SiKoSH
SICHERHEIT FÜR KOMMUNEN
IN SCHLESWIG-HOLSTEIN

Vorgehensweise: Einführung eines Informationssicherheitsmanagementsystems (ISMS)

Version:	1.2
Datum:	14.08.2018
Herausgeber:	Kommunales Forum für Informationstechnik (KomFIT e.V.) Reventlouallee 6 24105 Kiel sikosh@komfit.de https://www.sikosh.de

Inhalt

1 Allgemein

1.1 Übersicht für die Leitungsebene

Im Rahmen ihrer Organisationsverantwortung trägt die Behördenleitung neben der Verantwortung zur Umsetzung bestehender Gesetze (wie z. B. die Datenschutzgesetze) auch die Verantwortung zur Gewährleistung der Informationssicherheit. Hierzu ist es erforderlich, in den Verwaltungen ein Informationssicherheitsmanagementsystem (ISMS) aufzubauen und zu betreiben. Das Projekt SiKoSH (Sicherheit für Kommunen in Schleswig-Holstein) der Kommunalen Landesverbände hat es sich zur Aufgabe gesetzt, hierbei zu unterstützen.

Der vorliegende Standard (RK) bildet die Klammer für die Aktivitäten und Ergebnisse des Projektes SiKoSH. Es ersetzt nicht etablierte Standards wie die ISO27001 oder IT-Grundschutz, sondern referenziert ergänzende Hilfen, die im Rahmen des Projektes erzeugt oder bei Kooperationen mit Dritten zur Verfügung gestellt wurden. SiKoSH beleuchtet das Themenfeld Informationssicherheit in seiner gesamten Breite und berücksichtigt dabei auch Sicherheits- und Datenschutzaspekte, die neben der klassischen IT-Sicherheit zu beachten sind.

Der Standard soll den Verantwortlichen, insbesondere den Sicherheitsbeauftragten der Kommunen, einen Überblick über die Hilfsmittel bereitstellen und so den Einstieg in die Verwendung erleichtern. Für spezifische Anwendungszwecke und Fragestellungen dient der Standard ferner als "Wegweiser" durch die Hilfsmittel.

Die Fortschreibung und Pflege des Standards erfolgt aktuell innerhalb von Projektstrukturen (Projekt SiKoSH). Zukünftig soll die Pflege und Weiterentwicklung in einem Arbeitskreis der Kommunalen Sicherheitsbeauftragten weitergeführt werden. Das Standard und die Hilfsmittel werden sukzessive fortgeschrieben.

1.2 Länderübergreifende Kooperationen

Deutschlandweit gibt es gegenwärtig einige vergleichbare öffentliche Projekte zur Verbesserung der Informationssicherheit. Das Projekt SiKoSH nutzt gezielt Kooperationen, um Bewährtes zu adaptieren. Im Gegenzug sollen eigene Hilfsmittel, Regelungen und Konzepte den Kooperationspartnern zugänglich gemacht werden.

Gegenwärtig bestehen Kooperationen mit der Securion Rheinland-Pfalz GmbH (Projekt ISK.RLP), mit dem Bayerischen IT-Sicherheitscluster (ISIS 12) als auch mit der Finanzbehörde Hamburg.

1.3 Vereinfachtes Vorgehensmodell

Als weiterführende und vertiefende Vorgehensweise zum Aufbau und Betrieb eines Sicherheitsmanagementsystems wird die Vorgehensweise nach dem IT-Grundschutzstandards des Bundesamtes für Sicherheit in der Informationstechnik (BSI) empfohlen.

Im Oktober 2017 hat das BSI im Rahmen der Sicherheitsmesse das IT-Grundschutz-Kompendium veröffentlicht. Dieses ersetzt die bisher bekannten IT-Grundschutzkataloge. Hierzu wurden die Bausteine neu gegliedert und übersichtlicher dargestellt. Für jeden Baustein gibt es verschiedene Anforderungen (Basisanforderungen, Standardanforderungen und Anforderungen bei erhöhtem Schutzbedarf), die die bis dato bekannten Maßnahmen ersetzen. Gleichzeitig ist nun die Bildung sogenannter Grundschutzprofile möglich, die die Bausteine und Anforderungen nach den Anforderungen unterschiedlicher Organisationsformen neu gliedern. Dieses wurde zum Beispiel mit dem Kommunalen Grundschutzprofil[1] umgesetzt. Das reduzierte Anforderungsset des Kommunalen Grundschutzprofils bildet auch die Grundlage für den SiKoSH-Standard. Somit liefert SiKoSH die Grundlagen für einen Einstieg in ein strukturiertes ISMS.

1.4 Neuerungen des IT-Grundschutzkompendiums werden sukzessive in SiKoSH, soweit relevant, übernommen. Allgemeines

Die unter http://www.sikosh.de bereitgestellten Hilfsmittel sind als Vorlagen und Muster zu verstehen. Eine unveränderte Übernahme ist daher nur in Ausnahmefällen möglich. Die Regelungsmuster enthalten überwiegend Beispielregelungen (Beispieltexte). Die fachspezifischen Konzeptvorlagen stellen überwiegend Strukturvorlagen da. Beide Hilfsmitteltypen bedürfen der Anpassung an die jeweiligen Prozesse bzw. das jeweilige Fachverfahren.

Die Bearbeitung und Anpassung wird durch Umsetzungsvorschläge oder Hinweise zur Bearbeitung ergänzt. Diese finden sich typischerweise in der jeweiligen Mustervorlage wieder, damit eine unmittelbare Beachtung sichergestellt ist. In seltenen Fällen (wie beispielsweise der Informationssicherheitsleitlinie) sind Bearbeitungshinweise im Anhang an das Dokument zu finden.

Begleitend zum Projekt wird im unter http://www.sikosh.de ein Glossar aufgebaut, indem einheitliche Begriffe definiert werden.

Informationsquellen:

- www.sikosh.de
- www.isis12.de
- www.vds.de
- www.bsi.de

1.4.1 Bearbeitungshinweise

[1] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Hilfsmittel/Profile/Basis_Absicherung_Kommunalverwaltung.html

🕮 **[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.

1.5 Voraussetzungen

Für das Verständnis und die Nachvollziehbarkeit der Inhalte insbesondere der referenzierten Hilfsmittel wird vom Leser mindestens ein Grundverständnis im Bereich Informationssicherheitsmanagement (ISM) vorausgesetzt. Idealerweise wird dieses Wissen durch Kenntnisse im Bereich Schleswig-holsteinischen Datenschutzrechts (LDSG SH, DSDVO), Überblickswissen im Bereich IT-Grundschutzvorgehensweise (100-1; 200-1) sowie einem grundsätzlichen Verständnis der Informationstechnik ("technisches Verständnis") ergänzt.

1.6 Urheberschaft und Lizenzen

Die überwiegende Anzahl der SiKoSH-Dokumente sind unter den Regelungen der Creative Commons für eine kostenfreie Nutzung (CC BY-NC-SA) freigegeben und unter www.sikosh.de abrufbar. Diese Lizenz erlaubt es anderen, die SiKoSH-Materialien zu verbreiten, zu remixen, zu verbessern und darauf

aufzubauen, allerdings **nur nicht-kommerziell und solange das Projekt SiKoSH als Urheber des Originals genannt wird und die auf den SiKoSH-Ergebnissen basierenden Werke unter denselben Bedingungen veröffentlicht werden**.

Die genauen Vorgaben für eine weitere Verwendung finden sich unter http://creativecommons.org/licenses/.

Die vom Projekt ISK.RLP bereitgestellten Dokumente können gemäß Kooperationsvereinbarung durch die Mitgliedskörperschaften der Kommunalen Landesverbände Schleswig-Holstein genutzt werden. Hierfür ist eine gesonderte Zugriffsberechtigung erforderlich, die per E-Mail an info@sikosh.de beantragt werden kann. Der Aufruf der Dokumente erfolgt unter www.sikosh.de.

2 Vorgehensweise zur Einführung und Implementierung von SiKoSH

2.1 Generelle Einführung eines Informationssicherheitsmanagementsystem (ISMS) nach SiKoSH

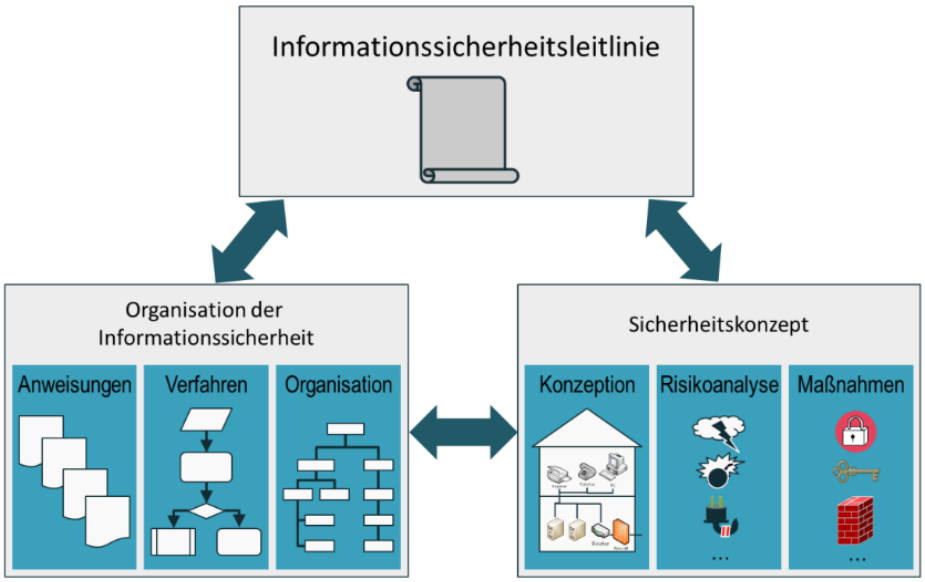
SiKoSH empfiehlt grundsätzlich einen nachhaltigen Aufbau und die Umsetzung eines ISMS entsprechend der Vorgehensweise bereits etablierter Informationssicherheitsframeworks, wie beispielsweise nach IT-Grundschutz 100-2 / 200-2 und den 12 Schritten des ISIS12 Vorgehensmodells.

