ITV.SH
Kommunale Digitalisierung

# Leitfaden:
# Einführung und Betrieb eines Informations-Sicherheits-Management-Systems (ISMS)




Aus der Praxis für die Praxis. Informationssicherheit ist Gemeinschaftsaufgabe.

# Informationen zum Dokument

**. 1: Kontakt**

| | |
|---|---|
| Herausgeber | IT-Verbund Schleswig-Holstein AöR (ITVSH)<br>https://itvsh.de/ |
| Web | https://www.sikosh.de |
| E-Mail | sikosh@itvsh.de |

**. 2: Nutzungsbedingungen**

| | |
|---|---|
| Urheberschaft und Nutzungsrecht | Es gelten die auf der SiKoSH Website aufgeführten Nutzungsbedingungen für SiKoSH. |
| Haftungsausschluss | Die Dokumente des SiKoSH ISMS durchlaufen einen mehrstufigen Prozess der Qualitätssicherung. Trotzdem können Fehler und unscharfe Formulierungen in den Dokumenten nicht ausgeschlossen werden, ebenso wenig Missverständnisse durch die Nutzer und Übernehmer. |
| Feedback | Das Projekt versteht sich als Gemeinschaftsaufgabe seiner Anwender. Informationen zu Veränderungen, Bearbeitungen, neue Gestaltungen oder sonstige Abwandlungen der bereitgestellten Dokumente an sikosh@itvsh.de verbessern die Dokumente und ihre Verwendbarkeit. |

**. 3: Dokumenten Informationen**

| | |
|---|---|
| Titel | Leitfaden: Einführung und Betrieb eines Informations-Sicherheits-Management-Systems (ISMS) |
| Version | 2.9.4 |
| Art | Leitfaden/Richtlinie |
| Formatierung | Styleguide 3.0.0 |
| TLP | Clear |
| Dateiname | SiKoSH_Leitfaden |
| veröffentlicht am | 19.10.2026 |

**. 4: Ihre Notizen**

| |
|---|
| |
| |
| |
| |
| |
| |
| |
| |
| |
| |
| |
| |

# Inhalt

0 Überblick 6
0.1 Zielsetzung von SiKoSH 6
0.2 Zielpersonen 6
0.3 Was ist SiKoSH? 6
0.4 Zertifizierung 7
0.5 Zentrale Aspekte, Komponenten und Begriffe 7
1 Einführung ISMS 10
1.1 Warum überhaupt ein ISMS? 10
1.2 Warum SiKoSH? 11
1.3 BSI IT-Grundschutz-Methodik und kommunales IT-Grundschutz-Profil 11
1.4 . Voraussetzungen für die erfolgreiche Anwendung von SiKoSH 12
1.5 Verankerung in der Organisation 13
1.6 Effizienz des ISMS 13
1.7 Wirtschaftlichkeit des ISMS 13
1.8 Internes Kontrollsystem, Nachhaltigkeit 13
2 SiKoSH einführen 15
2.1 Ziel von SiKoSH: Vermittler zwischen Theorie und Praxis 15
2.2 Vorteile von SiKoSH 17
3 Mit SiKoSH arbeiten 18
3.1 SiKoSH Aktivitätsdiagramm 18
3.2 Regelmäßig wiederkehrende Aufgaben 19
3.3 Arbeiten mit den Quickchecks 20
3.4 Tabellen „Übersicht Dokumente“ zu den SiKoSH Phasen 20
4 SiKoSH Phase 1: Sicherheitsmanagement und Organisation 22
4.1 Umsetzung Phase 1 22
4.2 Start: ISMS-Arbeitsgruppe gründen 22
4.3 Bestandsaufnahme Sicherheitsmanagement und Organisation 23
4.4 Grundlagen schaffen 23
4.5 Organisationsstruktur aufbauen 24
4.6 Identitäts- und Berechtigungsmanagement 25
4.7 Ziel SiKoSH Phase 1: Grundlegende ISMS-Struktur aufgebaut 25
4.8 Übersicht: Dokumente zur SiKoSH Phase 1 25
5 SiKoSH Phase 2: Personal, Sensibilisierung und Schulung 27

5.1 Bestandsaufnahme Personal, Sensibilisierung und Schulung ..... 27
5.2 Sensibilisierung planen und starten ..... 27
5.3 Informationssicherheit lernen ..... 29
5.4 Sensibilisierung der Leitungsebene ..... 29
5.5 Übersicht: Dokumente der SiKoSH Phase 2 ..... 30
6 SiKoSH Phase 3: Standardregelungen ..... 31
6.1 Überblick ..... 31
6.2 Übersicht: Dokumente der SiKoSH-Phase 3 ..... 31
7 SiKoSH Phase 4: Allgemeine Musterregelungen ..... 35
7.1 Überblick ..... 35
7.2 Übersicht: Dokumente der SiKoSH Phase 4 ..... 36
8 SiKoSH Phase 5: Technische Musterregelungen ..... 38
8.1 Überblick ..... 38
8.2 Übersicht: Dokumente der SiKoSH Phase 5 ..... 39
9 SiKoSH Phase 6: Regelungen für Verfahren ..... 41
9.1 Überblick ..... 41
9.2 Iteration – Zuordnung im Lebenszyklus ..... 41
9.3 Übersicht: Dokumente der SiKoSH Phase 6 ..... 41
10 SiKoSH Phase 7: Notfallmanagement ..... 42
10.1 Überblick ..... 42
10.2 Übersicht: Dokumente der SiKoSH-Phase 7 ..... 42
11 SiKoSH Ziel - Querschnittsprüfung ..... 43
11.1 Überblick ..... 43
11.2 Übersicht: Dokumente der SiKoSH-Querschnittsprüfung ..... 43
12 Sicherheitskonzept ..... 44
12.1 Was mit SiKoSH erreicht wird ..... 44
12.2 Empfehlung für das weitere Vorgehen ..... 44
12.3 IT-Strukturanalyse ..... 44
12.4 Bisher noch nicht berücksichtigte Basis-Anforderungen ..... 45
12.5 Standardabsicherung ..... 45
12.6 Risikomanagement ..... 45
12.7 Revision ..... 46
13 Anhang ..... 47
13.1 Glossar ..... 47

# Tabellen

Tabelle 1: Dokumente für den SiKoSH Kickoff 9
Tabelle 2: SiKoSH Phase 1 – Übersicht Dokumente 25
Tabelle 3: SiKoSH Phase 2 – Übersicht Dokumente 30
Tabelle 4: SiKoSH Phase 3 – Übersicht Dokumente 31
Tabelle 5: SiKoSH Phase 4 – Übersicht Dokumente 36
Tabelle 6: SiKoSH Phase 5 – Übersicht Dokumente 39
Tabelle 7: SiKoSH Phase 6 – Übersicht Dokumente 41
Tabelle 8: SiKoSH Phase 7 – Übersicht Dokumente 42
Tabelle 9: SiKoSH Schritt 9 – Querschnittsprüfung: Übersicht Dokumente 43

# Abbildungen

Abb. 1: Hierarchisch-analytisches Vorgehen ..... 15
Abb. 2: Beispiel: Theorie und Praxis in Schulsystemen ..... 16
Abb. 3: ISMS-Komponenten ..... 17
Abb. 4: SiKoSH Aktivitätsdiagramm ..... 18
Abb. 5: PDCA-Methode der Einführung und des Betriebs eines ISMS ..... 19
Abb. 6: Aktivitätsdiagramm SiKoSH Phase 1 ..... 22
Abb. 7: Aktivitätsdiagramm SiKoSH Phase 2 ..... 27
Abb. 8: Lernkontinuum Informationssicherheit ..... 29
Abb. 9: Aktivitätsdiagramm SiKoSH Phase 3 ..... 31
Abb. 10: Aktivitätsdiagramm SiKoSH Phase 4 ..... 35
Abb. 11: Aktivitätsdiagramm SiKoSH Phase 5 ..... 38
Abb. 12: Aktivitätsdiagramm SiKoSH Phase 6 ..... 41
Abb. 13: Aktivitätsdiagramm SiKoSH Phase 7 ..... 42

# 0 Überblick

## 0.1 Zielsetzung von SiKoSH

Mit vielen Hilfsmitteln wie Einstiegshilfen, Anleitungen und Vorlagen für die ISMS-Dokumentation.

Der hier vorliegende Leitfaden**: „Einführung und Betrieb eines Informationssicherheitssystems (ISMS)**“ ist ein vereinfachtes Vorgehensmodell für den Aufbau und Betrieb eines entwicklungsfähigen **Informations-Sicherheits-Management-Systems (ISMS)** mit vielen Hilfsmitteln wie Einstiegshilfen, Handreichungen, Anleitungen und Vorlagen für die ISMS-Dokumentation.

Kursiv gedruckte Begriffe werden im SiKoSH-Glossar (https://itvsh.de/was-wir-tun/it-sicherheit/sikosh-glossar) definiert.

Ein ***ISMS*** besteht grundsätzlich aus:

- einer *Aufbauorganisation* (Rollenträger),
- einer *Ablauforganisation* (Prozesse/Verfahren),
- einem Regelwerk (Richtlinien und Konzepte),
- Technologie
- und seiner Umsetzung

zur Gewährleistung der Sicherheitsziele *Vertraulichkeit*, *Integrität* und *Verfügbarkeit*.

## 0.2 Zielpersonen

SiKoSH wendet sich an alle Stakeholder im Informationssicherheitsmanagementprozess. Typischerweise sind das: Behördenleitung, *Informationssicherheitsbeauftragte (ISB)*, *Datenschutzbeauftragte (DSB)*, *IT-Verantwortliche (IT-Leitung)*, andere wichtige Rollenträger (Personalabteilung, Personalrat, etc.) und *Systemadministratoren*. Idealerweise haben die angesprochenen Personen ein Grundverständnis in den Bereichen *IT-Governance*, Informationssicherheitsmanagement, Datenschutzrecht und Informationstechnik[1].

