalte im Kapitel 6 beschrieben.

1.2 Bearbeitungshinweise

Im Folgenden wird die Symbolik erklärt, welche das Verständnis dieser Vorgehensweise erleichtert.

📖 **[Titel]** Ein solches Buchsymbol signalisiert ein weiterführendes Hilfsmittel, wie z.B. eine anzupassende Vorlage, oder vertiefende Erläuterungen. Alle referenzierten Hilfsmittel sind unter www.sikosh.de veröffentlicht.

Warnung	Vor Fehlern, die bei der Umsetzung von SiKoSH naheliegend sind, wird durch ein solches **Symbol** gewarnt.

Hinweis	Besondere Auswirkungen und Ziele der im vorliegenden Standard definierten Vorgehensweisen werden in einem solchen **Hinweis** erläutert.

Tipp	Wenn bereits Erfahrungswerte bei der Implementierung von SiKoSH vorliegen und damit ein zusätzlicher Nutzen verbunden ist, wird in einem **Tipp** darauf hingewiesen.

2 Vorüberlegungen zur Erstellung eines Sicherheitskonzepts nach SiKoSH

2.1 Erstellung eines institutionsspezifischen Leitfadens

Während in diesem Leitfaden die generelle Vorgehensweise zur Erstellung eines Sicherheitskonzepts erläutert wird, sollte die anwendende Institution innerhalb ihres Sicherheitskonzeptes die genaue, für sie jeweils passende und abgestimmte konkrete Vorgehensweise dokumentieren.

Damit gemeint sind z. B. für die Institution sinnvoll passende Nomenklaturen und Prozessabläufe, Kriterien für Schutzbedarfsfestellungen oder Risikoschwellwerte und Definitionen. Aber auch in der Wahl der weiteren Hilfsmittel zur Erstellung des Sicherheitskonzepts, wie z.B. Excel-Tabellen für Strukturanalyse, Vorlagen für Risikoanalyse oder auch die komplett toolbasierte Erstellung eines Sicherheitskonzepts, ist SiKoSH flexibel.

Die Vorgehensweise für die sich die anwendende Institution entscheidet, kann ebenfalls in den zu erstellenden Sicherheitskonzepten dokumentiert bzw. angepasst werden.

Zu diesem Zweck kann das folgende Hilfsmittel verwendet werden.

🕮 **SiKoSH- Konzept 01000_Sicherheitskonzept**

Tipp	Dieses Hilfsmittel kann parallel während der Durchsicht dieses Leitfadens bearbeitet werden. Es korrespondiert in seiner Struktur, so dass die notwendigen inhaltlichen Anpassungen „on the fly“ stattfinden können.

2.2 Anpassungen dieses Leitfadens durch den SiKoSH Anwender

Während sich die SiKoSH-Dokumente in Dokumente zur Vorgehensweise und Hilfsmittel zur eigenen Anpassung unterteilen, ist dieses Dokument eine Mixform, das heißt neben der Darstellung der Vorgehenseise sind hier auch individuelle Anpassungen möglich und erforderlich.

Dies dient der weiteren Vereinfachung der SiKoSH-Methodik, so kann der Anwender bereits direkt beim Studium dieses Standards beispielsweise die für seine Institution passende Nomenklatur definieren und im weiteren Verlauf der SiKoSH-Umsetzung nutzen. Entsprechende Stellen sind mit folgendem Hinweis gekennzeichnet:

Anpassen durch SiKoSH Anwender

Hinweis	In diesem Leitfaden kann der SiKoSH-Anwender eigene Anpassungen vornehmen und damit seine individuelle Vorgehensweise zur Erstellung eines Sicherheitskonzepts definieren, z. B. durch Anpassung der vorgeschlagenen Nomenklaturen oder Risikostufen.

2.3 Allgemeine Informationen zu Sicherheitskonzepten

Es ist möglich Sicherheitskonzepte in vielfältigen Formen, Ausprägungen und Standards zu erstellen. Dabei können Sicherheitskonzepte streng nach dem IT-Grundschutz Standard des BSI (100-2/3), bzw. 200-2/3) und den darin erläuterten Vorgehensweisen erstellt werden. Ebenso möglich ist es aber die Vorgehensweise um weitere Komponenten wie z.B. Datenflussanalysen und ähnliches zu ergänzen. Die ISO 27001 lässt weiteren Spielraum bei der Durchführung von Risikoanalysen zu. Sofern kein IT-Grundschutzzertifikat angestrebt wird, ist es durchaus möglich, bei der Erstellung von Risikoanalysen z. B. zunächst auf die Anwendung der einzelnen Gefährdungen des BSI IT-Grundschutzes zu verzichten und stattdessen eine freiere Vorgehensweise zu wählen.

Einfach ausgedrückt gibt es nicht DAS Sicherheitskonzept, welches für alle Institutionen und Anwendungsfälle ideal ist. Hier beschrieben wird die Erstellung eines Sicherheitskonzepts, welches sich bewusst an Institutionen und kommunale Anwender wendet, die bei der Erstellung eines Sicherheitskonzeptes zunächst einen einfachen Weg mit niedrigen Einstiegshürden bevorzugen. Natürlich wird dieser Vorteil der Einfachheit mit einer eingeschränkten Anwendbarkeit im Hinblick auf komplexere Fachverfahren oder institutionelle Prozesse (gerade auch mit sehr hohen Schutzbedarfen) erkauft. Weiterhin sind die hier beschriebenen Sicherheitskonzepte noch nicht im Rahmen eines IT-Grundschutzzertifizierungsverfahrens einsetzbar. Auf eine entsprechende „Aufwärtskompatibilität“ wurde aber geachtet, daher können diese somit zu einem späteren Zeitpunkt problemlos erweitert werden. Eine Erweiterung von SiKoSH in einen voll zertifizierungsfähigen BSI IT-Grundschutz ist hiermit problemlos möglich.

Institutionen, die noch gar kein eigenes Sicherheitskonzept haben, sollten zunächst einen sogenannten „IT-Verbund“ definieren. Einfach ausgedrückt den „Scope“ oder den Beschreibungsgegenstand. Es empfiehlt sich mit einem Querschnittsverbund, welcher die Institution in Ihrer Breite, also Ihre Infrastrukturen, IT-Komponenten und Prozesse beschreibt zu beginnen. Wie dies konkret geschieht, wird in diesem Leitfaden beginnend mit dem Kapitel 3.1.4 erläutert.

Warnung	Oftmals gängige Praxis ist es, die Erstellung eines Sicherheitskonzepts im Rahmen des Verfahrensbetriebs vollständig einem Outsourcing Partner zu überlassen. Der Outsourcing Partner kann aber keine Querschnitts-Sicherheitskonzepte für die originären Verantwortungsbereiche der anwendenden Institution, wie z. B. Gebäude, Räume, Personalprozesse usw. erstellen. Daher muss jede Institution zumindest ein eigenes Querschnittskonzept erstellen und pflegen.