SiKoSH bietet gegenüber den bereits etablierten Standards den Vorteil, dass es

- dediziert mit Blick auf kommunale Anforderungen und Gegebenheiten entwickelt wurde
- ein Einstiegsframework darstellt, welches zunächst einfach und mit geringem Ressourcenaufwand umsetzbar ist.
- nicht in Konkurrenz zu bereits etablierten ISMS Frameworks wie z.B. ISIS 12 oder IT-Grundschutz darstellt, sondern einen einfachen Einstieg in diese darstellt und später beliebig weiterentwickelt werden kann.
- auf eine „Quick-Win“ Strategie ausgerichtet ist. Mit Hilfe sogenannter Quickchecks, können die wichtigsten Informationssicherheitsmaßnahmen einfach und effizient überprüft und falls nötig, implementiert werden.

Ein ISMS besteht grundsätzlich aus einer Aufbauorganisation (Rollenträger), einer Ablauforganisation (Prozesse/Verfahren) sowie Regelwerk. Fehlt eine der 3 Säulen, ist ein dauerhafter Betrieb eines Managementsystems nicht möglich.

Tipp	Das klingt teilweise komplizierter als es ist. In den folgenden Kapiteln sind Erläuterungen und Hilfsmittel, wie effektiv eine Aufbauorganisation erstellt werden kann, zu finden. Auch werden Checklisten und Hilfsmittel genereller und verfahrensbezogener Art, bereitgestellt und erklärt.



Quelle: Handreichung zur Ausgestaltung der Informationssicherheitsleitlinie in Kommunalverwaltungen[2]

Der BSI-Ansatz ist ausführlich im aktualisierten BSI-Standard 200-1 beschrieben[3].

2.2 SiKoSH Inhalte

Die eigentliche Vorgehensweise zur Einführung von SiKoSH ist in folgenden Dokumententypen unterteilt, dabei sind die Dokumenttypen hierarchisch gegliedert.

2.2.1 Standard (S)

Innerhalb des Standards (vorliegendes Dokument) wird die allgemeine Vorgehensweise zur Einführung von SiKoSH innerhalb einer Organisation beschrieben.

2.2.2 Leitfaden (LF)

Ein Leitfaden konkretisiert und vertieft einzelne Themenfelder. Diese können zwar teilweise im Standard erläutert werden, die konkrete und detaillierte Darstellung würde aber im Standard zu einer gewissen Unübersichtlichkeit führen.

2.2.3 Handreichung (HR)

Eine Handreichung dient dem schnellen Einstieg in ein spezifisches Themenfeld. In ihr werden kurz knapp wesentliche Inhalte vermittelt um mit der Bearbeitung eines einzelnen Aspekts bei der Einführung von SiKoSH schnell und effizient beginnen zu können, bzw. Verständnis dafür zu gewinnen.

[2] http://www.staedtetag.de/fachinformationen/recht/081286/index.html
[3] S. www.bsi.de

2.2.4 QC = Quickcheck (QC)

Ein SiKoSH Quickcheck auf Excel Basis, stellt eine stark vereinfachte Form eines Basis-Sicherheitschecks (ohne vorherige Strukturanalyse bzw. Modellierungsphase) gemäß der IT-Grundschutzvorgehensweise des BSI dar. Damit sind diese zwar einfacher anwendbar, bieten aber andererseits nicht den Umfang und Detailierungsgrad eines Basissicherheitschecks nach der IT-Grundschutzvorgehensweise. Der Umgang mit Quickchecks wird im weiteren Verlauf des Standards und in einer dazugehörigen Handreichung beschrieben.

2.3 SiKoSH Hilfsmittel

SiKoSH stellt dem Anwender weitere Hilfsmittel in der Form von ebenfalls hierarchisch gegliederten Vorlagen zur Anpassung an die Gegebenheiten der eigenen Institution bereit.

Warnung	Alle Hilfsmittel sind lediglich Vorlagen zur individuellen Anpassung an die anwendende Institution. Der SiKoSH Anwender sollte alle Inhalte an die tatsächlichen Gegebenheiten anpassen.

2.3.1 Leitlinie (LL)

Eine Leitlinie stellt das führende Dokument in der Hierarchie der Sicherheitsdokumente in einer Institution dar.

2.3.2 Richtlinie (RL)

Richtlinien stellen Anforderungen an spezielle Themengebiete aus Informationssicherheitssicht auf.

2.3.3 Konzept (K)

Ein Konzept ist eher technischer Art und beschreibt oftmals wie Anforderungen einer Richtlinie konkret umgesetzt werden.

2.3.4 Empfehlungen (E)

Empfehlungen können sich an einzelne Rollen oder Benutzer einer Institution wenden.

2.3.5 Beispiele (B)

Beispiele sind Dokumente anderer Institutionen welche ohne weitere erläuternde Hinweise zur vollständigen eigenen Anpassung bereitgestellt werden.

3 Die SiKoSH-Vorgehensweise

3.1 Zielsetzung

SiKoSH soll die Einführung eines kommunalen ISMS erleichtern. Zur Reduzierung der Komplexität werden verschiedene wichtige Aspekte im Kontext Informationssicherheit zu unterschiedlichen Phasen zusammengelegt.

Jede Phase wird mit einem Quickcheck eingeleitet.

Innerhalb der Phasen stellt SiKoSH mit seinen Hilfsmitteln Orientierungspunkte bereit, welche auch Nicht-Spezialisten in die Lage versetzen, wichtige Maßnahmen zur Etablierung eines ständigen Verbesserungsprozesses der Informationssicherheit zu implementieren.

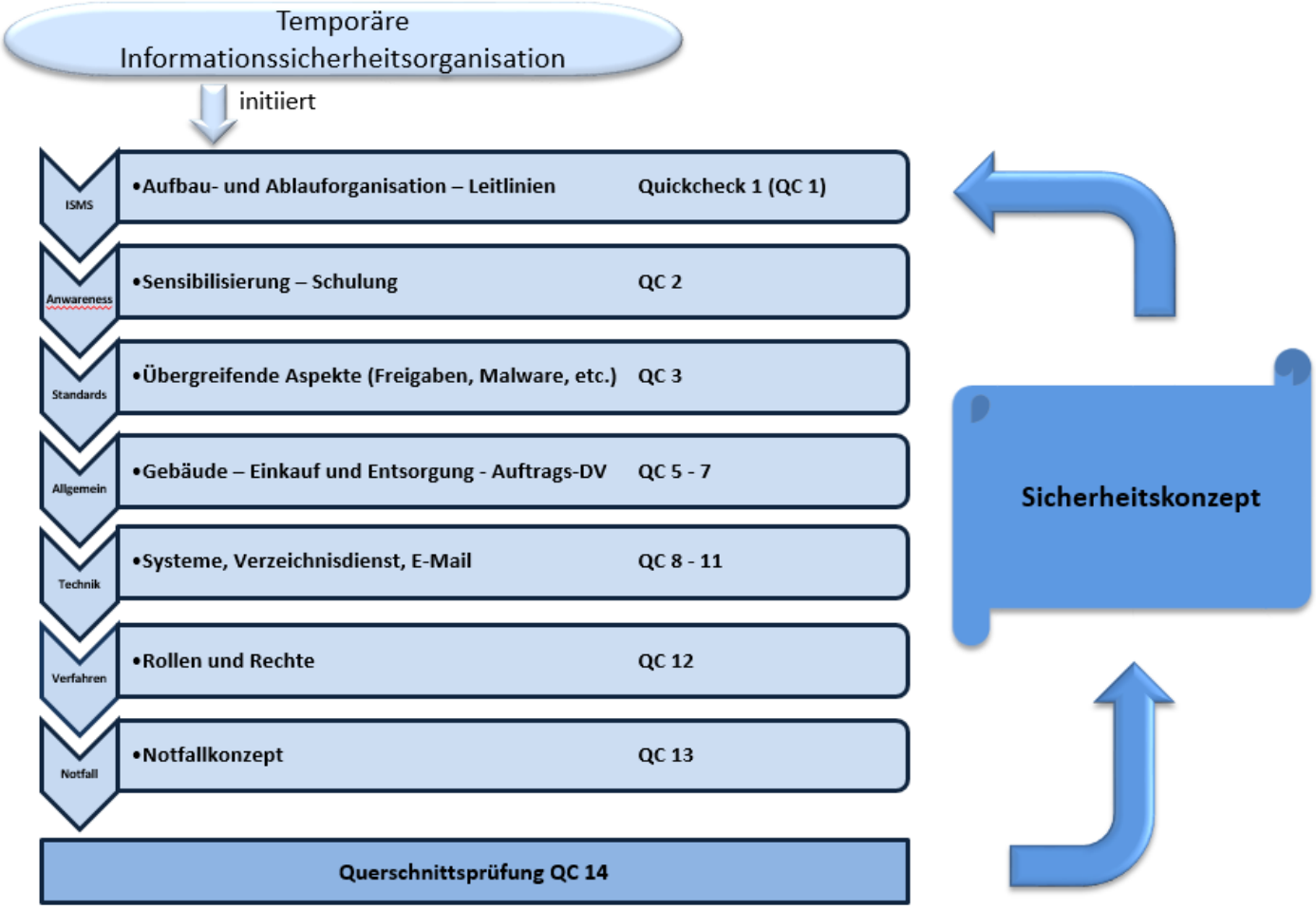
Zur Abarbeitung der Phasen ist es zwingend, mit der Phase 1 (Grundlagen ISMS) zu beginnen. SiKoSH empfiehlt, mit der Phase 2 (Mitarbeitersensibilisierung) fortzufahren. Die Priorisierung der weiteren Phasen sollte sich an den Ergebnissen der Quickchecks orientieren. Den Abschluss bilden dann die Querschnittsfragen als letzte Phase.