## 0.3 Was ist SiKoSH?

SiKoSH. Das ISMS aus der Praxis für die Praxis

SiKoSH (Sicherheit für Kommunen in Schleswig-Holstein) ist ein ISMS-Framework, das in partnerschaftlicher Zusammenarbeit durch den IT-Verbund Schleswig-Holstein (ITV.SH AöR), der Staatskanzlei Schleswig-Holstein (Zentrales IT-Management), dem Unabhängigen Landeszentrum für Datenschutz, dem Landesrechnungshof Schleswig-Holstein und zahlreichen Praktikern aus Schleswig-Holsteins Kommunalverwaltungen entwickelt und gepflegt wird.

SiKoSH ermöglicht einen einfachen und schnellen Einstieg in den Aufbau und den Betrieb eines entwicklungsfähigen Informationssicherheitsmanagementsystems (**ISMS)**. Obwohl primär für den Einsatz in schleswig-holsteinischen Kommunen entwickelt, steht es allen Interessierten kostenfrei zur Verfügung und kann nicht nur von Behörden, sondern prinzipiell auch von KMU eingesetzt werden. SiKoSH ist ein ISMS-Framework aus der Praxis für die Praxis und gibt den Anwendenden Vorlagen, Materialien, Hilfestellungen und Werkzeuge an die Hand.

… damit Informationssicherheits-Management machbar wird.

Dem **SiKoSH-Leitfaden** (auch SiKoSH-Framework genannt) liegt das *IT-Grundschutz-Profil „Basis-Absicherung* Kommunalverwaltung“ der bundesweiten Arbeitsgruppe Kommunale Basis-Absicherung (AG koBa) in der jeweils aktuellen Version zugrunde. Das IT-Grundschutz-

[1] Eine differenzierte Rollenbeschreibung erfolgt in der Informationssicherheitsleitlinie (*ISLL*) unter https://netzwerk.itvsh.de/project/sikosh-isms/file/sikosh_informationssicherheitsleitlinie_isll/download/SiKoSH_Informationssicherheitsleitlinie_(ISLL).docx.

Profil Basis-Absicherung Kommunalverwaltung[2] erleichtert den Einstieg in die Informationssicherheit und hilft die größten Schwachstellen aufzudecken.

SiKoSH erlaubt es, den gesetzlichen Verpflichtungen nachzukommen und eine sichere Informationsverarbeitung (Ordnungsmäßigkeit des staatlichen Handelns) zu etablieren.

## 0.4 Zertifizierung

BSI Testat Basis-Absicherung

Die Ergebnisse von SiKoSH tragen dazu bei, eine Prüfung auf ein Testat nach der *Basis-Absicherung*[3] beantragen zu können.

Das Testat stellt ein Zwischenschritt dar, um mit Umsetzung weiterer Sicherheitsanforderungen eine Zertifizierung nach *IT-Grundschutz* auf Basis *ISO 27001* er erlangen[4].

## 0.5 Zentrale Aspekte, Komponenten und Begriffe

### 0.5.1 SiKoSH-Prozess

9 Schritte, 7 Bearbeitungsphasen

Der SiKoSH-Prozess besteht aus **neun Schritten**: aus S – Start, Z – Ziel und dazwischen die **sieben SiKoSH-Phasen.**

Im ersten Schritt (Start) wird eine temporäre Arbeitsgruppe eingerichtet, die den ISMS-Prozess anstößt. Der neunte Schritt (Ziel) – die **Querschnittsprüfung** – wird nach Abschluss der SiKoSH-Phase 7 (Notfall-Management) getan.

Querschnitts-Check

Die **Querschnittsprüfung** (auch: Querschnitts-Check) fasst alle Anforderungen aus den Quickchecks der sieben Phasen zusammen. Die Querschnittsprüfung (QP) kann auch mit dem Start des SiKoSH-Prozesses als Selbsteinschätzung verwendet werden, um das allgemeine Sicherheitsniveau der Organisation einzuschätzen und eine fundierte Entscheidung darüber zu treffen, welche SiKoSH-Phase bzw. welche Regelungen und Vorgaben aus welchen SiKoSH-Phasen zeitnah und mit Nachdruck umgesetzt werden müssen.

### 0.5.2 SiKoSH Phasen

SiKoSH fasst die Regelungen, die für die Basis-Absicherung umgesetzt werden müssen, in diesen sieben Phasen zusammen:

- Phase 1: Informationssicherheitsmanagement und Organisation
- Phase 2: Personal – Mitarbeitersensibilisierung und -schulung
- Phase 3: Standardregelungen
- Phase 4: Allgemeine Regelungen
- Phase 5: Technische Regelungen
- Phase 6: Anwendungssicherheit

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

[3] https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/Zertifizierte-Informationssicherheit/Testat-nach-der-Basisabsicherung/Ablauf-eines-Testatverfahrens/ablauf-eines-testatverfahrens.html

[4] https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/Zertifizierte-Informationssicherheit/Testat-nach-der-Basisabsicherung/testat-nach-der-basisabsicherung_node.html

- Phase 7: Notfallmanagement

### 0.5.3 Arten von SiKoSH Dokumenten und Materialien

SiKoSH Dokumentenarten

Das SiKoSH ISMS Framework besteht aus dem SiKoSH-Leitfaden mit seinen Richtlinien und den SiKoSH-Hilfsmitteln.

Leitfaden und Richtlinien

Die Richtlinien fassen die Regelungen des SiKoSH Frameworks entsprechend den SiKoSH-Phasen in handhabbare Gruppen zusammen. Leitfaden und Richtlinien sagen im Wesentlichen was gemacht werden muss, was gemacht werden MUSS, SOLL und DARF, damit die definierten Sicherheitsziele erreicht werden.[5]

Informationssicherheitsleitlinie (ISLL)

Die *Informationssicherheitsleitlinie* (ISLL) hat als Leitdokument des SiKoSH-Dokumentensatzes eine besondere Rolle. Sie wird von SiKoSH als Vorlage zur Verfügung gestellt und schafft die Grundlagen für den Sicherheitsprozess in der anwendenden Einrichtung.

Hilfsmittel

Hilfsmittel helfen dem Anwender, die im SiKoSH Leitfaden mit seinen Richtlinien spezifizierten Anforderungen aufwandsarm zu erreichen. Zu den Hilfsmitteln zählen Vorlagen, Anleitungen, Beispiele, Hinweise und viele andere nützliche Hilfen. SiKoSH Hilfsmittel helfen dabei, die Regelungen des ISMS (Richtlinien) in der Praxis vor Ort umzusetzen.

Quickchecks

Ein besonderes Hilfsmittel sind die Quickchecks, die mit ihren Prüfpunkten einen Überblick über die Sicherheitslage geben und den Stand der Umsetzung des Leitfadens mit seinen Richtlinien dokumentieren. Jede SiKoSH-Phase wird von einem Quickcheck eingeleitet: Sie enthalten Prüffragen zu den kommunalen Basis-Anforderungen, Verweise auf hilfreiche SiKoSH-Dokumente, Umsetzungstipps und können als Soll/Ist Vergleich verstanden werden.

Richtlinien

Ab der Dokumentenversion 3.0 enthalten Richtlinien ausschließlich Regelungen und können nach individueller Anpassung direkt als Dienstanweisung oder Dienstvereinbarung genutzt werden.

Konzepte

Die Konzepte beschreiben die organisatorische und technische Umsetzung.

Sicherheitskonzept

Die in der Bearbeitung der SiKoSH-Phasen erstellten und an die Bedürfnisse der Behörde angepassten Handreichungen und Betriebshandbücher sind Teil der Sicherheitsdokumentation der anwendenden Einrichtung. Zusammen mit weiteren wichtigen Dokumenten wie der *Struktur*- und *Risikoanalyse* ergibt sich daraus im Anschluss von SiKoSH das Sicherheitskonzept.

SiKoSH Styleguide

Der SiKoSH Styleguide mit seiner Dokumentvorlage hilft den Anwendern dabei, ein einheitliches Design des Dokumentensatzes beizubehalten.

### 0.5.4 SiKoSH Start – Dokumente für den Kickoff

SiKoSH Anwender sollten sich mit diesen drei Dokumenten vertraut machen:

- SiKoSH-Leitfaden
- ISMS-Übersicht

[5] Siehe IT-Grundschutz-Kompendium (https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/it-grundschutz-kompendium_node.html)

- SiKoSH-Styleguide

Registrierte SiKoSH-Anwender laden SiKoSH Dokumente mit einem Klick auf die entsprechende Formatanzeige in der Tabelle (.pdf, .docx, .dotx, .xlsx) zur weiteren Verwendung herunter.

Tabelle 1: Dokumente für den SiKoSH Kickoff

| Titel des Dokuments – Beschreibung |
|---|
| **„Leitfaden – Einführung und Betrieb eines Informationssicherheitsmanagementsystems (ISMS)“** [dieses Dokument]<br>Hauptdokument des SiKoSH ISMS Frameworks mit Verweisen auf alle Richtlinien des Leitfadens |
| **Hilfsmittel „Styleguide“** [↓.pdf \| .dotx ]<br>Anleitung für Bearbeitung und Erstellung von Dokumenten in einem einheitlichen bzw. im SiKoSH Layout (mit MS Word Dokumentenvorlage) |
| **Hilfsmittel „Bearbeiten der ISMS-Übersicht“** [↓.pdf]<br>Anleitung zum Umgang mit der ISMS-Übersicht |

### 0.5.5 PDCA-Zyklus

PDCA

*„**P**lan – **D**o – **C**heck – **A**ct“ – der PDCA-Zyklus (*Demingkreis oder auch Shewhart Cycle) beschreibt einen iterativen drei- bzw. vierphasigen Prozess für Lernen und Verbesserung und ist ein permanenter Verbesserungsprozess: die sieben SiKoSH-Phasen und die Querschnittsprüfung werden immer wieder durchlaufen. Der ISMS-Prozess ist nie abgeschlossen: Er ist eine Qualitätsmanagement-Routine, die die permanente Anpassung des Sicherheitsniveaus an ein sich ständig änderndes Sicherheitslagebild erfordert (siehe auch 3.2 Regelmäßig wiederkehrende Aufgaben).