Sofern die Erstellung von Sicherheitskonzepten für Fachverfahren nicht sowieso schon durch Outsourcing Partner erfolgt, sollten anschließend kleinere und weniger komplexe Fachverfahren in demselben Querschnittsverbund beschrieben werden, komplexere und größere Fachverfahren können in einem eigenem Sicherheitskonzept beschrieben werden. Hier sind die Grenzen durchaus fließend, es sollte schlicht übersichtlich und für einen fachkundigen Dritten nachvollziehbar bleiben.

Tipp	Bei Unsicherheiten hinsichtlich der genauen Vorgehensweise innerhalb des Sicherheitskonzeptes, bzw. von möglichen Abweichungen zu der hier vorgestellten Vorgehensweise, hilft es, wenn sich SiKoSH Anwender folgende Prüffrage stellen: "Welchen Mehrwert hat die Vorgehensweise für mein Sicherheitskonzept?". Ein Mehrwert kann z.B. eine größere Detailschärfe oder Realitätsnähe und damit Nachvollziehbarkeit auf Seiten eines Lesers oder Prüfers des Konzeptes sein. Ein Mehrwert können auch Sicherheitsmaßnahmen oder –prozesse sein, welche sich aus einer bestimmten Vorgehensweise ableiten und helfen den Reifegrad der Informationssicherheit innerhalb einer anwendenden Institution zu erhöhen.

2.3.1 ISMS-Tool basierte vs. Office-basierte Erstellung von Sicherheitskonzepten.

Grundsätzlich sind eine Reihe von ISMS Tools bzw. IT-Grundschutztools zur Erstellung von Sicherheitskonzepten einsetzbar. Auf den Internetseiten des BSI[1], wird eine regelmäßig gepflegte Toolübersicht angeboten.

Sofern ein SiKoSH Anwender bereits über die Möglichkeit einer toolbasierten Erstellung von Sicherheitskonzepten verfügt, kann er diese Möglichkeit ganz oder teilweise zur Erstellung seiner Sicherheitskonzepte wählen. Zu diesem Zweck werden in den folgenden Erläuterungen jeweils Hinweise zu einer toolgestützten Erstellung eines Sicherheitskonzepts zu finden sein. SiKoSH empfiehlt aus wettbewerbsrechtlichen Gründen kein bestimmtes ISMS / IT-Grundschutztool. Daher werden im folgendem keine dedizierten toolspezifischen Erläuterungen zur Erstellung von Sicherheitskonzepten mit Hilfe eines Tools eines bestimmten Herstellers gegeben.

Tipp	Ein Sicherheitskonzept nach SiKoSH kann somit bereits ohne Tool, nur mit SiKoSH Hilfsmitteln erstellt werden. Es kann jederzeit zu einem späteren Zeitpunkt in einem ISMS- / IT-Grundschutztool weitergeführt werden.

[1] https://www.bsi.bund.de/DE/Themen/ITGrundschutz/GSTOOL/AndereTools/anderetools_node.html

3 Vorgehensweise zur Erstellung eines Sicherheitskonzepts nach SiKoSH

3.1 Strukturanalyse Vorgehen und Nomenklaturen

3.1.1 Vorgehen

Im Rahmen der Strukturanalyse werden die Daten, Informationen und Anwendungen ermittelt und die betroffenen IT-Systeme, Räume, Gebäude und Netze erfasst. Sinnvoll ist es dabei im Allgemeinen, zuerst die Anwendungen und Daten zu ermitteln. Ausgehend von den Anwendungen können dann die weiteren relevanten Zielobjekte erfasst werden. In einigen Fällen kann es aber auch sinnvoll sein, zuerst die die IT-Systeme zu erheben. Grundsätzlich sollte einfach mit den Objekttypen begonnen werden, mit denen ein einfacher Start der Strukturanalyse möglich ist.

Tipp	Sollten innerhalb der SiKoSH anwendenden Institution noch keine oder nur sehr begrenzte Erfahrungen mit Erhebungen von Strukturanalysen vorhanden sein, empfiehlt es sich mit einfach zu ermittelnden Objekttypen, wie z.B. Gebäude und Räume anzufangen. Mit Hilfe dieser Erfahrungen können dann komplexere Objekttypen, wie z.B. Systeme und Anwendungen erhoben werden.

Hinweis	Die hier beschriebene Vorgehensweise ist sowohl für toolbasierte Sicherheitskonzepte, als auch für Sicherheitskonzepte, welche alleine mit SiKoSH Hilfsmitteln erstellt werden, anzuwenden.

Bei der Planung einer Strukturanalyse ist es sinnvoll zu prüfen – insbesondere wenn es sich um einen neuen Informationsverbund handelt – inwieweit bereits vorhandene Datenquellen (z. B. Gerätedatenbanken, Listen, Asset-Management-Systeme, Active Directoryeinträge) genutzt werden können.

Sinnvoll sind weiterhin Netzpläne oder Architekturskizzen, welche innerhalb des Sicherheitskonzeptes eingepflegt werden. So erhält ein fachkundiger Dritter einen besseren Eindruck und Verständnis des Sicherheitskonzepts.

Tipp	Eine Strukturanalyse in Interviewform bei verantwortlichen IT-Leitern, Administratoren und weiteren Ansprechpartnern ist ein geeignetes Mittel, um ein Gefühl für die der Strukturanalyse zugrundeliegende IT-Architektur zu entwickeln

3.1.2 Nomenklaturen innerhalb der Strukturanalyse

Im Folgenden werden der besseren Übersicht halber zunächst einmal alle Nomenklaturen aller relevanten Objekttypen nebst Abbildungen aufgeführt. Im weiteren Verlauf des Kapitels 3 werden diese Objekttypen noch einmal in derselben Reihenfolge aufgeführt. Dann werden Verknüpfungsregeln und Hinweise zur Strukturanalyse besprochen.

Selbstverständlich können SiKoSH Anwender von der vorgestellten Nomenklatur abweichen und beispielsweise andere Kürzel verwenden. Dies wäre dann im Folgenden gesondert zu dokumentieren.

3.1.3 Nummernkreise innerhalb der Strukturanalyse

Jeder SiKoSH-Anwender sollte für die Objekte seines Sicherheitskonzepts einen entsprechenden Nummernkreis wählen (siehe dazu auch Abs. 3.1.4). Die Reihenfolge ist dabei durchaus willkürlich. Es sollte jedoch der besseren Übersicht halber angestrebt werden, größere „Lücken“ in der Nummerierung zu vermeiden.