Nach der Bearbeitung aller SiKoSH Quickchecks, der Umsetzung noch nicht implementierter Prüfpunkte und der Anpassung und Verabschiedung fehlender Hilfsmittel in einer Institution, sowie der Dokumentation eines Sicherheitskonzepts wurde eine solide Grundlage für den weiteren Ausbau eines ISMS in einer Kommune etabliert.

Warnung	Die Umsetzung von SiKoSH entbindet die Leitung der Institution nicht davon, ggf. weitere Anforderungen z.B. des IT-Grundschutzes, von Rechnungshöfen, datenschutzrechtlichen Aufsichtsbehörden oder anderen Prüforganisationen zu berücksichtigen. Sie stellt, wie oben erläutert, lediglich die Basis für den weiteren Ausbau dar und ist entsprechend zu ergänzen und fortlaufend zu verbessern.

Hinweis	SiKoSH lebt vom Mitmachen! Wünsche, Anregungen, Hinweise und insbesondere Muster für ergänzende Hilfsmittel sind herzlich willkommen (bitte senden an sikosh@komfit.de).

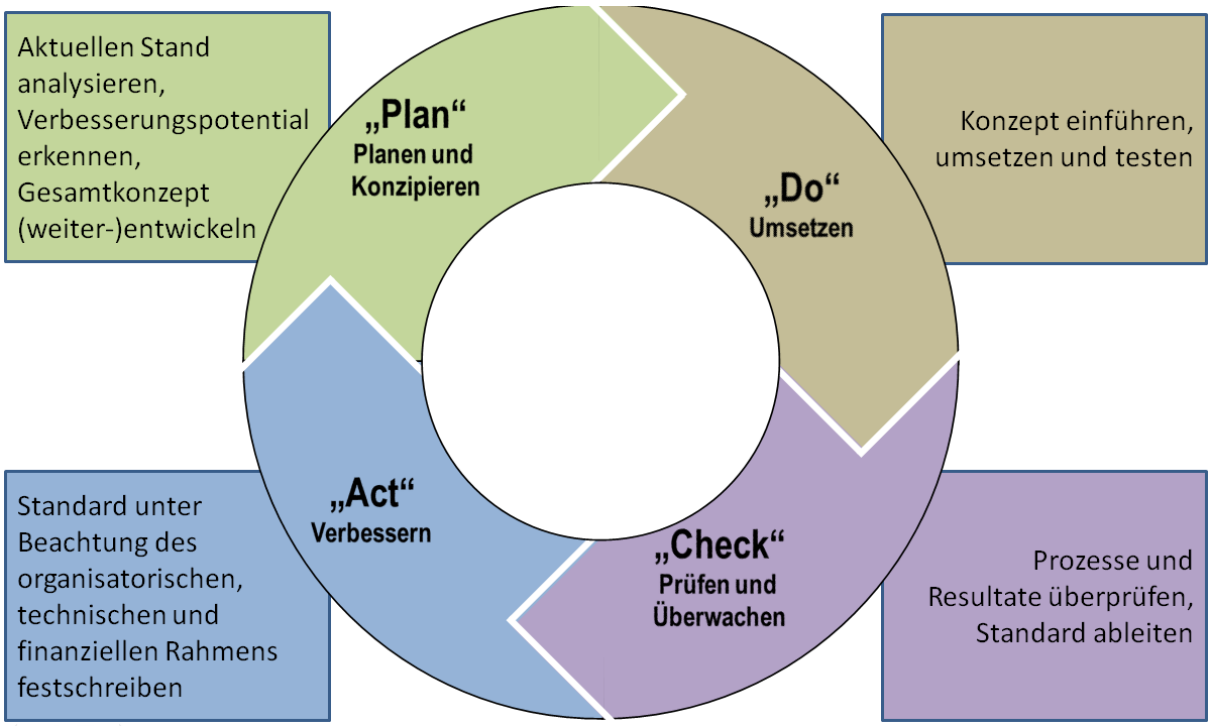
3.2 Prozessmodell



3.3 Regelmäßige Aufgaben

Die Planung, Umsetzung, Überprüfung und Verbesserung der Informationssicherheit ist ein regelmäßiger Prozess mit dem Ziel Risiken und Gefährdungen auf ein akzeptables Maß zu minimieren. Dieses setzt voraus, dass betroffene Einzelprozesse immer wieder an das aktuelle Sicherheitslagebild angepasst und verbessert werden.

Für diesen kontinuierlichen Verbesserungsprozess hat sich das PDCA-Modell bewährt.



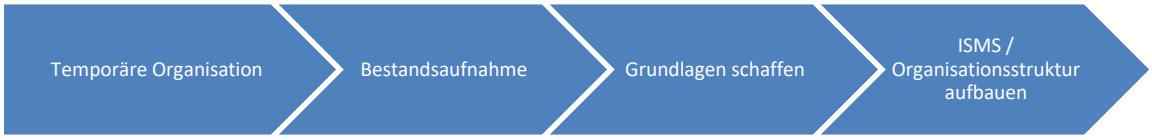
Quelle: Handreichung zur Ausgestaltung der Informationssicherheitsleitlinie in Kommunalverwaltungen

3.4 Referenzieren von Regelungen in der Praxis

Die jeweils relevanten Regelungen sind in den in Sicherheitskonzepten zu benennen (siehe Punkt 12). Daher empfiehlt es sich, Regelungen unabhängig von Erstellungsdatum oder Versionsstand zu benennen[4]. Dies reduziert den Pflegeaufwand von Sicherheitskonzepten erheblich.

[4] Nicht „Freigaberichtlinie V1.2.doc“ oder „2017-01-03 Freigaberichtlinie.docx“ sondern "Freigaberichtlinie"

4 Der SiKoSH-Einstieg in ein effektives ISMS



4.1 Temporäre Organisation schaffen

Da es beim Einstieg noch keine ISMS- Aufbau- und Ablauforganisation gibt, sollte eine Informationssicherheitsarbeitsgruppe eingerichtet werden mit folgender Besetzung Behördenleiter, IT-Leiter, sofern vorhanden der Datenschutzbeauftragte (bDSB) und ggf. weitere Rollenträger (Personalrat, Leiter Gebäudemanagement etc.). Die Aufgaben der temporären Organisation bestehen in der Schaffung organisatorischer Grundlagen und in einer ersten Bestandsaufnahme.

4.1.1 Einsatz der Quickchecks zur Bestandsaufnahme

Im Rahmen des Projektes wurden Fragebögen entwickelt, die bei der Erstaufnahme des Sachstandes der Informationssicherheit unterstützen sollen. Diese sogenannten Quickchecks umfassen Schwerpunktfragen aus spezifischen organisatorischen oder technischen Themengebieten, mit denen eine Sachstandserhebung auf Grundlage typischer Kern-Sicherheitsanforderungen durchgeführt werden kann.

Diese initiale Bestandsaufnahme dient insbesondere der Darstellung der aktuellen Sicherheitslage (technisch, organisatorisch und hinsichtlich der Dokumentation) und der besonders schützenswerten Objekte (z. B. der Personenstandsdaten). Diese grundlegenden Informationen unterstützen hinsichtlich der Argumentation der Notwendigkeit weitergehender Maßnahmen zur Erhöhung der Informationssicherheit und legen einen groben strategischen Rahmen hierfür fest. **Alle Quickchecks sind unter www.sikosh.de** frei zugänglich.