# 1 Einführung ISMS

## 1.1 Warum überhaupt ein ISMS?

SiKoSH – das ISMS für kommunale Einrichtungen

Behördenleitungen tragen im Rahmen ihrer Organisationsverantwortung auch die Gesamtverantwortung für den Schutz von sensiblen Informationen. Im Behördenumfeld sind das insbesondere *personenbezogene Daten*. Hier sind neben den *Schutzzielen* der Informationssicherheit auch die *Gewährleistungsziele* des Datenschutzes zu beachten.

Ein sicherer Betrieb von IT-Komponenten reicht alleine nicht aus, da dieser immer nur eine Momentaufnahme darstellt. Vielmehr ist es erforderlich die Informationssicherheits- und Datenschutzprozesse ganzheitlich zu denken und zu planen, den gesamten Ablauf von der Beschaffung von IT-Komponenten (Hardware, Software und Verfahren) bis zur Aussonderung.

Mindestanforderungen der Rechnungshöfe

Einen risikofreien IT-Betrieb gibt es nicht. Durch ein professionelles Informationssicherheits- und Datenschutzmanagement reduziert sich das Risiko für Systemausfälle (*Verfügbarkeit*), Datenabflüsse (*Vertraulichkeit*) oder Manipulation (*Integrität*) eingesetzter IT-Komponenten erheblich und damit auch das Risiko für einen Verstoß gegen Gesetze und den Eintritt materieller oder immaterieller Schäden. Auch die Rechnungshöfe des Bundes und der Länder erwarten zur Erreichung der grundlegenden Sicherheitsziele Vertraulichkeit, Integrität und Verfügbarkeit die Entwicklung einer übergreifenden Sicherheitsstrategie und den Betrieb eines der Einrichtung angemessenen *ISMS*[6].

Gesetzliche Vorgaben für Behörden

Behörden sind in einem besonderen Maße an gesetzliche Vorgaben gebunden. Im Kontext Informationssicherheit seien hier insbesondere die Leitlinie für die Informationssicherheit in der öffentlichen Verwaltung des IT-Planungsrates[7] als Voraussetzung für die Nutzung ebenenübergreifender IT-Verfahren, das Onlinezugangsgesetz (OZG) mit korrespondierender Rechtsverordnung zur Gewährleistung der IT-Sicherheit der im Portalverbund und zur Anbindung an den Portalverbund genutzten IT-Komponenten (ITSiV-PV)[8] sowie die Datenschutz-Grundverordnung (*DSGVO*) mit Grundsätzen zur Verarbeitung personenbezogener Daten genannt.

Informationssicherheit unterstützt den Datenschutz

Die Informationssicherheit kann als Unterstützungsprozess für den Datenschutz betrachtet werden. Der BSI-Grundschutz fordert im Baustein CON.2 die Beachtung der Datenschutzgesetze und empfiehlt die Umsetzung des Standard-Datenschutzmodells (*SDM*)[9]. Das SDM schreibt dazu: „Das SDM steht in einer engen Beziehung zur Grundschutzmethodik des Bundesamtes für Sicherheit in der Informationstechnik (BSI). Der vom BSI entwickelte IT-Grundschutz ermöglicht es, durch ein systematisches Vorgehen notwendige Sicherheitsmaßnahmen zu identifizieren und umzusetzen. Die BSI-Standards beschreiben bewährte Vorgehensweisen, das IT-Grundschutz-Kompendium konkrete Anforderungen. Bei der Auswahl von Maßnahmen orientiert sich der IT-Grundschutz vorrangig an den aus der IT-Sicherheit bekannten Schutzzielen Verfügbarkeit, Integrität und Vertraulichkeit.“

[6] Vgl. Nr. 2.3 der Mindestanforderungen der Rechnungshöfe des Bundes und der Länder zum Einsatz der Informationstechnik (https://www.bundesrechnungshof.de/SharedDocs/Downloads/DE/veröffentlichungen_brh_lrh/it-mindestanforderungen.html)

[7] https://www.it-planungsrat.de/fileadmin/beschluesse/2019/Beschluss2019-04_TOP12_Anlage_Leitlinie.pdf

[8] https://www.gesetze-im-internet.de/itsiv-pv/BJNR001800022.html

[9] https://www.datenschutzzentrum.de/sdm/

Somit fordern beide Managementsysteme die Umsetzung von Maßnahmen – in der BSI IT-Grundschutz Methodik auch Anforderungen und im Datenschutzrecht *technische und organisatorische Maßnahmen* (TOM) genannt – die das Risiko des Betriebs von IT-Komponenten auf ein vertretbares Restrisiko (*Risikoakzeptanz*) senken.

Die Gewährleistungsziele des Datenschutzrechts oder die Teilnahmevoraussetzungen für die Bereitstellung digitaler Dienste können ohne sichere Informationsverarbeitung nicht erreicht werden. Informationssicherheit wird durch den Aufbau und Betrieb eines ISMS gewährleistet.

Grundlage für Notfallmanagement

Die Dokumentation aller sicherheitsrelevanten Architekturen, Verfahren und Prozesse ist auch ein relevanter Unterstützungsprozess für den Aufbau eines *Notfallmanagements*.

Grundlage für Risikoverlagerung

Eine Verlagerung finanzieller Risiken durch Schäden - z. B. durch eine Cyberversicherung - ist zudem nach den Versicherungsbedingungen auch erst dann möglich, wenn man ein den entsprechenden Versicherungsobliegenheiten entsprechendes ISMS nachweisen kann.

## 1.2 Warum SiKoSH?

SiKoSH ist ein „Do-it-Yourself ISMS"

Der SiKoSH-Leitfaden ist kein Ersatz für andere, große ISMS-Frameworks ISO/IEC 27001 oder BSI IT-Grundschutz, führt aber dort hin. SiKoSH ist ein einfacher Einstieg in den professionellen Betrieb eines ISMS einer Behörde. SiKoSH begreift sich als *Do-it-Yourself ISMS,* welches durch Quickchecks, Mustervorlagen, Hinweise und viele andere Hilfsmittel den Weg zur Basis-Absicherung nach BSI IT-Grundschutz leichtmacht.

Der SiKoSH-Leitfaden erfüllt den Wunsch vieler Anwender nach einem einfachen Einstieg in Aufbau und Betrieb eines entwicklungsfähigen ISMS bis zur Basis-Absicherung nach BSI IT-Grundschutz. Ziel der Basis-Absicherung ist eine grundlegende Erst-Absicherung über alle Geschäftsprozesse mit vergleichsweise geringem finanziellem, personellem und zeitlichem Aufwand.

## 1.3 BSI IT-Grundschutz-Methodik und kommunales IT-Grundschutz-Profil

Die Grundschutzmethodik ist im BSI-Standard 200-2 beschrieben. Der BSI-Standard 200-2 ist die Grundlage für den Aufbau des SiKoSH-ISMS.

Die BSI IT-Grundschutz-Methodik unterscheidet zwischen

- *Kern-Absicherung*
- *Standard-Absicherung* und
- Basis-Absicherung.

Kern-Absicherung

Die **Kern-Absicherung** sichert besonders schützenswerte Informationen und Geschäftsprozesse und bietet maximalen Schutz für die „Kronjuwelen" der Einrichtung.

Standard-Absicherung

Mit der **Standard-Absicherung** wird durch die Umsetzung von organisatorischen, personellen, infrastrukturellen und technischen Sicherheitsanforderungen ein Sicherheitsniveau erreicht, das für den normalen Schutzbedarf angemessen ist und dem Stand der Technik[10] entspricht.

Basisabsicherung

Mit der **Basis-Absicherung** wird ein Sicherheitsniveau erreicht, das zwar unter dem der Standardabsicherung liegt, aber eine breite, grundlegende Erstabsicherung erreicht und eine gute Grundlage für eine spätere Standard-Absicherung ist.

Kommunale Basis-Absicherung

Ziel von SiKoSH ist ein ISMS mit dem Sicherheitsniveau „**kommunale Basis-Absicherung**“ auf Grundlage des „IT-Grundschutz-Profil BASIS-ABSICHERUNG KOMMUNALVERWALTUNG (kommunales IT-Grundschutz-Profil)“ der AG KoBA[11] in der jeweils aktuellen Version[12]. An dieser Stelle sei deutlich darauf hingewiesen, dass die Basis-Absicherung zwar einen vereinfachten Einstieg in die Grundschutz-Methodik darstellt, aber trotz des reduzierten Maßnahmensets insbesondere für kleinere Behörden immer noch mit einem spürbaren Aufwand an personellen und finanziellen Ressourcen verbunden ist.

kommunales IT-Grundschutz-Profil

Das Kommunale IT-Grundschutz-Profil benennt dabei auf der Basis einer typischen Kommunalverwaltung die umzusetzenden BSI-Bausteine und die zur Umsetzung der Basis-Absicherung erforderlichen Anforderungen.

Hinsichtlich des Schutzniveaus definiert das kommunale IT-Grundschutz-Profil ein Niveau, das nach Vorgabe der referenzierten BSI IT-Grundschutz Bausteine mindestens die Anforderungen der Basis-Absicherung umsetzt.

Basis-Absicherung und Testat

Die Beschränkung auf die Basis-Absicherung ermöglicht eine schnelle Anhebung des Sicherheitsniveaus der Einrichtung. Ziel ist die Definition von Mindestsicherheitsmaßnahmen, die in einer Kommunalverwaltung umzusetzen sind, damit eine Haftung aufgrund grober Fahrlässigkeit grundsätzlich ausgeschlossen werden kann.[13]

Das BSI bietet auch ein Testat zur Basisabsicherung an. SiKoSH bereitet auf die Zertifizierung nach BSI IT-Grundschutz Basisabsicherung vor.