Die Nummernkreise finden dann auch bei den Objekten Anwendung, welche in einem Verbund angelegt werden. Auch hier ist eine aufsteigende Reihenfolge zu wählen. Es empfiehlt sich aber, entsprechende kleinere „Lücken“ in der Nummerierung zu planen. Der Hintergrund ist der, dass sich im Laufe der Zeit durchaus noch weitere Objekttypen ergeben, welche man gern anhand der Nummernkreise übersichtlich einem Fachverfahren oder einem bestimmten Bereich der Sicherheitskonzeption zuordnen möchte. Daher könnte man, abhängig von der Anzahl der geschätzten zu erwartenden Objekte eines Sicherheitskonzeptes in 10er, 20er oder 50er Schritten neue Objekte anlegen (siehe dazu auch 3.1.9).

Hinweis	Diese Art der „Feinjustierung“ der Objektnummern ist durchaus optional zu sehen. Für SiKoSH-Neueinsteiger mag es zunächst schwierig sein, bei dem einen Anwendungsobjekt z.B. die Objektnummer 01050 und dem Anwendungsobjekt der nächsten Anwendung nun entweder die Objektnummer 01051, 01070 oder 01100 zu vergeben. Hier wird aber nach einiger Übung von ganz alleine der Sinn und Zweck dieser Zuordnung verinnerlicht.

3.1.4 Nomenklatur IT-Verbund

Im folgenden Beispiel wird eine Nomenklatur für IT-Verbünde beschrieben. SiKoSH Anwender sollten eine für Ihre Institution passende Nomenklatur definieren und hier entsprechend definieren.

Anpassen durch SiKoSH Anwender

Name	<5 stellige Nummer>_<Behördenlangname>
Beispiel	01000_ Behörde f. d. Erstellung von Sicherheitskonzepten
Objektkürzel	<5 stellige Nummer>_<SiKoSH Anwenderkürzel>

Tabelle 1 Beispiel-Nomenklatur von IT-Verbünden

Toolgestützte Erstellung

Bei einer toolgestützten Erstellung eines Sicherheitskonzepts, ist der jeweilige IT-Verbund entsprechend zu benennen.

Erstellung nur mit SiKoSH Hilfsmitteln

Sofern für die Erstellung des Sicherheitskonzepts auf ein ISMS-/GS-Tool verzichtet wird, ist der Verbundname zwar nicht in einem gesonderten SiKoSH Hilfsmittel zu dokumentieren, er sollte aber gemäß der definierten Nomenklatur Bestandteil aller Ordner und Dateinamen des Sicherheitskonzepts sein. Diese dienen dann zunächst als prophylaktischer „Verbund“.

Hinweis	Nun wird auch deutlich, welchen Zweck die Nummernkreise, im o.g. Beispiel für die Nomenklatur eines IT-Verbundes „01000“ erfüllen. Jeder IT-Verbund, bzw. jedes weitere IT-Sicherheitskonzept einer Institution kann nun entsprechend „hochgezählt“ werden, so dass der nächste IT-Verbund, bzw. das nächste IT-Sicherheitskonzept die laufende Nummer „02000“ erhalten würde. Alle weiteren Objekte dieses nächsten Sicherheitskonzeptes, wie beispielsweise Gebäude, Räume, Anwendungen, Systeme, Netze usw. würden dann ebenfalls mit „02000er“ Nummern gekennzeichnet werden. Der Vorteil dieser Vorgehensweise ist, dass so auf den ersten Blick zu erkennen ist, zu welchem Verbund oder IT-Sicherheitskonzept die entsprechenden Objekte angehören.

	Die führende „0“ dient übrigens dazu ungewolltes Umsortieren einiger ISMS-/IT-Grundschutztools, bzw. Office-Anwendungen zu vermeiden, wie es der Fall wäre, sobald ein Anwender dann Nummern oberhalb von 9999 verwenden würde.

3.1.5 Nomenklatur Gebäude

Gebäudeobjekte werden wie folgt angelegt.

Anpassen durch SiKoSH Anwender

Name	<SiKoSH Anwenderkürzel>_G_<4-stellige Nummer>_<Straße>_<Hausnummer>_<Funktion>
Bsp.	KomFIT_G_0100_Reventlouallee_6_Bürogebäude
Kürzel	<SiKoSH Anwenderkürzel>_G_<4-stellige Nummer >

Tabelle 2 Nomenklatur allgemeines Gebäude

3.1.6 Nomenklatur Räume

Raumobjekte werden wie folgt angelegt:

Anpassen durch SiKoSH Anwender

Name	<SiKoSH Anwenderkürzel>_R_<Raumnummer>
Bsp.	KomFIT _R_04000_Technikraum
Kürzel	R_<Raumnummer 5-stellig>

Tabelle 3 Nomenklatur Räume

3.1.7 Nomenklatur Netze

Netzobjekte werden wie folgt angelegt. Kommunikationsverbindungen werden analog zu dieser Definition angelegt, lediglich das „N“ wird durch ein „K“ substituiert.

Anpassen durch SiKoSH Anwender

Name	<SiKoSH Anwenderkürzel>_<N_5-stellige Nummer>_<Bezeichnung>
Bsp.	KomFIT_N_04120_WLAN-Router Besprechungsraum R 44

Kürzel	<SiKoSH Anwenderkürzel>_<N_5-stellige Nummer>

Tabelle 4 Nomenklatur Netze

3.1.8 Nomenklatur Daten

Datenobjekte werden wie folgt angelegt:

Anpassen durch SiKoSH Anwender

Name	<SiKoSH Anwenderkürzel>_D<5-stellige Nummer>_<Bezeichnung>
Bsp.	KomFIT _D_01550_Stammdaten-Testanwendung
Kürzel	<SiKoSH Anwenderkürzel>_D_<5-stellige Nummer>

Tabelle 5 Nomenklatur Datenobjekte

3.1.9 Nomenklatur Anwendungen

Anwendungsobjekte werden wie folgt angelegt:

Anpassen durch SiKoSH Anwender

Name	<SiKoSH Anwenderkürzel>_A_<5-stellige Nummer>_<Bezeichnung>
Bsp.	KomFIT_A_07050_Beispielanwendung
Kürzel	<SiKoSH Anwenderkürzel>_A_-<5-stellige Nummer>_<abgekürzte Bezeichnung>

Tabelle 6 Nomenklatur Anwendungen

3.1.10 Nomenklatur Mitarbeiter

Mitarbeiterobjekte werden wie folgt angelegt:

Anpassen durch SiKoSH Anwender

Name	<SiKoSH Anwenderkürzel>_M_<5-stellige Nummer><Bezeichnung>
Bsp.	KomFIT_M_<5-stellige Nummer> IT-Leiter
Kürzel	<SiKoSH Anwenderkürzel>_M_<5-stellige Nummer> <Bezeichnung>

Tabelle 7 Nomenklatur Mitarbeiter

3.1.11 Nomenklatur Systeme

Systemobjekte werden wie folgt angelegt:

Anpassen durch SiKoSH Anwender

Name	<SiKoSH Anwenderkürzel>_S_<5-stellige Nummer>_<Bezeichnung>
Bsp.	KomFIT_S_<5-stellige Nummer>_Client
Kürzel	<SiKoSH Anwenderkürzel>_S_<5-stellige Nummer>_ <Bezeichnung>

Tabelle 7 Nomenklatur Systeme

3.2 Strukturanalyse – Verknüpfungen

Verknüpfungen innerhalb eines Sicherheitskonzepts stellen logische Beziehungen der einzelnen Objekttypen untereinander da. Besonders relevant sind Verknüpfungen für die Vererbung von Schutzbedarfen.