Innerhalb einer kurzen Anleitung, werden die wichtigsten Kenntnisse zur Bearbeitung der Quickchecks zusammengefasst.

- 🕮 Hilfsmittel: SiKoSH-Handreichung Anleitung zum Bearbeiten der Quickhecks

Hinweis	Die Bearbeitung der Quickchecks zieht sich wie ein roter Faden durch alle Phasen der SiKoSH Umsetzung und korrespondiert mit den jeweils zur Verfügung gestellten Hilfsmitteln. Dabei wurde bei der hier empfohlenen Reihenfolge einerseits darauf geachtet, dass diese zunächst mit möglichst geringem Aufwand einen spürbaren Mehrwert für das Sicherheitsniveau der anwendenden Institution bietet. Andererseits wurde versucht zunächst Abhängigkeiten von bestimmten Grundvoraussetzungen zu vermeiden, um eine reibungslose Initiierung notwendiger Maßnahmen zu ermöglichen. Dennoch kann jederzeit die hier vorgeschlagene Reihenfolge der Umsetzung variiert werden, wenn es für die Implementierung des ISMS zielführend ist. Weiterhin ist die vorgegebene Priorisierung lediglich ein Vorschlag – die anwendende Institution kann die Priorisierung der Prüfpunkte jederzeit auf Ihre individuellen Gegebenheiten anpassen bzw. variieren. **Innerhalb des Prozessschrittes ‚Temporäre Organisation schaffen' und bis zum Abschluss des Schrittes ‚Grundlagen und Voraussetzungen schaffen' sollte zunächst der Quickcheck Sachstandsaufnahme Informationssicherheit / ISMS, bearbeitet werden. Dieser schafft die notwendigen Grundlagen für die Einführung des ISMS innerhalb der anwendenden Institution.**

- 🕮 Quickcheck Sachstandsaufnahme Informationssicherheit / ISMS
- 🕮 Quickcheck Mitarbeitersensibilisierung
- 🕮 Quickcheck Standardregelungen
- 🕮 Quickcheck Internetzugang/Nutzung
- 🕮 Quickcheck Gebäudesicherheit
- 🕮 Quickcheck Beschaffung / Entsorgung
- 🕮 Quickcheck Outsourcing
- 🕮 Quickcheck Clientsicherheit
- 🕮 Quickcheck Serverbetrieb / Zentrale Systeme
- 🕮 Quickcheck Active Directory
- 🕮 Quickcheck Mail
- 🕮 Quickcheck Anwendungssicherheit
- 🕮 Quickcheck Notfallvorsorgemanagement / Notfallmanagement
- 🕮 Quickcheck Querschnittsfragen

Die Quickchecks werden als separate Tabellen bereitgestellt. Die einzelnen Fragen zum Umsetzungsstand können über entsprechende Auswählmenüs innerhalb der Tabelle beantwortet werden. Ferner beinhalten die Checks eine einfache grafische Auswertung.

Tipp	Nachdem der aktuelle Umsetzungsstand des jeweiligen Quickchecks erfasst ist, d. h. zunächst der Umsetzungstand des Quickcheck Sachstandsaufnahme Informationssicherheit / ISMS, sollten die nicht positiv beantworteten Prüfpunkte bearbeitet werden. Die Prüfpunkte sind innerhalb der Quickchecks priorisiert (optional, niedrig, mittel hoch). Offene Prüfpunkte sollten, frei nach dem Pareto-Prinzip, in etwa zu 80% geschlossen bzw. Maßnahmen zur Umsetzung initiiert werden. Dabei sind die in den jeweiligen Kapiteln aufgeführten Hilfsmittel nützlich. Erst dann sollte die Umsetzung der nächsten SiKoSH-Phase begonnen werden.

4.2 Grundlagen und Voraussetzungen schaffen

4.2.1 Unterstützung der Leitungsebene sichern

Im Rahmen ihrer Organisationsverantwortung trägt die Behördenleitung neben der Verantwortung zur Umsetzung bestehender Gesetze (wie z. B. die Datenschutzgesetze) auch die Verantwortung zur Gewährleistung der Informationssicherheit. Insofern kann die Initiierung behördeninterner Informationssicherheitsprozesse auch nur durch die Behördenleitung erfolgen.

🕮 **SiKoSH-Handreichung Informationssicherheit für Behördenleiter**

4.2.2 Sicherheitsleitlinie erstellen, in Kraft setzen lassen

Die Informationssicherheitsleitlinie (ISLL) schafft die Grundlage für den Aufbau eines ISMS, das die Herstellung und den Erhalt des erforderlichen Sicherheitsniveaus aller Daten im Verantwortungsbereich der Behörde sicherstellt. Das ISMS beinhaltet Aufbauorganisation, Ablauforganisation (Prozesse) und Regelwerk, die geeignet sind, Planung, Umsetzung und Überprüfung von Sicherheitsmaßnahmen im Geltungsbereich zu gewährleisten. Das ISMS unterstützt die Behördenleitung dabei, ihrer gesetzlichen Verantwortung für die Informationssicherheit gerecht zu werden.

🕮 **SiKoSH-Leitlinie Informationssicherheitsleitlinie**
Grundsätzlich ist die Musterleitlinie allgemein gültig unabhängig von der Größenklasse. Wo textuelle Anpassungen erforderlich sind, gibt es einen entsprechenden Hinweis. Die Leitlinie ist auch von Verwaltungseinrichtungen, die nach dem IT-Sicherheitsgesetz als KRITIS einzustufen sind, anwendbar (z.B. kommunale Ver- oder Entsorger). Nötige (Mindest-) Anpassungen sind im Text vermerkt. Im Anhang des Regelungsmusters befinden sich zahlreiche Bearbeitungshinweise.

🕮

Warnung	**G**rößere Abweichungen und Änderungen der Musterleitlinie sind akzeptabel, ja sogar erwünscht! Eine Informationssicherheitsleitlinie sollte immer individuell für die anwendende Institution stehen. Die Informationssicherheitsleitlinie ist das „Herzstück“ aller Regelwerke, dementsprechend intensiv gilt es sich mit ihr zu beschäftigen.

4.3 ISMS / Organisationsstruktur aufbauen

4.3.1 Informationssicherheitsbeauftragten benennen und qualifizieren

Die Bestellung eines Informationssicherheitsbeauftragten (ISB) ist eine unverzichtbare Basismaßnahme bei der Etablierung eines ISMS. Der ISB ist der zentrale Ansprechpartner für alle Fragen rund um die behördliche Informationssicherheit, er ist für den weiteren Aufbau und die Aufrechterhaltung des ISMS und für die Pflege des Sicherheitskonzeptes und ggf. auch für die Notfalldokumentation verantwortlich (Details s. Richtlinie Datenschutz- und Informationssicherheitsmanagement).

- 🕮 **SiKoSH-Beispiel Bestellung eines ISB**
  Dieses Beispiel kann nach entsprechender Anpassung verwendet werden, um einen ISB zu bestellen. Des Weiteren werden die Rechte und Pflichten eines ISB dargestellt.
- 🕮 SiKoSH Konzept Schulung Rollenträger im Informationssicherheitsmanagement

4.3.2 Leitlinie Datenschutz- und Informationssicherheitsmanagement beschreiben

In der Leitlinie Informationssicherheits- und Datenschutzmanagement werden die Organisationstruktur, die Rollenträger und die Kernprozesse im Informationssicherheitsmanagement (ISM) und deren Zusammenwirken mit anderen Prozessen der Verwaltung beschrieben. Die Leitlinie ist die zentrale Regelung für das Sicherheitsmanagement selbst, da sie die formalen Grundlagen für Auf- und Ausbau und die Verankerung von Informationssicherheit festlegt.

Ferner legt sie Rahmenbedingungen und Schnittstellen zu anderen Prozessen fest. Sie konkretisiert somit die Informationssicherheitsleitlinie und ist zusammen mit dieser das zentrale Regelungsdokument des Informationssicherheitsmanagements.

Die Richtlinie definiert zudem grundlegende Anforderungen, die häufig in nachgelagerten Regelungen konkretisiert werden können oder konkretisiert werden müssen.

- 🕮 **SiKoSH-Leitlinie Datenschutz- und Informationssicherheitsmanagement**

4.4 Hinweise zur Rollenbesetzung

Für die Zuweisung klarer Verantwortlichkeiten innerhalb eines ISMS sind einige zwingende Rollen erforderlich.

4.4.1 Standardrollen im Kontext Informationssicherheit

Rolle im Sicherheitsmanagement	Kurzbeschreibung
Informationssicherheitsbeauftragter (ISB)	verantwortlich für die Etablierung und Aufrechterhaltung der Informationssicherheit
Behördlicher Datenschutzbeauftragter (bDSB)	wirkt auf die Einhaltung datenschutzrechtlicher Vorgaben hin[5] Achtung Änderung durch EU DSGVO, dann Überwachung der Einhaltung des Datenschutzes
Sicherheitskoordinator (Fachverfahren)	fachverfahrensbezogene Ansprechpartner für sicherheitsbezogene Fragen und die Erstellung/Fortschreibung eines verfahrensbezogenen Sicherheitskonzeptes Bei kleinen Verwaltungen kann diese Aufgabe ggf. auch vom ISB wahrgenommen werden.