An dieser Stelle sei ausdrücklich darauf hingewiesen, dass nach Erreichen der Basisabsicherung das ISMS schrittweise hin zur Standardabsicherung ausgebaut werden sollte. Hinweise hierzu gibt es im Kapitel 12.

## 1.4 Voraussetzungen für die erfolgreiche Anwendung von SiKoSH

Entwicklung und Betrieb eines ISMS nach dem SiKoSH-Leitfaden gelingen am besten, wenn der Anwender zumindest ein Grundverständnis im Bereich IT-Governance und Informationssicherheitsmanagement hat. Idealerweise wird dieses Wissen durch Grundkenntnisse im Bereich Datenschutzrecht (LDSG (SH)[14], DSGVO), IT-Grundschutz des BSI und einem grundsätzlichen Verständnis von Informationstechnik und Netzwerken ergänzt.

[10] IT-Grundschutzkompendium Seite 3, 2. Absatz
[11] https://info.it-sibe-forum.de/dokumente/it-grundschutz-profil
[12] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Hilfsmittel/Profile/Basis_Absicherung_Kommunalverwaltung.html
[13] Vgl. Nr. 5.2 des kommunalen IT-Grundschutz-Profils
[14] https://dsgvo-gesetz.de/ldsg-sh/

## 1.5 Verankerung in der Organisation

Gelebte Informationssicherheit

Die Verankerung der Informationssicherheit in allen Bereichen des Verwaltungsbetriebes braucht einige Rahmenbedingungen. Diese werden typischerweise mit entsprechenden Regelungen in der Organisation unter Einbeziehung der betroffenen Bereiche und weiterer Mitbestimmungsgremien abgestimmt und in Kraft gesetzt.

## 1.6 Effizienz des ISMS

Effiziente Informationssicherheit

Durch die Einbettung der Informationssicherheit in die Verwaltungsprozesse (Umsetzung und Beachtung von Sicherheitsmaßnahmen in bestehenden betrieblichen Prozessen und Arbeitsabläufen) soll erreicht werden, dass die Umsetzung von technischen und organisatorischen Sicherheitsmaßnahmen von den Mitarbeiterinnen und Mitarbeitern akzeptiert wird und verlässlich erfolgt (Effizienz des ISMS).

## 1.7 Wirtschaftlichkeit des ISMS

Finanzierbare Informationssicherheit

Sicherheitsmaßnahmen sollen wirtschaftlich umgesetzt werden können. Die Prozesse stellen daher standardisierte Abläufe bereit, die für spezifische Aufgaben des Sicherheits- und teilweise auch Datenschutzmanagements genutzt werden können (Wirtschaftlichkeit des ISMS).

ISMS-Vorgehensweisen

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

- **Variante 1:**
  Es werden immer einzelne, für einen spezifischen Aspekt relevante Regelungen in der Organisation verankert. Das kann beispielsweise auf Grundlage der bereitgestellten Regelungsmuster (Richtlinien) erfolgen. Dadurch wird es möglich, für konkrete Prozesse und Vorgänge dedizierte Sicherheitsanforderungen in fachbezogenen Regelungen zu verankern. Empfehlenswert ist dieses Vorgehen insbesondere für größere Organisationen, die typischerweise eine ausgeprägte Verwaltungsstruktur aufweisen.
- **Variante 2:**
  Die vom Leitfaden bereitgestellten Muster für sicherheitsrelevante Regelungen haben hier überwiegend Checklistencharakter („Habe ich an Punkt XY gedacht?“).

Diese Variante bietet sich insbesondere für (kleinere) Verwaltungen mit wenig fachbereichsbezogenen Strukturen an, bei denen es keine Spezialregelung gibt oder die Umsetzung nicht empfehlenswert ist.[15]

## 1.8 Internes Kontrollsystem, Nachhaltigkeit

ISMS-Verfügbarkeit ist wichtig

Um ein dauerhaft geltendes und aktuelles Regelwerk sowie einen durchgängigen Bekanntheitsgrad zu erreichen, müssen betroffene Mitarbeiter von den Regelungen Kenntnis haben und diese Regelungen jederzeit in ihrer aktuellen Version verfügbar sein (Publikation im Intranet, Fileserver, Dokumentenmanagementsystem etc.).

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

Die Aktualität des Regelwerkes ist durch regelmäßige Reviews, aber auch durch 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.

# 2 SiKoSH einführen

## 2.1 Ziel von SiKoSH: Vermittler zwischen Theorie und Praxis

ISMS-Frameworks werden von Sicherheitsschaffenden (Systembetreuer, Informationssicherheitsbeauftragte (ISB)) und ihren Vorgesetzten mitunter mit Skepsis betrachtet. Als wichtigster Grund für die Skepsis wird meist der Umfang der mit dem ISMS verbundenen Dokumentation genannt.

ISMS – dokumentiertes Informationssicherheitsmanagement

Zum einen füllen ISMS-Frameworks wie BSI IT-Grundschutz, *ISO/IEC 27001* und das *NIST Cybersecurity Framework* selbst viele Seiten und es kommt hinzu, dass alle ISMS-Frameworks auf Dokumentation Wert legen. Ohne dokumentiertes Informationssicherheitsmanagement gibt es kein Zertifikat der erreichten Sicherheit.

Sicherheitskultur

Natürlich kann man auch ohne ein von einer Fachorganisation oder einer Behörde gepflegtes ISMS-Framework das Netzwerk mit seinen Komponenten sicher machen. Aber tatsächlich haben auch Organisationen ohne ISMS ein ISMS. In Organisationen ohne dokumentiertes ISMS sind die Regeln für den Umgang mit Informationssicherheit und Datenschutz lediglich nicht aufgeschrieben**.** Es gibt eine Art „orale Sicherheitskultur“ und das ist bekanntermaßen kein guter Weg, die Herausforderungen der Digitalisierung zu bewältigen. Checklisten und Konfigurationsanleitungen hat jeder, der komplizierte Geräte und Abläufe in Ordnung halten will und muss.

Ein ISMS ist nichts anderes als die Fortentwicklung von vor-professionellem Management von IT- und Informationssicherheit zu professionellem Management von IT- und Informationssicherheit. Einer der wichtigsten Zwecke eines ISMS ist dabei die Dokumentation der Regeln und Maßnahmen mit denen in einer Organisation Informationssicherheit hergestellt wird.

Im Laufe der Jahre haben sich ISMS-Frameworks entlang des üblichen und gewohnten hierarchisch-analytischen Vorgehens bei der Bewältigung umfangreicher und komplizierter Probleme entwickelt.

**Abb. 1: Hierarchisch-analytisches Vorgehen**

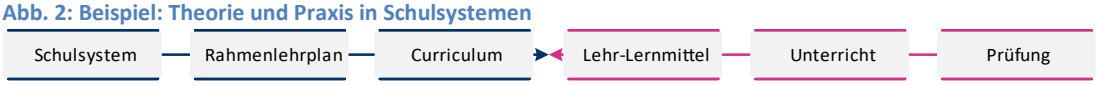



Das hierarchisch-analytische Vorgehen kennen wir aus allen Lebensbereichen. Nehmen wir das Schulsystem als Beispiel:
Das Schulsystem setzt eine bestimmte Vorstellung davon um, wie man die nachwachsende Generation mit den notwendigen Fähigkeiten und Fertigkeiten für z.B. ein erfolgreiches Leben ausstatten kann. Die Vorstellungen werden in den verschiedenen Kultusministerien als dokumentierte und gelebte Vorgehensweisen entwickelt. Das Ministerium gibt einen Rahmenlehrplan (Grobziele) vor. Aus dem Rahmenlehrplan entstehen Curricula (Feinziele), die in Schulen mit Lehr- und Lernmitteln (Ressourcen) im Unterricht vermittelt werden (Umsetzung) und der Erfolg des Systems am Ende mit Prüfungen getestet wird und auch zertifiziert (Zeugnis).

Abb. 2 zeigt das generelle Problem, das mit dieser Strategie verbunden ist: Die Planung funktioniert nur, wenn die Ressourcen für die Umsetzung zur richtigen Zeit in der richtigen Art

und Weise vorhanden sind. Ohne gute Schulgebäude in denen gute Lehrer mit guter Ausstattung an Lehr- und Lernmitteln auf interessierte Schüler treffen wird es schwer mit dem Unterricht. Am Ende wird gemessen und die von den Schülern im nationalen und internationalen Vergleich erzielten Prüfungsleistungen sagen, wie gut die Pläne in der Praxis umgesetzt werden konnten.

**Abb. 2: Beispiel: Theorie und Praxis in Schulsystemen**




Im Umgang mit ISMS-Frameworks zeigt sich ein ähnliches Dilemma: ISMS-Frameworks wie BSI IT-Grundschutz oder ISO 27001 sind umfangreich und geben für alle Funktionsbereiche der Informationstechnik vor, was man tun muss und was man lassen sollte, will man bei Technik, Organisation und Nutzung auf der sicheren Seite sein.

Sicherheitsverantwortlichen – den Lehrern der Informationssicherheit, wenn man im Bild bleibt – erscheinen die enzyklopädisch umfangreichen ISMS-Frameworks allerdings oft eher wie eine Bremse und nicht wie ein Gaspedal für „echte Informationssicherheit“. Die „großen“ ISMS-Frameworks enthalten Regelungen für alles, was in einem Netzwerk bei Technik, Menschen und Prozessen gesichert werden kann und muss. Für die meisten Organisationen treffen nicht alle Regelungen zu, schon deshalb, weil die zu regelnden Komponenten gar nicht vorhanden sind. Die erste Begegnung vermittelt oft den Eindruck des „viel zu viel“ und die Ahnung, schon für die Auswahl der für die Organisation relevanten Regelungen einen Berater zu brauchen.

Bedenken gegenüber ISMS-Frameworks sagen oft, dass Aufbau und Betrieb eines ISMS so viel Dokumentation erfordert, dass für die eigentliche Sicherheitsarbeit keine Ressourcen mehr zur Verfügung stehen. Das ohnehin überlastete Personal ist so sehr mit dem Schreiben beschäftigt, dass keine Zeit mehr bleibt, die notwendigen Sicherheitsmaßnahmen in der Praxis umzusetzen.