3.2.1 Verknüpfungen IT-Verbund

Toolgestützte Verknüpfung

Bei einer toolgestützten Erstellung sind alle Objekte eines Sicherheitskonzepts mit dem jeweiligen IT-Verbund zu verknüpfen.

Verknüpfung nur mit SiKoSH Hilfsmitteln

Der Verbund wird hier durch das jeweilige Sicherheitskonzeptdokument symbolisiert. Da es alle dem Sicherheitskonzept zugehörigen Objekte enthält, sind dedizierte Verknüpfungen mit einem „Verbundobjekt“ unnötig, da sie nur der Übersichtlichkeit abträglich wären.

3.2.2 Verknüpfungen Gebäude

Toolgestützte Verknüpfung

Bei einer toolgestützten Erstellung werden Gebäude mit allen relevanten Informationsverbünden verknüpft, i.d.R. mit dem entsprechenden SiKoSH Anwenderverbund / Institutionsverbund.

Verknüpfung nur mit SiKoSH Hilfsmitteln

Das Gebäude wird im Hilfsmittel

- 🕮 **SiKoSH- Konzept 01000_Sicherheitskonzept**

innerhalb einer Tabelle mit den relevanten Raumobjekten verknüpft. Ein Raumobjekt ist dann relevant, wenn es einen anderen Objekttyp des Sicherheitskonzepts enthält, wie z.B. ein IT-System.

3.2.3 Verknüpfungen Raum

Toolgestützte Verknüpfung

Räume werden mit dem entsprechenden Gebäude verknüpft. Im Allgemeinen ist ein Raum mit genau einem Gebäude verknüpft.

Verknüpfung nur mit SiKoSH Hilfsmitteln

Räume werden im Hilfsmittel

- 🕮 **SiKoSH- Konzept 01000_Sicherheitskonzept**

innerhalb einer Tabelle mit einem Gebäude verknüpft.

3.2.4 Verknüpfungen IT-Systeme

Toolgestützte Verknüpfung

IT-Systeme werden mit den Räumen verknüpft, die ihrem Standort entsprechen.

IT-Systeme werden mit mindestens einem Netz verknüpft, sofern es sich nicht um stand-alone Systeme handelt.

IT-Systeme können bei Bedarf auch mit anderen IT-Systemen verknüpft werden, dies macht i.d.R. Sinn, sofern virtuelle Maschinen zum Einsatz kommen.

Verknüpfung nur mit SiKoSH Hilfsmitteln

IT-Systeme werden im Hilfsmittel

- 🕮 **SiKoSH- Konzept 01000_Sicherheitskonzept**

innerhalb einer Tabelle mit den entsprechenden Räumen, Netzen und bei Bedarf weiteren Systemen verknüpft, wie oben erläutert.

3.2.5 Verknüpfungen Netze

Toolgestützte Verknüpfung

Netze werden mit den IT-Systemen verknüpft, die Teil des jeweiligen Netzes sind.

Der Subtyp Kommunikationsverbindungen wird dann gewählt, wenn man verdeutlichen will, dass besonders kritische Informationen von einem System zum nächsten, eventuell über besondere Netze wandern. Die Endpunkte der Kommunikationsverbindungen sind also ebenfalls mit den IT-Systemen und dem oder den entsprechenden Netzen zu verknüpfen.

Verknüpfung nur mit SiKoSH Hilfsmitteln

Netze werden im Hilfsmittel

- 🕮 **SiKoSH- Konzept 01000_Sicherheitskonzept**

innerhalb einer Tabelle mit den entsprechenden IT-Systemen verknüpft, wie oben erläutert.

3.2.6 Verknüpfungen Anwendungen

Toolgestützte Verknüpfung

Anwendungen werden mit den IT-Systemen verknüpft, die für die Ausführung der Anwendung erforderlich sind.

Anwendungen können auch mit Anwendungen verknüpft werden, wenn diese stark voneinander abhängen. Bei der Verknüpfung von Anwendungen mit Anwendungen kann, je nach Toolhersteller, die Richtung der Verknüpfung für die Darstellung des Abhängigkeitsverhältnisses für die Vererbung von Schutzbedarfen entscheidend sein. Es wird dann zwischen der Datenquelle und der Datensenke differenziert.

Verknüpfung nur mit SiKoSH Hilfsmitteln

Anwendungen werden im Hilfsmittel

- 🕮 **SiKoSH- Konzept 01000_Sicherheitskonzept**

innerhalb einer Tabelle mit den entsprechenden IT-Systemen verknüpft. Auf eine Verknüpfung von Anwendungen untereinander wird allerdings verzichtet. Eine solche Komplexität wäre innerhalb einer Office Vorlage nur schwer nachvollziehbar und der Mehrwert für das Sicherheitskonzept wäre überschaubar.

3.2.7 Verknüpfungen Mitarbeiter

Toolgestützte Verknüpfung

Die Verknüpfung von Mitarbeitern zu Zielobjekten sollte möglichst über eine generische Bezeichnung, z.B. einer Organisationseinheit oder Stabsstelle, geschehen. Auf Verknüpfungen von Klarnamen oder natürlichen Personen sollte möglichst verzichtet werden. Damit bleibt ein IT-Sicherheitskonzept langlebig und unabhängig von aktuellen Personalien.

Die Verknüpfungen von Mitarbeitern oder Organisationseinheiten bleibt innerhalb der SiKoSH Vorgehensweise allerdings optional. Diese sollte nur verknüpft werden, wenn damit ein deutlicher Mehrwert für das Sicherheitskonzept erzeugt wird. Dies kann z.B. der Fall sein, wenn man verdeutlichen möchte, dass externe Administratoren sensible Daten administrieren.

Verknüpfung nur mit SiKoSH Hilfsmitteln

Auf eine Verknüpfung von Mitarbeiterobjekten wird hier verzichtet. Eine solche Komplexität wäre innerhalb einer Office Vorlage nur schwer nachvollziehbar und der Mehrwert für das Sicherheitskonzept überschaubar.

3.2.8 Verknüpfungen Daten

Toolgestützte Verknüpfung

Datenobjekte sollten mit den Anwendungen verknüpft werden, von denen sie verarbeitet werden.

Datenobjekte sollten mit den Kommunikationsverbindungen verknüpft werden, über die sie übertragen werden.