4.4.2 Weitere wichtige Rollen im Kontext Informationssicherheit

Allgemeine Rolle	Kurzbeschreibung
Behördenleitung	Gesamtverantwortung (einschl. Datenschutz und Informationssicherheit)
IT-Leiter (IT-Verantwortlicher)	Verantwortlich für die Organisation der IT und deren IT-Betrieb[6]
Fachverfahrensverantwortliche	Verantwortlich für ein oder mehrere Fachverfahren (z.B. Fachbereichsleitung, Referatsleiter)
Mitarbeiterinnen und Mitarbeiter (allgemein)	Verantwortlich für die Einhaltung einschlägiger Dienstanweisungen zur Erhöhung von Informationssicherheit und Datenschutz

📖 **SiKoSH-Empfehlung Rollenbesetzung im Informationssicherheitsmanagement**

4.4.3 Erste Umsetzungsschritte

Aus dem Portfolio zahlreicher unterschiedlicher Aufgaben im Informationssicherheitsmanagement empfiehlt es sich zunächst Maßnahmen zur Mitarbeitersensibilisierung umzusetzen. Diese sind in der Regel unabhängig von institutionsspezifischen Besonderheiten und bieten einen großen Mehrwert für das Sicherheitsniveau der Institution (Quick Wins).

[5] Mit Wirksamwerden der EU-DSGVO ändert sich die gesetzlich vorgeschriebene Aufgabe in ‚Überwachung des Datenschutzes'

[6] Das schließt auch IT-bezogene Leistungen ein, die im Rahmen eines Outsourcings von Dritten erbracht werden

5 Mitarbeitersensibilisierung

5.1 Bestandsaufnahme

- 🕮 Quickcheck Sachstandsaufnahme Informationssicherheit / ISMS
- 🕮 Quickcheck Mitarbeitersensibilisierung
- 🕮 Quickcheck Standardregelungen
- 🕮 Quickcheck Internetzugang/Nutzung
- 🕮 Quickcheck Gebäudesicherheit
- 🕮 Quickcheck Beschaffung / Entsorgung
- 🕮 Quickcheck Outsourcing
- 🕮 Quickcheck Clientsicherheit
- 🕮 Quickcheck Serverbetrieb / Zentrale Systeme
- 🕮 Quickcheck Active Directory
- 🕮 Quickcheck Mail
- 🕮 Quickcheck Anwendungssicherheit
- 🕮 Quickcheck Notfallvorsorgemanagement / Notfallmanagement
- 🕮 Quickcheck Querschnittsfragen

5.2 Sensibilisierung planen und starten

Internationale Erfahrungen mit Sensibilisierung, Schulung und Training von Organisationen und individuellen Benutzern zeigen, dass Informationssicherheit ein abstraktes Konzept ist, das nur schwer gelernt werden kann. Andererseits zeigt die tägliche Praxis, dass Sicherheitsbedrohungen nicht ausschließlich technisch abgefedert werden können (bestes Beispiel sind Verschlüsselungstrojaner wie z. B. Locky oder WannaCry).

Es genügt in der Regel nicht, die Kenntnisse im Bereich Schadensmöglichkeiten, Schadvektoren und Verhalten zu erweitern. Der Mitarbeiter – und Benutzer ganz allgemein – muss sein persönliches Verhalten anpassen wollen, die entsprechenden Fähigkeiten und Fertigkeiten haben, sein persönliches Verhalten anpassen zu können und im speziellen Kontext die Fähigkeiten und Fertigkeiten auch aktivieren.

Im Rahmen durchzuführender Sensibilisierungskampagnen sollten insbesondere nachfolgende Ratschläge beachtet werden:

- ✓ Mitarbeiter ermutigen, Verdächtiges zu melden, ohne Angst vor Repressalien zu haben. Dies muss von den Vorgesetzten unterstützt und vorgelebt werden.

- ✓ Berücksichtigen, dass Mitarbeiter unter erhöhtem Arbeitsdruck schnell in alte Verhaltensmuster verfallen und dann eine erhöhte Risikobereitschaft aufweisen, um Dinge vom Tisch zu bekommen. Wo immer möglich, bereits in der Aufgabenstellung deutlich machen, dass die Sicherheitsthemen zur Aufgabenerledigung dazugehören.

- ✓ Sensibilisierung ist ein Prozess, der immer wieder aufgefrischt werden muss. Mit Schulungen alleine ist es nicht getan, es muss eine Veränderung des Verhaltens der Mitarbeiter erreicht werden. Dies ist leichter, wenn das Thema Informationssicherheit in Anweisungen, Prozessen und Vorgehensweisen sowie bei den Arbeitsaufträgen stetig eingebunden ist. Im folgendem werden weitere Hilfsmittel aufgeführt, welche die Umsetzung von Maßnahmen zur positiven Beantwortung der im Quickcheck Sensibilisierung definierten Prüfpunkte erleichtern.

📖 **SiKoSH-Beispiel Sensibilisierung**
In diesem Dokument werden die Grundlagen für eine erfolgreiche Sensibilisierungskampagne erwähnt.

5.3 Schulung

5.3.1 Training

Trainingsmaßnahmen dienen dazu richtiges Verhalten zu stärken und falsche Verhaltensweisen zu löschen; z. B. Erkennen von bösartigen Mails bzw. Webseiten.

5.3.2 Bildung

Bildung dient dazu den Rollenträgern im Schulungsumfeld die Fertigkeiten zu vermitteln, die für effektive Trainingsmaßnahmen erforderlich sind.

📖 SiKoSH-Konzept Schulung der Mitarbeiterinnen und Mitarbeiter
Dieses Schulungskonzept regelt die Planung, Vorbereitung, Teilnahmeverpflichtungen und Durchführung von Schulungsveranstaltungen zur Informationssicherheit.

5.4 Organisatorische Regelungen

📖 SiKoSH-Beispiel Verhalten bei Sicherheitsvorfällen
Das Merkblatt erläutert, was ein Sicherheitsvorfall ist und wer bei der Feststellung oder dem Verdacht zu informieren ist.

Die Stadt Oldenburg i. O. hat 2014 zusammen mit dem Maskottchen WOLFI eine erfolgreiche Mitarbeitersensibilisierungskampagne durchgeführt. Ein Jahr lang wurde jeden Monat ein Flyer mit einem bestimmten Sensibilisierungsthema veröffentlicht. Die Flyer können auf der Webseite heruntergeladen und unter Beachtung der einschlägigen Lizenzbestimmungen für die eigene Verwaltung adaptiert werden.

6 Standardregelungen

6.1 Überblick

An dieser Stelle werden zahlreiche Musterregelungen bereitgestellt, die wesentliche Aspekte des Sicherheitsmanagements aufgreifen. Die Verantwortung für diese Regelungen liegt typischerweise nicht beim Informationssicherheitsbeauftragten (ISB), sondern in den jeweiligen Fach- oder Querschnittsabteilungen. Die Musterregelungen sollen dabei helfen, typische sicherheitsbezogene Regelungsbedarfe in der Verwaltung zu verankern oder bereits vorhandene Regelungen auf Lücken zu prüfen und zu ergänzen.

6.2 Verankerung in der Organisation

Die Verankerung von Informationssicherheit im allen Bereichen des Verwaltungsbetriebes bedarf einiger Rahmenbedingungen. Diese werden typischerweise mit entsprechenden Regelungen in der Organisation unter Einbeziehung der betroffenen Bereiche und weiterer zu beteiligender Mitbestimmungsgremien abgestimmt und in Kraft gesetzt. Grundlagen für die Verankerung sind in der Richtlinie Informationssicherheits- und Datenschutzmanagement (s. o.) festzulegen.

Durch die Einbettung der Informationssicherheit in die Verwaltungsprozesse (Umsetzung und Beachtung von Sicherheitsmaßnahmen in bestehende betriebliche Prozesse und Arbeitsabläufe) soll erreicht werden, dass die Umsetzung von technischen und organisatorischen Sicherheitsmaßnahmen von den Mitarbeiterinnen und Mitarbeitern akzeptiert wird und verlässlich erfolgt (Effektivität des ISMS). Dies erfolgt insbesondere durch die in der Richtlinie Informationssicherheits- und Datenschutzmanagement beschriebenen Prozesse aber auch weiterer flankierender Maßnahmen in ergänzenden Regelungen und Konzepten (Mitarbeitersensibilisierung, Schulung etc.).

Ferner soll erreicht werden, dass Sicherheitsmaßnahmen weitestgehend wirtschaftlich umgesetzt werden können. Die Prozesse stellen daher standardisierte Abläufe (z.B. für Anforderungsmanagement, Test und Freigabe) bereit, die für spezifische Aufgaben des Sicherheits- und teilweise auch Datenschutzmanagements genutzt werden können (Wirtschaftlichkeit des ISMS).