Theorie vs. Praxis

Bei der Frage nach den Ressourcen mit denen die in den ISMS-Frameworks niedergelegte Planung umgesetzt werden kann, treffen Theorie und Praxis aufeinander. Das ISMS-Framework möchte das Problem Informationssicherheit allumfassend in den Griff bekommen und lösen, die ISMS-Praxis möchte ein Problem der Informationssicherheit vor Ort dann lösen, wenn es nötig ist.

Genau an dem Punkt an dem die Regeln in Konfigurationen umgesetzt werden sollen, beginnen die Probleme zwischen Theorie und Praxis. Die in ISMS-Frameworks dokumentierten Regeln für Informationssicherheit können nur mit geeigneten Ressourcen in ein ISMS umgesetzt werden, welches in der Organisation gelebt wird. Für die informationssichere Konfiguration von Technik, Menschen und Prozessen braucht man Zeit, Geld, Fähigkeiten und Fertigkeiten und von all dem haben Sicherheitsverantwortliche nur in sehr großen Organisationen genug und manchmal nicht einmal dort.

Der idealtypische Planer eines ISMS-Frameworks stellt sich vor, dass die vorgegebenen Regelungen („controls“ im englischen Sprachgebrauch) alle abgearbeitet werden, dass genau dokumentiert wird, wie die Regeln in die Praxis umgesetzt wurden und am Ende die Umsetzung mit einem Zertifikat bestätigt werden kann.

Der idealtypische Praktiker möchte aber lieber die jetzt und vorhersehbar dringenden Sicherheitsprobleme seiner Konfiguration in den Griff bekommen, so wenig Zeit wie nur möglich

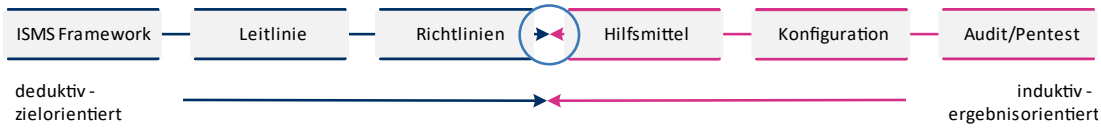
mit Dokumentation verbringen und ein Zertifikat ist für ihn nur dann wichtig, wenn es verlangt wird. Das sind sehr unterschiedliche Perspektiven und Herangehensweisen.

SiKoSH – Brücke zwischen Theorie und Praxis

SiKoSH kennt die Problematik und wählt aus den Bausteinen und Regeln des BSI IT-Grundschutz nur die aus, die vom IT-Grundschutz-Profil "Basis-Absicherung Kommunalverwaltung" vorgeschlagen werden. Dadurch wird das ISMS-Framework deutlich schlanker und SiKoSH baut mit seinen Hilfsmitteln die von Sicherheitspraktikern gewünschte Brücke zwischen Theorie und Praxis, zwischen Plan und Umsetzung. Das lässt die Aufgabe „ISMS" für kommunale Praktiker besser machbar erscheinen.

SiKoSH unterstützt die Umsetzung des ISMS selbst durch viele Hilfsmittel – von denen manche nur ausgefüllt werden müssen, um die Dokumentationsanforderungen eines ISMS zu erfüllen.

**Abb. 3: ISMS-Komponenten**




SiKoSH wurde mit dem Fokus auf kommunale Sicherheitsanforderungen für den Praktiker entwickelt und versetzt Anwender in die Lage, im **Do-it-Yourself-Verfahren** ein **ISMS** auf die Beine zu stellen, auf Dauer zu betreiben, stetig zu verbessern und einer sich ständig verändernden Sicherheitslage anzupassen.

Do-it-Yourself-ISMS

**Do-it-Yourself** bedeutet:

- man ist nicht auf teure Berater angewiesen.
- es gibt Hilfsmittel für die Umsetzung und
- es gibt unterstützende Personen aus der Community, die SiKoSH-Anwendern mit Rat und Tat zur Seite stehen.

## 2.2 Vorteile von SiKoSH

SiKoSH hat im Vergleich zu anderen Vorgehensmodellen diese Vorteile:

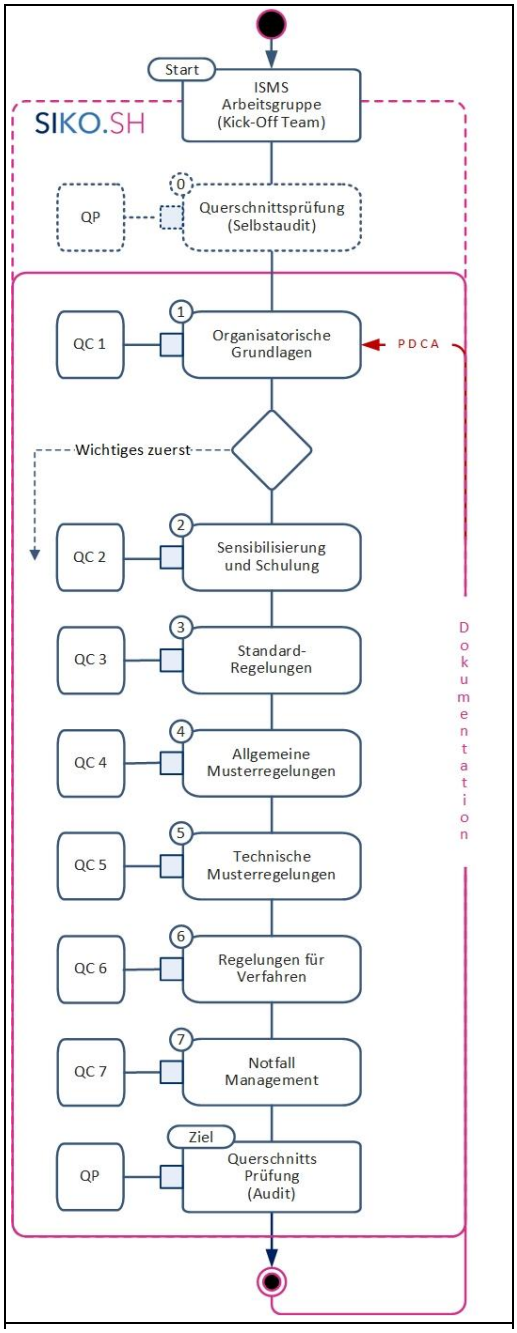
- SiKoSH wurde mit Blick auf Anforderungen und Gegebenheiten kommunaler Einrichtungen entwickelt.
- SiKoSH ist als Einstiegsframework leicht zu handhaben und mit **geringerem Ressourcenaufwand** umsetzbar.
- SiKoSH ergänzt andere etablierte ISMS-Frameworks - wie z.B. BSI IT-Grundschutz, ISO/IEC 27001 - gewährleistet einen **einfachen Einstieg** in das Management von Informationssicherheit und Datenschutz, der **beliebig auf- und ausgebaut** werden kann.
- SiKoSH ist einer „Quick Win" – Philosophie verpflichtet, die es dem Anwender mit Phasenchecks erlaubt, **schnell und einfach** den aktuellen Stand der Informationssicherheit zu messen und nötige Sicherheitsmaßnahmen mit Hilfsmitteln, Mustervorlagen und Beispielen für „best practices" ebenso schnell wie einfach implementieren zu können.

# 3 Mit SiKoSH arbeiten

## 3.1 SiKoSH Aktivitätsdiagramm

SiKoSH fasst die Arbeiten bei Einführung und Betrieb eines ISMS in ***Phasen*** zusammen, die nach Maßgabe des PDCA-Zyklus regelmäßig oder bei aktuellem Anlass überbearbeitet werden. Das Aktivitätsdiagramm (Abb. 4: SiKoSH Aktivitätsdiagramm) zeigt den Ablauf des SiKoSH ISMS-Prozesses. Am Anfang der Einführung eines ISMS steht ***immer*** *die Bildung einer temporären Arbeitsgruppe (das „Kick-Off-Team)*, die den **Gesamtprozess** anstößt.

Abb. 4: SiKoSH Aktivitätsdiagramm




Das ISMS-Kick-Off Team beginnt mit einem Selbstaudit

Die **temporäre Arbeitsgruppe beginnt im ersten Schritt** mit einer Querschnittsprüfung, die als **Selbstaudit** das aktuelle Niveau der Informationssicherheit der Einrichtung einschätzt. Die Querschnittsprüfung ist ein Quickcheck, der die zentralen Prüfpunkte aller Quickchecks zusammenfasst.

Die Ergebnisse werden evaluiert und der SiKoSH-Prozess beginnt. Werden alle Phasen durchlaufen und alle Quickchecks präzise angewandt, dient die Querschnittsprüfung nur noch der Gesamtschau des jeweils erreichten Status quo.

In den **sieben Phasen der konkreten ISMS-Arbeit** stellt SiKoSH mit seinen Hilfsmitteln Prüfpunkte und Orientierungen bereit, die auch Nicht-Spezialisten in die Lage versetzen, wichtige Maßnahmen zur Etablierung eines ständigen Verbesserungsprozesses der Informationssicherheit zu implementieren.

Jede SiKoSH-Phase beginnt mit einem Quickcheck

Jede Phase besteht aus **mehreren Zwischenschritten** und wird durch einen **Quickcheck** eingeleitet**.** Nach der Bearbeitung aller SiKoSH-Phasenchecks, nach der Umsetzung noch nicht implementierter Prüfpunkte, nach der Anpassung und Verabschiedung fehlender Hilfsmittel in einer Organisation sowie der anschließenden Dokumentation eines Sicherheitskonzepts (siehe Kap. 12 auf Seite 44) ist eine solide Grundlage für den weiteren Ausbau eines ISMS in einer Organisation geschaffen.