Verknüpfung nur mit SiKoSH Hilfsmitteln

Datenobjekte werden im Hilfsmittel

- 🕮 **SiKoSH- Konzept 01000_Sicherheitskonzept**

innerhalb einer Tabelle mit den entsprechenden Anwendungen und Kommunikationsverbindungen verknüpft.

3.3 Schutzbedarfsfeststellungen

In diesem Kapitel wird die Logik von Schutzbedarfsfestellungen und deren Vererbung erläutert. Innerhalb der SiKoSH Vorgehensweise sollte i.d.R. mit der Feststellung des Schutzbedarfs von Datenobjekten begonnen werden, da diese initial ihren Schutzbedarf weiter vererben.

3.3.1 Schutzbedarfsfeststellung für Daten

Toolgestützte Schutzbedarfsfeststellung

Innerhalb eines ISMS-/IT-Grundschutztools kann der Schutzbedarf der primären Informationssicherheitswerte Vertraulichkeit und Integrität in den entsprechenden Feldern dokumentiert werden. In den meisten gängigen Tools können diese Schutzbedarfe direkt begründet werden, bzw. auf eine externe Schutzbedarfsfeststellung verwiesen werden.

Bei Datenobjekten sollte auf eine Feststellung des Schutzbedarfs des primären Informationssicherheitsgrundwerts „Verfügbarkeit“ verzichtet werden. Dieser sollte erst im weiteren Verlauf der Sicherheitskonzepterstellung während der Schutzbedarfsfeststellung für Anwendungen ermittelt werden.

Schutzbedarfsfeststellung nur mit SiKoSH Hilfsmitteln

Schutzbedarfsfestellungen für Datenobjekte werden im Hilfsmittel

- 🕮 **SiKoSH- Konzept 01000_Sicherheitskonzept**

innerhalb einer Tabelle gemäß der oben erläuterten Vorgehensweise festgestellt und dokumentiert.

3.3.2 Schutzbedarfsfeststellung für Anwendungen

Toolgestützte Schutzbedarfsfeststellung

Wie bereits innerhalb des Abschnitts 3.3.1. erläutert, wird der Schutzbedarf von Vertraulichkeit und Integrität von den in den in der Anwendung verarbeiteten Daten vererbt. Innerhalb eines ISMS-/IT-Grundschutztools kann dem Vorschlag i.d.R. gefolgt werden. Allerdings sind mögliche Kumulationseffekte einzelner Schutzbedarfe von Datenobjekten, hin zu einem höheren Gesamtschutzbedarf eines Anwendungsobjekts zu beachten.

Der Schutzbedarf der Verfügbarkeit sollte im Anwendungsobjekt festgestellt werden. Begründet wird diese Vorgehensweise damit, dass primär die Anwendung verfügbar sein soll, nicht deren Daten oder Systeme, die z.B. redundant sein können.

Schutzbedarfsfeststellung nur mit SiKoSH Hilfsmitteln

Schutzbedarfsfestellungen für Datenobjekte werden im Hilfsmittel

🕮 **SiKoSH- Konzept 01000_Sicherheitskonzept**

innerhalb einer Tabelle gemäß der oben erläuterten Vorgehensweise festgestellt und dokumentiert.

3.3.3 Schutzbedarfsfeststellung für IT-Systeme

Toolgestützte Schutzbedarfsfeststellung

IT-Systeme erben ihren Schutzbedarf von der (den) mit ihnen verknüpften Anwendung(en) und damit von den in dieser(n) Anwendung(en) verarbeiteten Daten. Sofern kein anderer Schutzbedarf definiert wird, wird der Schutzbedarf der Anwendung(en) übernommen. Dazu kann je nach verwendetem der Schutzbedarf des Feldes „Vorschlag“ als Schutzbedarf beim jeweiligen Grundwert ausgewählt werden. Als Begründung wird „Maximumprinzip“ eingetragen.

Der Schutzbedarf eines IT-Systems in einem Grundwert kann vom Schutzbedarf der Anwendung abweichen (z. B. aufgrund von Verteilungs- oder Kumulationseffekten). Dann kann diese Abweichung durch Auswahl des Schutzbedarfs und entsprechender Begründung für diesen Grundwert dokumentiert werden.

Hinweis	Verteilungseffekte sind häufig bei der Vererbung von Schutzbedarfen des Informationssicherheitswerts Verfügbarkeit anzutreffen, wenn z.B. mehrere IT-Systeme eine Anwendung redundant halten. Kumulationseffekte sind häufig bei der Vererbung von Vertraulichkeiten festzustellen, wenn z. B. mehrere Datenobjekte zusammengenommen eine höheren Schutzbedarf aufweisen als für sich alleine.

Schutzbedarfsfeststellung nur mit SiKoSH Hilfsmitteln

Schutzbedarfsfestellungen für IT-Systemen werden im Hilfsmittel

🕮 **SiKoSH- Konzept 01000_Sicherheitskonzept**

innerhalb einer Tabelle gemäß der oben erläuterten Vorgehensweise festgestellt und dokumentiert.

3.3.4 Schutzbedarfsfeststellung für Netze und Kommunikationsverbindungen

Toolgestützte Schutzbedarfsfeststellung

Netzobjekte und Kommunikationsverbindungen erben ihren Schutzbedarf von den mit Ihnen verknüpften IT-Systemen. In der Regel kann innerhalb eines Tools der Schutzbedarf am Netzobjekt abweichend begründet oder mit Hilfe des Maximumprinzips von verknüpften Objekten abgeleitet werden.

Schutzbedarfsfeststellung nur mit SiKoSH Hilfsmitteln

Schutzbedarfsfestellungen für Netze und Kommunikationsverbindungen werden im Hilfsmittel

- 🕮 **SiKoSH- Konzept 01000_Sicherheitskonzept**

innerhalb einer Tabelle gemäß der oben erläuterten Vorgehensweise festgestellt und dokumentiert.

3.3.5 Schutzbedarfsfeststellung für Gebäude und Räume

Toolgestützte Schutzbedarfsfeststellung

Ein Raum erbt grundsätzlich den Schutzbedarf des in ihm verarbeiteten / enthaltenen Objektes, i.d.R. eines IT-Systems entsprechend des Maximumprinzips. Mögliche Kumulationseffekte sollten berücksichtigt werden.

Gebäude wiederum erben den Schutzbedarf der Räume, welcher ebenfalls mit dem Maximumprinzip zu dokumentieren ist. Auch hier sind mögliche Kumulationseffekte zu berücksichtigen.

Schutzbedarfsfeststellung nur mit SiKoSH Hilfsmitteln

Schutzbedarfsfestellungen für Gebäude und Räume werden im Hilfsmittel

- 🕮 **SiKoSH- Konzept 01000_Sicherheitskonzept**

innerhalb einer Tabelle gemäß der oben erläuterten Vorgehensweise festgestellt und dokumentiert.