Die Integration von sicherheitsbezogenen Vorgaben und Prozessschritten kann grundsätzlich in zwei verschiedene Varianten erfolgen:

Variante 1:

Es werden immer einzelne, für einen spezifischen Aspekt relevante Regelungen in der Organisation verankert (z.B. Regelungen für den Einkauf, Regelungen für Entsorgung). Dies kann beispielsweise auf Grundlage der bereitgestellten Regelungsmuster erfolgen. Dies ermöglicht es, für konkrete Prozesse und Vorgänge dedizierte Sicherheitsanforderungen in fachbezogenen Regelungen zu verankern. Empfehlenswert ist dieses Vorgehen insbesondere für größere Verwaltungen, die typischerweise eine ausgeprägte Verwaltungsstruktur aufweisen (z.B. dedizierte Beschaffungsabteilung, etc.).

Variante 2:

Erforderliche sicherheitsrelevante Regelungen werden (ausschließlich oder überwiegend) in der Richtlinie Informationssicherheits- und Datenschutzmanagement geregelt. Die vom Standard bereitgestellten Regelwerksmuster haben hier überwiegend einen Checklistencharakter („Habe ich an Punkt XY gedacht“).

Diese Variante bietet insbesondere für (kleinere) Verwaltungen mit wenig fachbereichsbezogenen Strukturen an, bei denen es keine Spezialregelung gibt oder die Umsetzung nicht empfehlenswert ist.[7]

- 🕮 Quickcheck Sachstandsaufnahme Informationssicherheit / ISMS
- 🕮 Quickcheck Mitarbeitersensibilisierung
- 🕮 Quickcheck Standardregelungen
- 🕮 Quickcheck Internetzugang/Nutzung
- 🕮 Quickcheck Gebäudesicherheit
- 🕮 Quickcheck Beschaffung / Entsorgung
- 🕮 Quickcheck Outsourcing
- 🕮 Quickcheck Clientsicherheit
- 🕮 Quickcheck Serverbetrieb / Zentrale Systeme
- 🕮 Quickcheck Active Directory
- 🕮 Quickcheck Mail
- 🕮 Quickcheck Anwendungssicherheit
- 🕮 Quickcheck Notfallvorsorgemanagement / Notfallmanagement
- 🕮 Quickcheck Querschnittsfragen

6.3 Internes Kontrollsystem / Nachhaltigkeit

Um ein dauerhaft geltendes und aktuelles Regelwerk sowie einen durchgängigen Bekanntheitsgrad zu etablieren, ist sicherzustellen, dass betroffene Mitarbeiter von den Regelungen Kenntnis haben und diese Regelungen auch jederzeit verfügbar sind (Publikation im Intranet, Laufwerke, Dokumentenmanagementsystem etc.).

Die Aktualität des Regelwerkes ist ferner durch regelmäßige Reviews, aber auch interne Kontrollen (z.B. im Rahmen von Stichprobenprüfungen) sicherzustellen. Es wird empfohlen, den regelmäßigen Review des Regelwerkes unter Nennung des Prüfers, des Prüfdatums und des Prüfungsergebnisses zu dokumentieren.

6.4 Regelungen

- 🕮 **SiKoSH-Richtlinie Freigabe**
- 🕮 **SiKoSH-Richtlinie Freigabe – Anlagen 1-5 Freigabevermerke**

[7] Dies kann beispielsweise auch der Fall sein, wenn es für spezifische Fragegestellungen keinen zentralen Ansprechpartner und damit Regelungsverantwortlichen gibt.

Die Freigaberichtlinie definiert, unter welchen Rahmenbedingungen (welche Rollen/Personen, Dokumentationsanforderungen, etc.) Verfahren oder Infrastrukturen in der Verwaltung freigeben werden dürfen. Diese Regelung setzt wesentliche Anforderungen aus dem Datenschutz um.

Die Richtlinie stellt ebenfalls ein Muster für verschiedene Freigabevermerke inklusive eines Glossars.

🕮 **SiKoSH-Richtlinie Passwortrichtlinie**

Die Regelung legt grundsätzliche Aspekte beim Einsatz von Passworten fest (Komplexität, Lebensdauer). Sofern nicht in der Bürokommunikationsregelung oder vergleichbaren Regelungen enthalten, sollten auch das Prozedere zum Zurücksetzen von Passworten festgelegt werden.

🕮 SiKoSH-Konzept Kryptokonzept (in Planung)
Das vorliegende Konzept benennt kryptografische Verfahren und Produkte, die für einen Einsatz in der anwendenden Institution freigegeben wurden.

🕮 **SiKoSH-Richtlinie Mobile Endgeräte**

Die Richtlinie ergänzt bzw. konkretisiert die Regelungen einer Bürokommunikationsrichtlinie bzgl. des Einsatzes von mobilen Geräten. Dies umfasst beispielsweise dienstliche Notebooks oder Tabletts als auch - sofern relevant - den Einsatz privater Geräte im Kontext Bring Your Own Device (BYOD).

🕮 SiKoSH-Konzept Datensicherungskonzept (in Planung)

🕮 **SiKoSH-Richtlinie Bürokommunikationssysteme (BKS)**

Die Richtlinie regelt den grundsätzlichen und fachverfahrensunabhängigen Umgang mit Verwaltungs-IT und damit zusammenhängenden Aspekten. Dies reicht von Regelungen zur Telearbeit, Vorgaben zur Mailkommunikation, den Umgang mit mobilen Datenträgern, allgemeine Vorgaben zur Datenablage etc. Diese Regelung stellt eine wesentliche Säule für die Absicherung der Standard-IT-Ausstattung bereit.

🕮 SiKoSH-Richtlinie Antivirenkonzept (in Planung)

🕮 **SiKoSH-Richtlinie Patchmanagement**

Das Richtlinienmuster "Patchmanagement" legt Rahmenbedingungen für das Patchen von Infrastruktur- und Fachanwendungskomponenten sowie den Bezug von sicherheitsrelevanten Meldungen (z.B. über ein CERT) fest. Dies umfasst ferner Verantwortlichkeiten sowie Fristen für das Einspielen von Patches in Abhängigkeit der Kritikalität etwaiger Fehler oder Lücken in der jeweiligen Komponenten. Die Kritikalität wird hier ebenfalls definiert.

🕮 SiKoSH-Richtlinie Nutzung Internet (in Planung)

7 Allgemeine Musterregelungen

7.1 Überblick

Innerhalb der allgemeinen Musterregelungen werden insbesondere die Aspekte physikalische Infrastruktur (Gebäudesicherheit), die Beschaffungs- und Entsorgungsprozesse und ein mögliches Outsourcing betrachtet. Während der Bereich der Gebäudesicherheit aufgrund seiner vielfältigen Schnittstellen zu allen möglichen Sicherheitsaspekten von auf der Hand liegender zentraler Bedeutung ist, sind insbesondere die Entsorgungsaspekte in einem engen Zusammenhang mit Vertraulichkeitsaspekten der verarbeiteten Daten zu sehen.

Da innerhalb moderner IT-gestützter Verwaltungsprozesse ein Outsourcing von IT-Dienstleistungen eher die Regel als die Ausnahme darstellt, sollte ebenfalls sorgfältig geprüft werden, ob der Quickcheck Outsourcing ebenfalls bearbeitet werden sollte.

- 🕮 Quickcheck Sachstandsaufnahme Informationssicherheit / ISMS
- 🕮 Quickcheck Mitarbeitersensibilisierung
- 🕮 Quickcheck Standardregelungen
- 🕮 Quickcheck Internetzugang/Nutzung
- 🕮 Quickcheck Gebäudesicherheit
- 🕮 Quickcheck Beschaffung / Entsorgung
- 🕮 Quickcheck Outsourcing
- 🕮 Quickcheck Clientsicherheit
- 🕮 Quickcheck Serverbetrieb / Zentrale Systeme
- 🕮 Quickcheck Active Directory
- 🕮 Quickcheck Mail
- 🕮 Quickcheck Anwendungssicherheit
- 🕮 Quickcheck Notfallvorsorgemanagement / Notfallmanagement
- 🕮 Quickcheck Querschnittsfragen

7.2 Regelungen

- 🕮 **SiKoSH-Richtlinie Gebäudesicherheit**

  Die Richtlinie legt grundsätzliche Aspekte der Raum- und Gebäudesicherheit (Einsatz von Sicherheitszonen, Einsatz eines Zutrittskontrollsystems, Raumsicherheit etc.) fest.

- 🕮 SiKoSH-Richtlinie Beschaffung (in Planung)

- 🕮 **SiKoSH-Richtlinie Aussonderung schützenswerter Betriebsmittel**

  Diese Richtlinie legt den Umgang mit aussonderungsbedürftiger Hardware fest.