Das Wichtigste wird zuerst erledigt

**In der praktischen Anwendung** kommt es üblicherweise vor allem in der Anfangsphase des Aufbaus eines ISMS zu Abweichungen von der sequentiellen Abarbeitung der SiKoSH Phasen: Es werden die Phasen priorisiert, in denen nach dem Ergebnis der Querschnittsprüfung – des

Selbst-Audits (Quickcheck) – die wichtigsten Maßnahmen auf dem Weg Informationssicherheit der Einrichtung ergriffen werden können und müssen.

Selbstaudit – Lagebild mit der Querschnittsprüfung

Der *Selbstaudit* mit der *Querschnittsprüfung* am Anfang zeigt ein Bild der Gesamtlage und lässt eklatante Lücken und Versäumnisse im Schutzniveau erkennen: Wo brennt es bezüglich Informationssicherheit und Datenschutz aktuell am meisten?

In der Folge kann auf die einzelnen Phasen mit den jeweiligen Quickchecks direkt näher eingegangen werden und im Sinne einer *Phasen- und Bearbeitungs-Priorisierung* die dringendsten Probleme im Schutzniveau bearbeitet und beseitigt werden.

**Ist das ISMS in Betrieb genommen** und sind alle aktuellen und kritischen Sicherheitslücken behoben, sollten alle in den SiKoSH-Phasen zusammengefassten Sicherheitsvorgaben und Richtlinien geprüft und – wenn nötig – umgesetzt werden.

## 3.2 Regelmäßig wiederkehrende Aufgaben

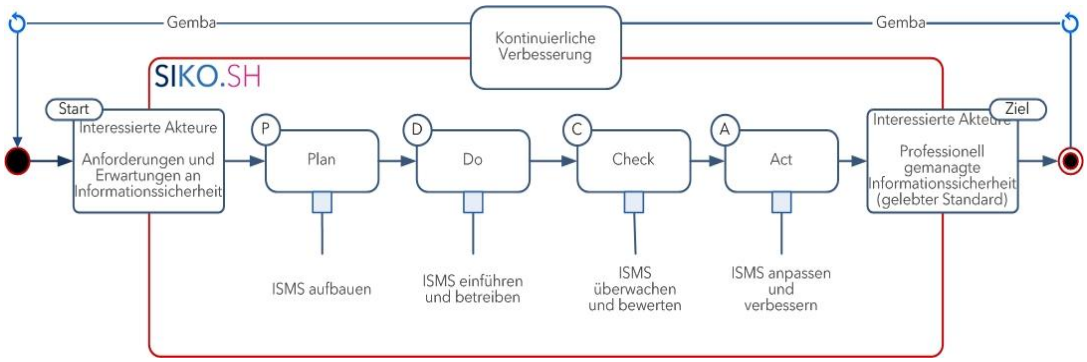
PDCA

Planung, Umsetzung, Überprüfung und Verbesserung der Informationssicherheit ist ein Prozess. Er hat das Ziel, Risiken für Informationssicherheit und Datenschutz auf ein akzeptables und beherrschbares Maß zu minimieren. Da sich Gefährdungslage, Informationstechnik, organisatorische Prozesse, Aufgaben der Organisation und Anzahl und Art der Mitarbeiter ändern, müssen Aufbau und Wirksamkeit des ISMS und seiner Komponenten überwacht und immer wieder an das aktuelle Sicherheitslagebild angepasst und verbessert werden. Für diesen kontinuierlichen Prozess der Verbesserung von Standards hat sich das PDCA-Modell bewährt, das in “Abb. 5: PDCA-Methode der Einführung und des Betriebs eines ISMS“ dargestellt ist.

PDCA – es gibt einen Anfang, aber kein Ende

Die PDCA-Methode geht auf einen in den 30er Jahren entwickelten Ansatz der Physiker Shewhart und Deming zum Qualitätsmanagement zurück und wurde im Wesentlichen in Japan im Rahmen des „lean manufacturing“ zur heutigen Form weiterentwickelt. PDCA ist praxisorientiert und „gemba“ – der „eigentliche Ort“ oder auch „Ort der Wertschöpfung“ ist ein integraler Bestandteil der Arbeitsphilosophie. Gemba in der Informationssicherheit heißt, dass im Falle von Problemen die ISBs direkt vor Ort aktiv werden sollten, um die Ursachen des Problems zu erkennen und zu verstehen. Gemba impliziert „management by walking around“ und ist in diesem Sinne nichts anderes als ein professionell durchgeführter Sicherheitsaudit.

**Abb. 5: PDCA-Methode der Einführung und des Betriebs eines ISMS**



Gemba

Die Grundidee ist, dass der Manager nur vor Ort sehen kann, ob und wie seine Vorgaben und Vorstellungen umgesetzt werden können, ob sie vor Ort in seinem Sinne interpretiert werden oder ob er vollkommen an der Realität der Umsetzbarkeit vorbeiplant.

## 3.3 Arbeiten mit den Quickchecks

Quickchecks sind der erste Schritt in jeder Phase von Einführung und Betrieb des ISMS und korrespondieren mit den jeweils zur Verfügung gestellten Hilfsmitteln.

Quickchecks sind wichtige Hilfsmittel bei der Einführung und dem Betrieb von SiKoSH. Jeder SiKoSH Phase geht ein Quickcheck voraus, der den schon erreichten Stand der Informationssicherheit der Behörde feststellt. Die Quickchecks beinhalten Prüffragen zu den kommunalen Basis-Anforderungen. Anhand einer vorgegebenen Gewichtung können mit dem Quickcheck relevante Fragen wie „Wo drückt der Schuh besonders?“ oder „Welche Quick Wins sind besonders effizient?“ beantwortet werden.

Quickchecks sind Kalkulationstabellen mit Auswahlmenüs zur Dokumentation des Umsetzungsstands kommunaler Basis-Anforderungen. In vorherigen SiKoSH Versionen wurden dafür separate Tabellen je Phase bereitgestellt. Mit der Version 3.0.0 sind die Tabelleninhalte in das Dokument „SiKoSH ISMS-Übersicht“ zusammengeführt. Dies hat den Vorteil, dass Inhalte des Dokumentes automatisch ausgewertet, in Verbindung gebracht und für den Management-Bericht dargestellt werden können.

Das Tabellenblatt „Quickchecks“ beinhaltet nun alle Anforderungen, kann aber über die Spalte „Phase“ nur die für die aktuellen Phasenbearbeitung relevante Anforderungen anzeigen lassen (Nutzung der Filter-Funktion).

Eine Sonderrolle spielt der Quickcheck im Tabellenblatt „Querschnittsprüfung“. Er enthält zusammenfassende Prüffragen über alle Phasen-Quickchecks. Mit der Querschnittsprüfung bekommt die SiKoSH-Anwenderin bzw. der SiKoSH-Anwender einen soliden Überblick über den Stand der Informationssicherheit ihrer oder seiner Einrichtung.

## 3.4 Tabellen „Übersicht Dokumente“ zu den SiKoSH Phasen

SiKoSH hilft dabei die kommunale Basis-Absicherung nach Maßgabe des „IT-Grundschutz-Profil: Basis-Absicherung Kommunalverwaltung“[16] umzusetzen. Die SiKoSH-Dokumente werden dabei kontinuierlich fortgeschrieben.

Das bedeutet aber auch, dass SiKoSH sich regelmäßig und auch ad-hoc von schon veröffentlichten Dokumenten verabschieden muss, wenn sie ganz oder teilweise auf Bausteinen beruhen, die sich in den jeweiligen Versionen der IT-Grundschutz-Methodik oder im IT-Grundschutz-Profil: Basis-Absicherung-Kommunalverwaltung geändert haben.

Die jeweils aktualisierten Dokumente sind im SiKoSH-Leitfaden bei blauen [↓. xslx] Hyperlinks hinterlegt, wie hier in „SiKoSH Phase 1 – Übersicht Beispiel-Dokumente“.

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

SiKoSH Phase 1 – Ausschnitt von Dokumenten

| Titel des Dokuments – Beschreibung |
| --- |
| **Quickcheck Phase 1 – Informationssicherheit und Organisation,**<br>**enthalten in „SiKoSH ISMS-Übersicht“** [↓.xslx]<br>In der SiKoSH ISMS-Übersicht befinden sich u.a. die Quickchecks aller sieben Phasen.<br>Der Quickcheck der Phase 1 behandelt die kommunalen Basis-Anforderungen der BSI-Bausteine ISMS.1 (Sicherheitsmanagement), ORP.1 (Organisation), ORP.4 (Identitäts- und Berechtigungsmanagement) und ORP.5 (Compliance Management). |
| **Hilfsmittel „Informationssicherheit für Behördenleitungen“** [↓.pdf \| .docx ]<br>Eine einseitige Zusammenfassung (Onepager), der kurz und knapp die Ziele der Informationssicherheit und des Datenschutzes beschreibt. |

Ist ein Dokument noch nicht auf die gerade gültige Hauptversion des Leitfadens aktualisiert, kann einstweilen die Vorversion verwendet werden. In diesem Fall ist der Hyperlink in der entsprechenden Tabelle „Übersicht Dokumente“ inaktiv und grau [↓.xlsx ] wie hier in „Virtualisierung“ der Phase 5.