3.4 Schutzbedarfsklassifikation

3.4.1 Definition der Schutzbedarfskategorien

Die SiKoSH-anwendende Institution sollte die von ihr verwendeten Schutzbedarfskategorien normal, hoch und sehr hoch definieren und den folgenden Vorschlag ggf. auf ihre institutionsspezifischen Bedürfnisse anpassen. Die Anpassung kann direkt in diesem Leitfaden vorgenommen werden und anschließend in einer institutionsspezifischen Version 2.0 dieses Leitfadens weiter verwendet werden.

Anpassen durch SiKoSH Anwender

Schutzbedarf / Kriterien	normal	hoch	sehr hoch
Verstoß gegen Gesetze, Verträge, internes Regelwerk	• Verstöße mit geringfügigen Konsequenzen • Haftungsschäden sind geringfügig	• Verstöße mit erheblichen Konsequenzen • Haftungsschäden sind erheblich	• Fundamentaler Verstoß gegen Rechtsvorschriften • Haftungsschäden sind existenzbedrohend
Beeinträchtigung des Rechts auf informationelle Selbstbestimmung	Personenbezogene Daten, durch deren Missbrauch die/der Betroffene in ihrer/seiner gesellschaftlichen Stellung oder den wirtschaftlichen Verhältnissen beeinträchtigt werden kann.	Personenbezogene Daten (**insb. besondere Arten**[2]), durch deren Missbrauch die/der Betroffene in ihrer/seiner gesellschaftlichen Stellung oder den wirtschaftlichen Verhältnissen erheblich beeinträchtigt werden kann.	Personenbezogene Daten **insb. besondere Arten**, durch deren Missbrauch die/der Betroffene in ihrer/seiner gesellschaftlichen Stellung oder den wirtschaftlichen Verhältnissen ruinös beeinträchtigt werden kann.
Beeinträchtigung der persönlichen Unversehrtheit	Beeinträchtigung erscheint nicht möglich.	Beeinträchtigung kann nicht absolut ausgeschlossen werden.	Gravierende Beeinträchtigung ist möglich (**Gefahr für Leib und Leben**).
Beeinträchtigung der Aufgabenerfüllung	• Die Beeinträchtigung würde von Betroffenen als tolerabel eingeschätzt werden. • tolerierbare **Ausfallzeit > 24 Std**.[3]	• Die Beeinträchtigung würde von einzelnen Betroffenen als nicht tolerabel eingeschätzt. • tolerierbare **Ausfallzeit > 1 Std. und < 24 Std**.	• Die Beeinträchtigung würde von allen Betroffenen als nicht tolerabel eingeschätzt. • tolerierbare **Ausfallzeit < 1 Std**.
Negative Innen- oder Außenwirkung	Eine **geringe Ansehens- oder Vertrauensbeeinträchtigung** ist zu erwarten.	Eine **breite Ansehens- oder Vertrauensbeeinträchtigung** ist zu erwarten.	Eine **öffentliche Ansehens- oder Vertrauensbeeinträchtigung**, evtl. sogar **existenzgefährdender** Art, ist denkbar.
Finanzielle Auswirkungen	• Der Schaden bewirkt geringe finanzielle Verluste. • finanzieller Schaden in € **bis 5% vom Umsatz/Budget**	• Der Schaden bewirkt beachtliche finanzielle Verluste, ist jedoch nicht existenzbedrohend. • finanzielle Schaden in € **von 5% bis 10% vom Umsatz/Budget**	• Der finanzielle Schaden ist für die Institution existenzbedrohend. • finanzielle Schaden in € **mehr als 10% vom Umsatz/Budget**
Unberechtigte Offenlegung vertraulicher Informationen	Offenlegung interner Daten erscheint möglich	Offenlegung vertraulicher Daten erscheint möglich	Offenlegung streng vertraulichen Daten erscheint möglich

[2] Wie beispielsweise Daten die spezifischen Amtsgeheimnissen unterliegen (Steuerdaten, Sozialdaten etc.), Gesundheitsdaten, Sexuelle Präferenzen, Gewerkschaftszugehörigkeit, Religion, etc.

[3] Achtung: Dies bedeutet einen beliebig langen Ausfall!

3.5 Modellierung

Toolgestützte Modellierung

Mit Hilfe der Modellierung wird der betrachtete Informationsverbund mittels IT-Grundschutz Bausteinen abgebildet. Diese können innerhalb eines ISMS-/IT-Grundschutztools oftmals direkt im Rahmen einer Strukturanalyse schon vorausgewählt und in der eigentlichen Modellierungsphase nachdefiniert werden.

Eine toolbasierte Modellierung hängt direkt von den jeweiligen Methoden und Herangehensweisen des jeweils verwendeten ISMS-/IT-Grundschutztools ab. In einem solchen ist daher i.d.R. auch wenig Spielraum für SiKoSH spezifische Herangehensweisen, sofern SiKoSH nicht explizit unterstützt wird. Daher wird an dieser Stelle nicht weiter auf eine mögliche toolgestützte Modellierungsphase eines Sicherheitskonzepts eingegangen.

Modellierung nur mit SiKoSH Hilfsmitteln

3.5.1 Alternative 1 – Maßnahmenmodellierung nach dem alten IT-Grundschutzkatalog

Eine Modellierung mit SiKoSH Hilfsmitteln wird initial im Hilfsmittel

📖 **SiKoSH- Empfehlung Maßnahmenklassifikation-und-Bewertung**

durchgeführt.

Eine detaillierte Anleitung zur Nutzung dieses Hilfsmittels kann in der folgenden Vorgehensweis gefunden werden.

📖 **SiKoSH- Handreichung Maßnahmenklassifikation-und-Bewertung**

Auszugsweise aus der o.g. Handreichungen seien die drei möglichen Vorgehensweisen aufgeführt. Die anwendende Institution sollte sich für eine der Vorgehensweisen entscheiden, im folgendem bzw. einen Zeitplan für die sukzessive Umsetzung der möglichen fünf SiKoSH-Umsetzungsstufen definieren.

1. Die erste SiKoSH Umsetzungsstufe wird mit der Implementierung der Quickchecks wie im SiKoSH Standard Vorgehensweise zur Einführung eines ISMS nach SiKoSH beschrieben.

2. SiKoSH empfiehlt einen Einstieg in die Sicherheitskonzepterstellung mit den Maßnahmen aus dem ISIS 12 – Katalog des Bayerischen IT-Sicherheitsclusters e. V. In der o.g. Handreichung wird eine entsprechende Filtermöglichkeit beschrieben.

3. SiKoSH empfiehlt als Ziel mindestens die Stufe SiKoSH 2 anzustreben. Diese beinhaltet als Stufe 1 neben den ISIS 12 – Maßnahmen auch weitere Empfehlungen des Unabhängigen Landeszentrums für Datenschutz (ULD) und des Landesrechnungshofs (LRH). In der o.g. Handreichung wird eine entsprechende Filtermöglichkeit beschrieben.