- 🕮 SiKoSH-Richtlinie Auftragsdatenverarbeitung (in Planung)

8 Technische Musterregelungen

8.1 Überblick

Technische Musterregelungen und die dazugehörigen Quickchecks adressieren insbesondere die interne und externe IT und deren Administratoren. Eine klassische Unterteilung in Endgeräte (Clientsicherheit) und Server, sowie Checks und Hilfsmittel für den Betrieb der beiden primären IT-Infrastrukturdienste Active Directory und Mail bilden die Grundlage für einen sicheren Betrieb dieser technischen Aspekte nach SiKoSH:

- 🕮 Quickcheck Sachstandsaufnahme Informationssicherheit / ISMS
- 🕮 Quickcheck Mitarbeitersensibilisierung
- 🕮 Quickcheck Standardregelungen
- 🕮 Quickcheck Internetzugang/Nutzung
- 🕮 Quickcheck Gebäudesicherheit
- 🕮 Quickcheck Beschaffung / Entsorgung
- 🕮 Quickcheck Outsourcing
- 🕮 Quickcheck Clientsicherheit
- 🕮 Quickcheck Serverbetrieb / Zentrale Systeme
- 🕮 Quickcheck Active Directory
- 🕮 Quickcheck Mail
- 🕮 Quickcheck Anwendungssicherheit
- 🕮 Quickcheck Notfallvorsorgemanagement / Notfallmanagement
- 🕮 Quickcheck Querschnittsfragen

8.2 Regelungen

- 🕮 SiKoSH-Konzept Virtualisierung (in Planung)
- 🕮 SiKoSH-Konzept Systemhärtung (in Planung)
- 🕮 **SiKoSH-Richtlinie Fernzugriff und Fernwartung**

  Diese Richtlinie regelt die Voraussetzungen für den Fernzugriff auf alle im eigenen Verantwortungsbereich betriebenen IT-Systeme und Verfahren. Neben dem Eigenbetrieb schließt dies auch Fernzugriffe auf externe (im Auftrag betriebene) Systeme ein.

- 🕮 **SiKoSH-Richtlinie Multifunktionsgeräte**

  Diese Technische Richtlinie regelt die Einsatzrahmenbedingungen für Multifunktionsgeräte (typischerweise Multifunktionsdrucker). Es umfasst Vorgaben zu Aufstellort und Authentisierung (z.B. bei Follow Me Print) sowie der Administration der Geräte.

- 🕮 **SiKoSH- Richtlinie Webserverbetrieb**

Die Richtlinie legt Rahmenbedingungen zum Betrieb von Webservern fest. Dies reicht von der Planung, dem Aufbau bis zu betriebsnahen Aspekten wie der Absicherung der Kommunikation.

📖 SiKoSH-Richtlinie Verzeichnisdienst (in Planung)

9 Verfahrensbezogenes Regelwerk

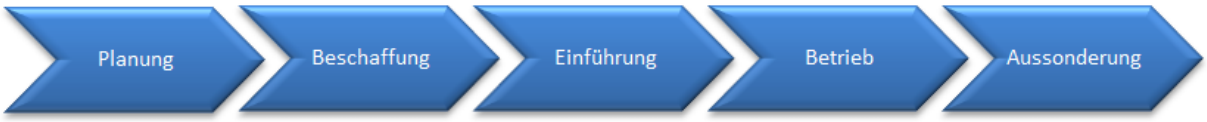
9.1 Überblick

Das Projekt stellt verschiedene verfahrensbezogene Hilfsmittel bereit. Verfahrensbezogen bedeutet, dass diese Vorlagen/Muster typischerweise im Rahmen der betrieblichen Dokumentation zu einem Fachverfahren erstellt/ergänzt werden müssen.

- 🕮 Quickcheck Sachstandsaufnahme Informationssicherheit / ISMS
- 🕮 Quickcheck Mitarbeitersensibilisierung
- 🕮 Quickcheck Standardregelungen
- 🕮 Quickcheck Internetzugang/Nutzung
- 🕮 Quickcheck Gebäudesicherheit
- 🕮 Quickcheck Beschaffung / Entsorgung
- 🕮 Quickcheck Outsourcing
- 🕮 Quickcheck Clientsicherheit
- 🕮 Quickcheck Serverbetrieb / Zentrale Systeme
- 🕮 Quickcheck Active Directory
- 🕮 Quickcheck Mail
- 🕮 Quickcheck Anwendungssicherheit
- 🕮 Quickcheck Notfallvorsorgemanagement / Notfallmanagement
- 🕮 Quickcheck Querschnittsfragen

9.2 Iteration / Zuordnung im Lebenszyklus

Ein Fachverfahren bzw. IT-Komponenten durchlaufen idealtypisch folgende Lebensphasen:



9.3 Regelungen

- 🕮 **SiKoSH-Konzept Rollen- und Rechte**

  Diese Vorlage für ein Rechte und Rollenkonzept setzt die Anforderungen des BSI IT-Grundschutz sowie datenschutzrechtlichen Anforderungen im Hinblick auf die Dokumentation von Fachverfahren um.

- 🕮 **SiKoSH-Konzept Rollen- und Rechte - Anlage Berechtigungsmanagement**
  Das Muster für ein Berechtigungskonzept enthält Empfehlungen zur Gliederung und zur inhaltlichen Ausgestaltung. In diesem Konzept werden Rollen und deren Berechtigungen definiert. Das Berechtigungskonzept adressiert immer ein konkretes Verfahren.

- 🕮 SiKoSH-Konzept Protokollierung Fachverfahren (in Planung)

10 Notfallmanagement

10.1 Überblick

Die Notfallvorsorge ist logisch zum Ende der Dokumentation eines Fachverfahrens oder anderer IT-Komponenten zu sehen, daher wird final dieser Bereich umgesetzt.

- 🕮 Quickcheck Sachstandsaufnahme Informationssicherheit / ISMS
- 🕮 Quickcheck Mitarbeitersensibilisierung
- 🕮 Quickcheck Standardregelungen
- 🕮 Quickcheck Internetzugang/Nutzung
- 🕮 Quickcheck Gebäudesicherheit
- 🕮 Quickcheck Beschaffung / Entsorgung
- 🕮 Quickcheck Outsourcing
- 🕮 Quickcheck Clientsicherheit
- 🕮 Quickcheck Serverbetrieb / Zentrale Systeme
- 🕮 Quickcheck Active Directory
- 🕮 Quickcheck Mail
- 🕮 Quickcheck Anwendungssicherheit
- 🕮 Quickcheck Notfallvorsorgemanagement / Notfallmanagement
- 🕮 Quickcheck Querschnittsfragen

10.2 Regelungen

- 🕮 SiKoSH-Konzept Notfall (in Planung)
- 🕮 SiKoSH-Muster Notfallübungen (in Planung)

11 Querschnittsprüfung

11.1 Überblick

Schlussendlich hat mit der Abarbeitung des letzten Quickchecks aber auch das ISMS seine erste Iteration durchlebt. Daher sollte nun mit der Bearbeitung des Quickchecks Querschnittsfragen der Erfolg der ISMS Einführung bewertet werden. Dieser Quickcheck kann im weiteren Verlauf der Umsetzung noch offener Prüfpunkte verwendet werden um eine erste, rudimentäre, kennzahlenbasierte Messung des Erfolgs der ISMS-Einführung darzustellen. Dazu kann der Quickcheck Querschnittsfragen z. B. über den Zeitraum von einem Jahr einmal im Quartal neu bearbeitet werden. Idealerweise sollte ein deutlicher Fortschritt bei der Umsetzungsgrad der Prüfpunkte erkennbar sein.

- 🕮 Quickcheck Sachstandsaufnahme Informationssicherheit / ISMS
- 🕮 Quickcheck Mitarbeitersensibilisierung
- 🕮 Quickcheck Standardregelungen
- 🕮 Quickcheck Internetzugang/Nutzung
- 🕮 Quickcheck Gebäudesicherheit
- 🕮 Quickcheck Beschaffung / Entsorgung
- 🕮 Quickcheck Outsourcing
- 🕮 Quickcheck Clientsicherheit
- 🕮 Quickcheck Serverbetrieb / Zentrale Systeme
- 🕮 Quickcheck Active Directory
- 🕮 Quickcheck Mail
- 🕮 Quickcheck Anwendungssicherheit
- 🕮 Quickcheck Notfallvorsorgemanagement / Notfallmanagement
- 🕮 Quickcheck Querschnittsfragen

12 Sicherheitskonzept

12.1 Vorgehensempfehlung

Die Erstellung von Sicherheitskonzepten orientiert sich in ihrer Vorgehensweise am BSI-Standard 100-2 bzw. 200-2.

Das Sicherheitskonzept ist das Hauptdokument im Sicherheitsprozess der Behörde. Es stellt somit die Klammer für die in den SiKoSH-Phasen erstellten Dokumente dar. Es dient der Dokumentation der Sicherheitsstrategie und des Umsetzungsstands der Maßnahmen zur Erreichung der definierten Sicherheitsziele.

🕮 SiKoSH-Konzept 1000_Sicherheitskonzept

Hinweis	Die Erstellung eines (Teil-)Sicherheitskonzeptes stellt auch nach SiKoSH bereits hohe fachliche Anforderungen. Der Einsatz eines Tools zur Unterstützung wird empfohlen[8].