SiKoSH Phase 5 – Ausschnitt von Dokumenten

| Titel des Dokuments – Beschreibung |
| --- |
| **„Virtualisierung“** [↓.pdf \| .docx ]<br>Diese Richtlinie regelt die Voraussetzungen für den Betrieb von Virtualisierungsumgebungen in der anwendenden Behörde. |

# 4 SiKoSH Phase 1: Sicherheitsmanagement und Organisation

## 4.1 Umsetzung Phase 1

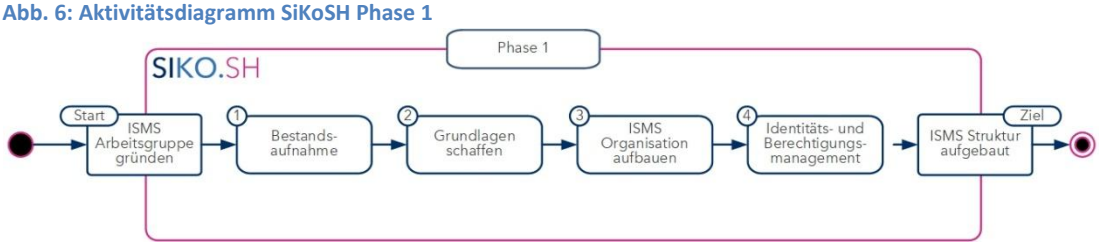
→Aktivitätsdiagramm

Die im SiKoSH-Leitfaden vorgeschlagene Reihenfolge der Umsetzung kann geändert werden, wenn es für die Implementierung des ISMS unter den Bedingungen einer bestimmten Organisation zielführend ist. Da die Phase 1 aber die Aufbau- und Ablauforganisation des ISMS grundlegend regelt, sollte hiermit gestartet werden.

In der SiKoSH Phase 1 werden folgende BSI-Bausteine angewendet:

- ISMS.1 Sicherheitsmanagement
- ORP.1 Organisation
- ORP.4 Identitäts- und Berechtigungsmanagement
- ORP.5 Anforderungsmanagement (Compliance Management)

Abb. 6: Aktivitätsdiagramm SiKoSH Phase 1




## 4.2 Start: ISMS-Arbeitsgruppe gründen

Start mit dem Kick-Off Team

Sofern es innerhalb der Organisation noch keine Aufbau- und Ablauforganisation für die Herstellung und Aufrechterhaltung der Informationssicherheit gibt, wird im ersten Schritt („Start“) durch die **temporäre Arbeitsgruppe** (das „Kick-Off-Team“, das den Gesamtprozess anstößt) eine **ISMS**-Arbeitsgruppe zur Schaffung der nötigen Voraussetzungen für den Aufbau und Betrieb eines ISMS eingerichtet.

Mitglieder der **ISMS**-Arbeitsgruppe sind idealerweise:

- Organisationsleitung, Behördenleitung,
- IT-Verantwortliche (IT-Leitung),
- Datenschutzbeauftragte (bDSB) und ggf.
- Designierte bzw. designierter ISB
- weitere Rollenträger wie z.B. Personalrat, Leiter Gebäudemanagement etc.

Die Aufgabe der **ISMS-Arbeitsgruppe** ist die Bearbeitung der SiKoSH Phase 1. Hier werden die organisatorischen Grundlagen eingerichtet und eine erste Bestandsaufnahme „Informationssicherheit“ gemacht.

## 4.3 Bestandsaufnahme Sicherheitsmanagement und Organisation

Querschnittsprüfung

Um einen schnellen Überblick über alle SiKoSH-Phasen gewinnen zu können und zu sehen, wo es im Gesamtsicherheitsprozess besonders schwierig ist bzw. wo Quick Wins realisierbar sind, empfiehlt sich an dieser Stelle die Durchführung des Quickchecks „Querschnittsprüfung“. Erst wenn die Umsetzung der SiKoSH-Phase mit den jeweiligen Quickchecks, frei nach dem Pareto-Prinzip, mindestens 80% abgeschlossen ist, sollte mit der Umsetzung der nächsten SiKoSH-Phase begonnen werden. Die Bearbeitung der restlichen 20% sollten nach Abschluss der anderen Phasen wieder aufgenommen werden.

## 4.4 Grundlagen schaffen

### 4.4.1 Unterstützung der Leitungsebene sichern

Informationssicherheit für die Behördenleitung

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

### 4.4.2 Informationssicherheitsleitlinie erstellen und in Kraft setzen

Informationssicherheitsleitlinie

Die Informationssicherheitsleitlinie (ISLL) schafft die Grundlage für den Aufbau eines ISMS, das die Herstellung und den Erhalt des erforderlichen Sicherheitsniveaus aller Objekte und Daten im Verantwortungsbereich der Organisation sicherstellt. Die ISLL beschreibt Aufbauorganisation, Ablauforganisation (Prozesse), einschlägige Regelwerke und Gesetze, die die Planung, Umsetzung und Überprüfung von Sicherheitsmaßnahmen im Geltungsbereich gewährleisten. Das ISMS unterstützt die Leitung der Organisation dabei ihrer gesetzlichen Verantwortung für die Informationssicherheit gerecht zu werden.

Aufgabe der temporären Arbeitsgruppe ist hierbei die Erstellung eines Entwurfs einer ISLL, die zunächst insbesondere die Themen

- Verantwortung der Behördenleitung
- Sicherheitsstrategie
- Bereitstellung von Ressourcen inkl. Bestellung eines ISB

adressiert. Die Finalisierung kann dann durch den später bestellten ISB oder die später bestellte ISB erfolgen.

Anpassen der Informationssicherheitsleitlinie

Grundsätzlich ist die Musterleitlinie allgemein gültig, unabhängig von der Größenklasse der Organisation. Bei Passagen, bei denen textuelle Anpassungen erforderlich sind, gibt es einen entsprechenden Hinweis. Im Anhang des Regelungsmusters gibt es zahlreiche Bearbeitungshinweise.

Anpassen von SiKoSH Vorlagen

Das Anpassen der Informationssicherheits-Musterleitlinie (ISLL) oder einer anderen SiKoSH-Vorlage beeinträchtigen die Qualität des ISMS nicht. Im Gegenteil, Änderungen und Anpassungen sind der Normalfall. Eine Informationssicherheitsleitlinie sollte immer individuell für die anwendende Behörde angepasst sein. Die ISLL ist das „Herzstück“ aller Regelwerke des ISMS und funktioniert am besten, wenn sie exakt zur Organisation mit allen ihren individuellen Merkmalen passt.

### 4.4.3 Informationssicherheitsbeauftragten benennen und qualifizieren

Bestellung einer oder eines ISB (siehe Hilfsmittel Bestellung des oder der Informationssicherheitsbeauftragten)

Die Bestellung eines Informationssicherheitsbeauftragten (ISB) ist eine unverzichtbare Basismaßnahme bei der Einführung eines ISMS. Der ISB ist der **zentrale Ansprechpartner** für alle Fragen rund um die Informationssicherheit. Er ist für den weiteren Aufbau und Betrieb des ISMS verantwortlich, für die Pflege des Sicherheitskonzeptes und oft auch für die Notfalldokumentation.

## 4.5 Organisationsstruktur aufbauen

### 4.5.1 Aufbauorganisation

ISMS-Organisation

Ein ISMS braucht – wie jedes Managementsystem – klare Verantwortlichkeiten. Die Richtlinie „ISMS“ beschreibt die Organisationstruktur, die Rollenträger und die Kernprozesse im Informationssicherheitsmanagement (ISM) und deren Zusammenwirken mit anderen Prozessen der Verwaltung. Die Richtlinie ist die zentrale Regelung für das Sicherheitsmanagement selbst, da sie die formalen Grundlagen für Aufbau, Ausbau und Verankerung der Informationssicherheit festlegt.

Neben der Rolle „ISB“ sind insbesondere auch diese Rollen für das Funktionieren eines ISMS unerlässlich (definiert über die ISLL):

- Die Behördenleitung hat die sogenannte organisationsschuldnerische Verantwortung für das rechtskonforme Verwaltungshandeln, inklusive Informationssicherheit und Datenschutz.
- IT-Verantwortliche und Fachverfahrensverantwortliche setzen die Regelungen für Informationssicherheit und Datenschutz um.
- Die Aufgabe aller Mitarbeiterinnen und Mitarbeiter ist es das ISMS mit Leben zu füllen und eine sichere Organisationskultur zu etablieren. In diesem Sinne ist auch und vor allem die Personalabteilung der Organisation in der Pflicht.
- Der IT-Verantwortliche (IT-Leiter) verantwortet einen ordnungsgemäßen IT-Betrieb.
- Zur Reduzierung von Risiken wie z. B. der Haftung wegen grober Fahrlässigkeit werden verschiedene Rollen in diesen Bereichen besetzt
    - Informationssicherheitsmanagement (ISM)
    - IT-Notfallmanagement (Business Continuity Management – BCM)
    - Datenschutzmanagement (DSM)
    - Compliance Management

### 4.5.2 Ablauforganisation

RL ISMS

Die Richtlinie „ISMS“ beschreibt typische Aufgaben des ISMS wie anstehende Maßnahmen, die Definition von Ausnahmen und die Listung von Sicherheitsvorfällen und sicherheitsrelevanter Rechtsnormen (Compliance Management). Es werden Musterlisten zur Erfassung bereitgestellt.

Zudem wird der Prozess der Steuerung und Verwaltung von Dokumenten innerhalb der Behörde beschrieben. Dies umfasst die Erstellung, Aufbewahrung, Überprüfung, Versionierung, Freigabe, Archivierung und Vernichtung von Dokumenten, sodass der gesamte Lebenszyklus der Dokumente mit allen Revisionen lückenlos nachvollziehbar ist.

Weitere Regelungen zur Dokumentenlenkung finden sich auch im SiKoSH-Styleguide und in der Richtlinie ISMS.

SiKoSH Styleguide
RL ISMS

## 4.6 Identitäts- und Berechtigungsmanagement

Die Richtlinie „Identitäts- und Berechtigungsmanagement“ regelt den Zugang zu den schützenswerten Ressourcen der Behörde gemäß BSI-Baustein ORP.4.

Identitäts- und Berechtigungsmanagement

## 4.7 Ziel SiKoSH Phase 1: Grundlegende ISMS-Struktur aufgebaut

Nach dem Abschluss der SiKoSH Phase 1

- ist die Organisationsstruktur aufgebaut,
- ist der Informationssicherheitsbeauftragte (ISB) benannt,
- ist die Informationssicherheitsleitlinie (ISLL) verabschiedet,
- sind die notwendigen Rollen im Informationssicherheitsmanagement der Organisation benannt und die Rollenträger auf die Wahrnehmung ihrer Aufgaben verpflichtet,
- sind die Zugänge zu schützenswerten Ressourcen abgesichert.