4. Je nach örtlichen Gegebenheiten und dem Schutzbedarf kann die Einbeziehung weiterer Maßnahmen das Sicherheitsniveau weiter erhöhen. In der o.g. Handreichung wird eine entsprechende Filtermöglichkeit beschrieben.

5. Die Umsetzung alle BSI IT-Grundschutzmaßnahmen würde zu einer Stufe 5 und damit zu einer Umsetzung des BSI IT-Grundschutzstandards führen, soweit alle weiteren SiKoSH Anforderungen der SiKoSH Standards umgesetzt wurden.

Das Hilfsmittel enthält zur Zeit noch Maßnahmen aus dem alten IT-Grundschutzkatalog. Das modernisierte IT-Grundschutzkompendium wird zu einem späteren Zeitpunkt implementiert.

3.5.1.1 Zuordnung der Modellierung zur Strukturanalyse

Toolgestützte Modellierung

Moderne ISMS-/IT-Grundschutztools verbinden die notwendigen Bausteine direkt mit dem in der Strukturanalyse erhobenen Objekt. Eine weitere, manuelle Zuordnung von Bausteinen / Maßnahmen zu einem einzelnen Objekt ist damit nicht notwendig.

Modellierung nur mit SiKoSH Hilfsmitteln

Eine initiale Modellierung kann durch eine Beschränkung der gefilterten Bausteine im Hilfsmittel

🕮 **SiKoSH- Empfehlung Maßnahmenklassifikation-und-Bewertung**

erfolgen. Damit können zunächst zu der Strukturanalyse gar nicht passende Bausteine ausgeschlossen werden. Ein einfaches, plausibles Beispiel dafür wäre der Ausschluss von Bausteinen wie z.B. Active Directory oder Email oder Rechenzentrum, wenn diese gar nicht von der anwendenden Institution betreiben werden, sondern von einem Outsourcing Dienstleister.

Nun unterteilt sich die weitere Vorgehensweise in zwei Varianten

Modellierungen innerhalb kleinerer und einfacherer Informationsverbünde

Hier kann einfach wie oben beschrieben, dass Hilfsmittel

🕮 **SiKoSH- Empfehlung Maßnahmenklassifikation-und-Bewertung**

genutzt werden, um eine initiale Filterung der relevanten Bausteine vorzunehmen und die gefilterten Maßnahmen aus der Spalte C in die Anlage 1 des Hilfsmittels

🕮 **SiKoSH- Konzept 01000_Sicherheitskonzept**

zu kopieren.

Bei dieser Variante wird davon ausgegangen, dass entweder jeder Baustein nur jeweils einmal im Informationsverbund vorkommt, bzw. alle gleichartigen Objekte in der Strukturanalyse des Sicherheitskonzeptes denselben Umsetzungstand der Maßnahmen aufweisen.

Modellierungen innerhalb größerer und komplexerer Informationsverbünden

Auch hier kann einfach wie oben beschrieben, dass Hilfsmittel

> 🕮 **SiKoSH- Empfehlung Maßnahmenklassifikation-und-Bewertung**

genutzt werden um eine initiale Filterung zu erstellen. Allerdings wird hier von der Annahme ausgegangen, dass die Bausteine mehrfach innerhalb des Informationsverbunds direkt an die jeweiligen Objekte der Strukturanalyse modelliert werden sollten, da Bausteine mehrfach an völlig verschiedenen Objekten mit unterschiedlichen Umsetzungsständen von Maßnahmen vorkommen. Die Beschreibung der Umsetzung der Maßnahmen ist jeweils so spezifisch, dass eine allgemeine Beschreibung für unterschiedliche Typen nicht mehr ausreichend ist.

Hier kann in der o.g. Empfehlung auf den jeweiligen Baustein gefiltert werden und die Maßnahmen der Spalte C direkt unterhalb der Strukturanalyse des jeweiligen Bausteins innerhalb des Hilfsmittels

> 🕮 **SiKoSH- Konzept 01000_Sicherheitskonzept**

kopiert werden.

3.5.2 Alternative 2 – Maßnahmenmodellierung nach dem kommunalem Profil des neuen IT-Grundschutzkompendiums

Toolgestützte Modellierung

Moderne ISMS-/IT-Grundschutztools verbinden die notwendigen Bausteine direkt mit dem in der Strukturanalyse erhobenen Objekt. Eine weitere, manuelle Zuordnung von Bausteinen / Maßnahmen zu einem einzelnen Objekt ist damit nicht notwendig.

Modellierung nur mit SiKoSH Hilfsmitteln

Eine initiale Modellierung

Innerhalb des Kapitels 2.2 des Hilfsmittels

> 🕮 **SiKoSH- Konzept 01000_Sicherheitskonzept**

wurde bereits ein Verbund (Baustein und Anforderungsmodellierung) auf Grundlage des Entwurfs des kommunalen Grundschutzprofils vormodelliert. Dieser kann einfach ausgefüllt werden und damit der Umsetzungstand der IT-Grundschutzanforderungen dokumentiert werden.

Bei Bedarf kann diese Vormodellierung gemäß der üblichen IT-Grundschutzvorgehensweise um ganze Bausteine oder auch einzelne Anforderungen ergänzt werden.

3.6 Basis-Sicherheitscheck / Dokumentation der Maßnahmenumsetzung

Der Umsetzungsgrad aller modellierten Maßnahmen sollte mit den Umsetzungsstufen

- Ja
- Teilweise
- Nein
- Entbehrlich

dokumentiert werden.

Toolgestützter Basis-Sicherheitscheck.

Moderne ISMS-/IT-Grundschutztools bieten zahlreiche Möglichkeiten den Umsetzungsstand einzelner Maßnahmen toolgestützt zu dokumentieren. Die exakte Ausprägung hängt von dem jeweils verwendeten Tool ab.

Basis-Sicherheitscheck mit SiKoSH Hilfsmitteln

Ein erster rudimentärer Basis-Sicherheitscheck ist bereits innerhalb der Quickcheck Phase, wie innerhalb des

🕮 **SiKosH Standard -Vorgehensweise zur Einführung eines ISMS nach SiKoSH**

beschrieben, erfolgt.

Nun können die, je nach SiKoSH-Stufe ausgewählten, modellierungsspezifischen Maßnahmen, wie im Kapitel 3.5.1.1 beschrieben, ausgewählt und dokumentiert werden. Die Dokumentation sollte direkt innerhalb der Maßnahmentabelle, welche unterhalb der Strukturanalyse des jeweiligen Bausteins innerhalb des Hilfsmittels

🕮 **SiKoSH- Konzept 01000_Sicherheitskonzept**

kopiert wurde, dokumentiert werden.