In größeren Verwaltungen ermöglicht die Aufteilung in Teilverbünde eine verteilte Bearbeitung und Pflege durch die jeweiligen Verantwortlichen und reduziert die Aufwände der einzelnen Verfahrensbetrachtung erheblich. Bei Einführung des Sicherheitsmanagements sollte daher einleitend die Aufteilung und Inhalte der einzelnen Teilkonzepte mit allen Bereichen festgelegt werden (Abgrenzung). Folgende Aufteilung ist möglich, hängt konkret dennoch immer von den jeweiligen Bedarfen und individuellen Anforderungen der umsetzenden Institution ab:

Informationsteilverbund	Beschreibung	Verantwortlichkeiten
Raum- und Gebäudeinfrastruktur	Von der Verwaltung genutzte Gebäude, Räume (Büro und Technik), Systemräume, Rechenzentren	Gebäudeverwaltung, (eigene oder die des/der Vermieter), ggf. IT-Outsourcingpartner
Zentrale Infrastruktur	Zentrale und übergreifend genutzte Dienste (z.B. Storage, Monitoring, Softwareverteilung, zentraler Virenschutz, Virtualisierungshosts), Managementsysteme, Netzkomponenten und Netzmanagementsysteme (Sicherheitsgateways/Firewalls, Paketfilter, Application Level Gateways); Zentrale Systemadministration	IT oder externer Dienstleister bei Outsourcing

[8] Eine (nicht abschließende) Liste marktüblicher Tools finden Sie auf den Webseiten des BSI und im Rahmenvertragsangebot des KomFIT.

Informationsteilverbund	Beschreibung	Verantwortlichkeiten
Bürokommunikationsinfrastruktur (BK)	Clientsysteme und Clientmanagement	IT, ggf. IT-Outsourcing-partner
Fachverfahren	Betrachtung der Fachanwendungssoftware sowie weiterer spezifischer Komponenten Sofern erforderlich: Betrachtung verfahrensspezifischer Hardware oder verfahrensspezifischer virtueller Maschinen),	Fachverantwortliche

12.2 Strukturanalyse

Im Rahmen der Strukturanalyse erfolgt die Beschreibung der Verfahrensinfrastruktur, insbesondere die Erfassung aller relevanten Komponenten. Dieses umfasst insbesondere folgende Punkte:

- Relevante Regelungen
- Relevante Raum- und Gebäudeinfrastruktur
- Relevante IT-Systeme und Netze (einschließlich der maßgeblichen Managementsysteme)
- Relevante Personen (insbesondere mit administrativen Rechten)
- Relevante Anwendungen
- Kommunikationsbeziehungen zwischen beteiligten Systemen (insbesondere, wenn diese nicht Teil des betrachteten Verbundes sind[9])

Die identifizierten Komponenten sind zu dokumentieren. Dies kann beispielsweise in Listenform erfolgen. Idealerweise wurden diese Komponenten bereits in einem entsprechenden Verwaltungssystem (wie Configuration Management Database/Asset Management Systemen) erfasst, so dass die für die Strukturanalyse erforderlichen Daten bereits verfügbar sind.

🕮 **SiKoSH-Leitfaden: Erstellung eines Sicherheitskonzepts nach SiKoSH** (Abschnitt Strukturanalyse)

12.3 Schutzbedarfsfeststellung

🕮 **SiKoSH-Leitfaden: Erstellung eines Sicherheitskonzepts nach SiKoSH** (Abschnitt Schutzbedarfsfeststellung)

Zur Erstellung eines Sicherheitskonzeptes ist die Festlegung eines Schutzbedarfes (SB) eine wesentliche Voraussetzung. Es wird empfohlen, die Schutzbedarfsfeststellung insbesondere auf

[9] Das sind beispielsweise IT-Systeme Dritter, mit denen Daten ausgetauscht werden, kann aber auch eine händische Schnittstelle umfassen, wenn hier exportierte Daten weitergegeben werden.

Grundlage der im Verfahren oder der betrachteten Infrastruktur verarbeiteten Daten durchzuführen. Die Feststellung erfolgt auf Grundlage einheitlicher und organisationsweit festgelegter Kriterien (z.B. in der Richtlinie Informationssicherheits- und Datenschutzmanagement).

Zur Durchführung der SB-Feststellung müssen verantwortliche und aussagekräftige Vertreter des Fachbereichs einbezogen werden. Für einfache Verfahren kann der ISB auch den Schutzbedarf eigenständig ermitteln. Eine Bestätigung durch den (Fach-)Verantwortlichen ist jedoch zwingend erforderlich.

12.4 Modellierung und Auswahl der Anforderungen

Mit Vorliegen der Komponenten eines Informationsverbundes kann die Identifikation der relevanten Anforderungen erfolgen. In Abhängigkeit der jeweiligen Komponenten werden die relevanten Bausteine ausgewählt, die wiederum Anforderungen beinhalten. Modellierung nach dem IT-Grundschutzkompendium

Sofern noch keine Vorarbeiten auf Basis der IT-Grundschutzkataloge (BSI-Standard 100-2) durchgeführt worden sind, empfiehlt sich der Einstieg auf Basis des aktualisierten IT-Grundschutzkompendiums (BSI-Standard 200-2) in Verbindung mit dem Kommunalen Grundschutzprofil[10]. Das reduzierte und den Bedürfnissen einer Kommunalverwaltung angepasste Anforderungsset nach diesem Profil ist direkt in die SiKoSH-Mustervorlage zur Erstellung eines Sicherheitskonzepts eingeflossen.

Sofern bereits ein Sicherheitskonzept auf Basis der IT-Grundschutzkataloge erstellt wurde, kann übergangsweise auch deren Maßnahmenset angewendet werden.

SiKoSH-Handreichung Maßnahmenklassifikation und -bewertung

Zur Priorisierung der erforderlichen Maßnahmen sollte diese Excel-Maßnahmenliste verwendet werden. Hier lassen sich die relevanten Bausteine komfortabel auswählen und das erforderliche Maßnahmenset erzeugen.

12.5 Anforderungsprüfung

Die für den Verbund als maßgeblich festgelegten Anforderungen bedürfen der individuellen Überprüfung. Sofern Anforderungen bereits in anderen Verbünden betrachtet wurden (z. B. Anforderungen für dasselbe Gebäude) oder es Standardumsetzungsbeschreibungen gibt (z. B. auf Grundlage einer einheitlichen Regelung für den Betrieb zentraler Server), müssen diese Anforderungen miteinander abgeglichen werden.

[10] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Hilfsmittel/Profile/Basis_Absicherung_Kommunalverwaltung.html

12.6 Risikoanalyse

📖 **SiKoSH-Leitfaden: Erstellung eines Sicherheitskonzepts nach SiKoSH (Abschnitt Sicherheits- und Risikoanalyse)**

Die Risikoanalyse (RA) dient bei der Verfahrensbetrachtung der Identifikation von erhöhten Gefährdungen und der Ableitung von Maßnahmen zur Risikoreduktion. Es empfiehlt sich, eine Risikoanalyse durchzuführen, wenn die Schutzbedarfsfeststellung in einem der Grundwerte Verfügbarkeit/Vertraulichkeit/Integrität mit "hoch" bewertet wurde oder beim Betrieb des Verfahrens unübliche Rahmenbedingungen beachtet werden müssen.

Die bereitgestellte RA-Vorlage umfasst eine Auflistung der möglichen Gefährdungen (46 elementare Gefährdungen), die im Rahmen der RA einzeln bewertet werden müssen. Im Anschluss an diese Bewertung werden für die als "erhöht" bewerteten Gefährdungen Maßnahmen identifiziert, die diese Risiken reduzieren können. Nach der Identifikation erfolgen die Bewertung der Zweckmäßigkeit und Umsetzbarkeit, die Dokumentation und die Inkraftsetzung durch den Infrastruktur- oder Verfahrensverantwortlichen.

13 Kommunenübergreifende Kooperation

Hinweis	Die Ergänzung und Detailbetrachtung der Kooperationsmöglichkeiten sowie Möglichkeiten zur konkreten Umsetzung wird fortlaufend im SiKoSH-Arbeitskreis betrachtet und beschrieben.

Folgende grundsätzlich geeignete Kooperationsfelder wurden bisher identifiziert:

- Standardisierung von technischen Lösungen
- Gemeinsame Betrachtung gleicher bzw. ähnlicher Verfahren
    - Schutzbedarf/Risikoanalyse
    - Sicherheitsbezogene Konzepte
    - …
- Vereinheitlichung von Anforderungen im Rahmen der Beschaffung
- Notfallvorsorge und Notfallmanagement
- Gegenseitige/Wechselseitige Prüfungen der festgelegten Sicherheitsmaßnahmen
- Dokumentationsaufgaben

14 Anhang

14.1 Glossar

Begriffe werden zentral unter www.sikosh.de erklärt.

15 Qualitätssicherung

Zur laufenden Qualitätssicherung ist ein Feedback in Form von Anregungen, Wünschen, Änderungsvorschlägen sehr erwünscht. Senden Sie hierzu bitte eine E-Mail an sikosh@komfit.de.

16 Das Kleingedruckte

Dieses und alle weiteren SiKoSH-Dokumente wurde von der Projektgruppe SiKoSH im Auftrag der Kommunalen Landesverbände in Schleswig-Holstein entwickelt.

Bei Rückfragen wenden Sie sich bitte an Herrn Frank Weidemann (frank.weidemann@komfit.de).