Sofern die Vorgehensweis nach Alternative 2, wie oben beschrieben gewählt wurde, kann einfach die vormodellierte Tabelle innerhalb des Hilfsmittels unter Kapitel 2.2 genutzt werden.

3.7 Risikoanalyse

Eine Risikoanalyse nach SiKoSH erfolgt im Wesentlichen wie in den BSI Standards 100-3, bzw. 200-3 beschrieben. Alle Objekte mit hohen Schutzbedarfen sollten bei Bedarf einer Risikoanalyse unterzogen werden. Ausnahmen sind Gleichartigkeiten zu bereits analysierten Objekten, wo eine weitere Risikoanalyse keinen neuen Erkenntnisgewinn mit sich bringen würde.

3.7.1 Risikomatrix

Zu diesem Zweck sollte die anwendende Institution im Folgenden Ihre spezifischen Risikoschwellwerte innerhalb einer Risikomatrix definieren.

Die folgende Matrix soll Eintrittswahrscheinlichkeiten und Schadensausmaß kategorisieren.

Wichtig ist die Unterscheidung zur Schutzbedarfsfeststellung. Zwar mag eine Schutzbedarfsfeststellung Indikative Wirkung ausüben, letztlich ist aber der Schaden, der aus einer konkreten Gefährdung resultiert, völlig unabhängig von der Schutzbedarfsfeststellung zu bewerten.

Sollten in der Schutzbedarfsfeststellung finanzielle Risiken benannt worden sein, können diese ggf. in die Risikomatrix übernommen werden.

Anpassen durch SiKoSH Anwender

Risikomatrixen gibt es in unterschiedlichen Ausprägungen. Der SiKoSH-Anwender kann bei Bedarf an dieser Stelle auch eine Matrix seiner Wahl dokumentieren, sollte diese besser zu seiner Institution passen.

Eintrittswahrscheinlichkeit **Auswirkung**	**1: Selten** (0 - 5%) Bei Bedarf sind die Prozentwerte anzupassen.	**2: Gering** (YX-40%) Bei Bedarf sind die Prozentwerte anzupassen.	**3: Mittel** (XY-60%) Bei Bedarf sind die Prozentwerte anzupassen.	**4: Hoch** (XY-90%) Bei Bedarf sind die Prozentwerte anzupassen.	**5: Nahezu sicher** (XY-99%) Bei Bedarf sind die Prozentwerte anzupassen.
5: Sehr hoch (≥ XY Mio. €) Bei Bedarf weitere Indikatoren, siehe z.B. Kapitel 3.4.1	**3**	**4**	**4**	**5**	**5**
4: Hoch (X bis <XY Mio. €) Bei Bedarf weitere Indikatoren, siehe z.B. Kapitel 3.4.1	**2**	**3**	**3**	**4**	**5**
3: Mittel (X00.000€ bis <X Mio. €) Bei Bedarf weitere Indikatoren, siehe z.B. Kapitel 3.4.1	**2**	**2**	**3**	**3**	**4**
2: Gering (XY.000 bis < X00.000€)	**1**	**2**	**2**	**2**	**3**

Bei Bedarf weitere Indikatoren, siehe z.B. Kapitel 3.4.1					
1: Unbedeutend (<X0.000€) Bei Bedarf weitere Indikatoren, siehe z.B. Kapitel 3.4.1	**0**	**1**	**1**	**2**	**3**

Der SiKoSH Anwender sollte hier seinen Schwellwert definieren, ab dem Risiken und Restrisiken nicht akzeptabel sind, ein gängiger Wert wäre die Stufe höher als „2“, mittleres Risiko.

Risikostufen:

- **0**: entfallenes Risiko
- **1**: unbedeutendes Risiko
- **2**: mittleres Risiko
- **3**: bedeutendes Risiko
- **4**: beeinträchtigendes Risiko
- **5**: schwerwiegendes Risiko

3.7.2 Dokumentation einer Risikoanalyse

Die folgende Tabelle stellt einen Auszug aus Hilfsmittel

📖 **SiKoSH- Konzept 01000_Sicherheitskonzept**

dar.

2 Risikoanalyse zu Objekt: KomFIT_G_0100_Reventlouallee_6_Bürogebäude

Lfd.-Nr.	Generische Gefährdung	Mögliche risikomindernde Maßnahmen	Eintrittswahrscheinlichkeit[4]		Schaden[5]		Gesamtrisiko[6]		Risikobehandlung (RB) (a[7], b[8], c[9], d[10])	Managemententscheidung: Maßnahmen umsetzen / Restrisiko tragen	
			Vor RB	Nach RB	Vor RB	Nach RB	Vor RB	Nach RB			
1	G 0.1 Feuer Durch das Fehlen einer Feuerlöschanalage und veralteter Feuerlöscher ist die Gefährdung erhöht.	Organisatorische Maßnahme: Besuchern werden Feuerzeuge abgenommen und das Aufstellen von Adventskränzen verboten.	3	1	2	1	2	1	c	Auftraggeber bitte mit ja oder nein ausfüllen.	./.
	G 0.2 Ungünstige klimatische Bedingungen	./.	./.	./.	./.	./.	./.	./.	./.	./.	./.

[4] Auf einer Skala von 0 bis 5: selten, gering, mittel, hoch, nahezu sicher
[5] Auf einer Skala von 0 bis 5: unbedeutend, gering, mittel, hoch, existenzbedrohend
[6] Auf einer Skala von 0 bis 5: entfallen, gering, mittel, hoch, sehr hoch (Eintrittswahrscheinlichkeit x Schaden)
[7] Risikomindernde Maßnahmen
[8] Risikovermeidung
[9] Risikoakzeptanz
[10] Risikotransfer

	Die Gefährdung ist nicht relevant, in Schleswig Holstein ist immer gutes Wetter.										
	Usw.										

Die Werte des Beispiels der oben gezeigten Tabelle können verwendet werden, um Eintrittswahrscheinlichkeiten und Schadensausmaß zu quantifizieren. Sobald ein nicht ausreichender Schutz festgestellt wird, ist dies in der Gefährdung im Feld „Begründung“ entsprechend zu dokumentieren.

Dokumentationsbeispiel:

Eintrittswahrscheinlichkeit (vor Maßnahmenumsetzung) 2

Schadensausmaß (v.M.): 4

Gesamtrisiko (v.M.): 3

Eintrittswahrscheinlichkeit (nach Maßnahmenumsetzung) : 1

Schadensausmaß (n.M.): 2

Restrisiko (n.M.): 1

3.7.3 Zyklen von Risikoanalysen

Alle Risikoanalysen sind innerhalb eines Zeitraums von maximal zwei Jahren zu aktualisieren. Dieser Revisionsprozess ist geeignet zu dokumentieren.

2 Versionierung

0.1	Anpassung	[Datum]	[Bearbeiter]