Aus den **folgenden sechs Phasen der Einführung eines ISMS** empfiehlt es sich zunächst, die SiKoSH-Phase 2 „Personal, Sensibilisierung und Schulung“ umzusetzen. Da alle Regelungen nur dann wirksam sind, wenn sie auch verstanden und umgesetzt werden, kümmert sich diese Phase insbesondere um eine rollenbezogene Sensibilisierung und Schulung aller am Informationssicherheitsprozess beteiligten Personen. Ein sicheres Verhalten kann nur dann eingefordert werden, wenn die hierfür notwendigen Fähigkeiten und Fertigkeiten geschult und trainiert werden.

Mitarbeiter sind der Schlüssel zur Informationssicherheit

## 4.8 Übersicht: Dokumente zur SiKoSH Phase 1

Tabelle 2 zeigt die wichtigsten Dokumente der SiKoSH Phase 1. Registrierte SiKoSH-Anwender laden SiKoSH Dokumente mit einem Klick auf die entsprechende Formatanzeige in der Tabelle (.pdf, .docx, .dotx, .xlsx) zur weiteren Verwendung herunter.

**Tabelle 2: SiKoSH Phase 1 – Übersicht Dokumente**

→Aktivitätsdiagramm

| Titel des Dokuments – Beschreibung |
|---|
| **Quickcheck Phase 1 – Informationssicherheit und Organisation,**<br>**enthalten in „SiKoSH ISMS-Übersicht“** [↓.xslx]<br>Der Quickcheck der Phase 1 behandelt die kommunalen Basisanforderungen der BSI-Bausteine ISMS.1 (Sicherheitsmanagement), ORP.1 (Organisation), ORP.4 (Identitäts- und Berechtigungsmanagement) und ORP.5 (Compliance Management). |
| **Hilfsmittel „Informationssicherheit für Behördenleitungen“** [↓.docx]<br>Ein Onepager, der kurz und knapp die Ziele der Informationssicherheit und des Datenschutzes beschreibt. |
| **Leitlinie „Informationssicherheitsleitlinie“** [↓.docx ]<br>Muster einer Informationssicherheitsleitlinie zur individuellen Anpassung an die Bedürfnisse der Behörde. |

| Titel des Dokuments – Beschreibung |
| --- |
| **Hilfsmittel „Bestellung des/der Informationssicherheitsbeauftragten“** [↓.docx ]<br>Formular zur ISB-Bestellung |
| **Richtlinie „ISMS“** [↓.docx ]<br>Vorgaben, Best Practice und Muster für den Betrieb eines ISMS<br>Anlage 3: Maßnahmenliste [↓.xslx]<br>Anlage 4: Sicherheitsvorfallliste [↓.xslx]<br>Anlage 5: Risikoliste [↓.xslx]<br>Anlage 6: Ausnahmeliste [↓.xslx] |
| **Richtlinie „Identitäts- und Berechtigungsmanagement“** [↓.docx ]<br>Diese Richtlinie regelt den Zugriff auf schützenswerte Ressourcen einer Behörde. |
| **Hilfsmittel „Melden von Sicherheits- und Datenschutz-Vorfällen“** [↓ .docx]<br>Ein Merkblatt zum Aushang |
| **„QC QP – Querschnittsprüfung“,**<br>**enthalten in „SiKoSH ISMS-Übersicht“** [↓.xslx]<br>Der Quickcheck Querschnittsprüfung besteht aus einer initialen Selbsteinschätzung und enthält zusammenfassende Prüfpunkte der Quickchecks der 7 SiKoSH-Phasen. Er zeigt somit auf, wo vordringlich noch nachgebessert werden muss (siehe Kap. 11 - SiKoSH Ziel - Querschnittsprüfung). Die Querschnittsprüfung dient außerdem dem späteren Vergleich mit der tatsächlichen Umsetzungsquote, siehe abschließende Querschnittsprüfung, Kapitel 11. |
| **Hilfsmittel „Beispielprozesse“** [↓.pptx \|.pdf]<br>Modellierte Beispielprozesse |
| **Community Dokumente [ Link ]**<br>In diesem Ordner sind weitere Hilfsmittel aus der SiKoSH Community zu finden. Diese dürfen genutzt, angepasst oder als Inspiration für eigene Umsetzungen verwendet werden. |

# 5 SiKoSH Phase 2: Personal, Sensibilisierung und Schulung

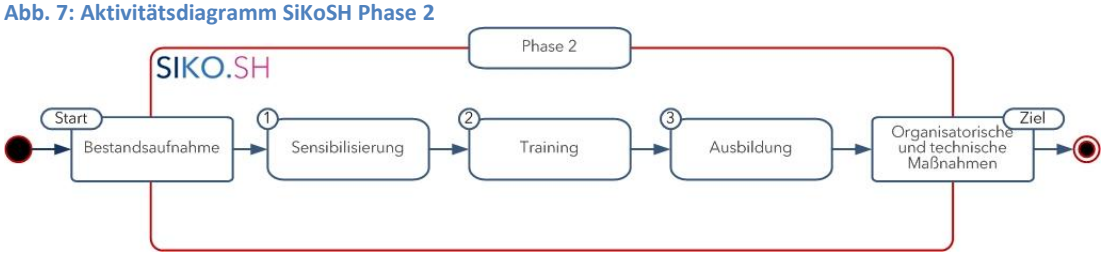
Die Regelungen eines ISMS sind nur wirksam, wenn sie den Benutzern der IT-Umgebung bekannt sind und die Nutzer die entsprechenden Verhaltensweisen zeigen, immer und auch unter schwierigen Bedingungen. Benutzer und Betreiber von IT-Geräten müssen deshalb ausreichend und regelmäßig geschult und trainiert werden.

→Aktivitätsdiagramm

In der SiKoSH Phase 2 werden folgende BSI-Grundschutz-Bausteine angewendet:

- ORP.2 Personal
- ORP.3 Sensibilisierung und Schulung zur Informationssicherheit

Abb. 7: Aktivitätsdiagramm SiKoSH Phase 2




## 5.1 Bestandsaufnahme Personal, Sensibilisierung und Schulung

Die Phase beginnt mit der Bearbeitung des Quickchecks der Phase 2 „Personal, Sensibilisierung und Schulung“ in der SiKoSH ISMS-Übersicht. Nachdem der aktuelle Umsetzungsstand festgestellt ist, sollten alle Prüfpunkte entsprechend Bearbeitungsstatus und Priorität abgearbeitet werden.

Quickcheck Phase 2

Für nicht vollständig erfüllte Prüfpunkte sollten, Maßnahmen eingeleitet werden, die zur Erfüllung des Prüfpunktes im geforderten Maße führen. Die Umsetzung der Anforderungen wird durch die SiKoSH-Hilfsmittel erleichtert.

## 5.2 Sensibilisierung planen und starten

Die tägliche Praxis zeigt immer wieder, dass Sicherheitsbedrohungen nicht ausschließlich technisch abgefedert werden können. Im Gegenteil, fast alle Angriffe auf die IT-Infrastruktur brauchen die (unfreiwillige) Mitarbeit von Menschen für den Erfolg (bestes Beispiel sind Schadprogramme wie z. B. Locky oder Emotet).

Mitarbeitende kommen aus der Regelschule grundsätzlich ohne nennenswerte Befähigung, für das Erkennen und Bewältigen von Gefahrsituationen im Umgang mit vernetzten digitalen Geräten. Die Vermittlung solcher Fähigkeiten stellt somit eine wesentliche Aufgabe der beruflichen Weiterbildung dar.

Wissen reicht nicht

Das ist aus den folgenden Gründen aber eine besondere Herausforderung, denn

1. Informationssicherheit ist ein abstraktes Konzept, das nur schwer gelernt werden kann.
2. Oft besteht der Eindruck, dass Informationssicherheit doch eine Aufgabe der IT sei und die Technik es schon richten wird.

3. Sicherheit kommt an zweiter Stelle. Die Erledigung von Arbeitsaufgaben (oft unter Zeitdruck) hat Vorrang, oft werden Sicherheitsvorgaben und Sicherheitserwägungen als störend wahrgenommen.
4. Die Entscheidung des individuellen Mitarbeiters für Sicherheit hat kein sichtbares Ergebnis und es gibt keine sichtbare Bedrohung.
5. Die Belohnung für sicheres Verhalten ist, dass die Wahrscheinlichkeit, dass etwas Schlimmes geschieht, weniger groß ist.
6. Wenn aber etwas Schlimmes geschieht, dann kann das tage-, wochen- oder monatelang von der falschen Entscheidung entfernt sein.

Bevor also Schulungsmaßnahmen umgesetzt werden, ist es erforderlich die Aufmerksamkeit der Mitarbeiter für das Thema Informationssicherheit zu gewinnen, Interesse für die selbständige Beschäftigung mit dem Thema Sicherheit zu wecken und (intrinsische) Motivation zu erzeugen, das in den Schulungs- und Trainingsmaßnahmen gewonnene Wissen, die erworbenen Fähigkeiten und Fertigkeiten im Arbeitsalltag dann auch umzusetzen.

Hieraus folgt, dass erfolgreiche **Schulungsmaßnahmen** erfolgreiche **Sensibilisierungsmaßnahmen** voraussetzen.

Bei der Umsetzung der Schulungsmaßnahmen ist zu beachten, dass es hier in der Regel nicht reicht, die Kenntnisse im Bereich Schadensmöglichkeiten, Schadvektoren und Verhalten zu erweitern. Die Mitarbeitenden müssen ihr persönliches Verhalten anpassen wollen, über die entsprechenden Fähigkeiten und Fertigkeiten verfügen, um ihr persönliches Verhalten anpassen zu können und imstande sein, im speziellen Kontext ihrer Aufgaben und ihres Umfelds die Fähigkeiten und Fertigkeiten auch aktivieren zu können.

Bei der Durchführung von Sensibilisierungskampagnen sollten insbesondere nachfolgende grundsätzliche Ratschläge beachtet werden:

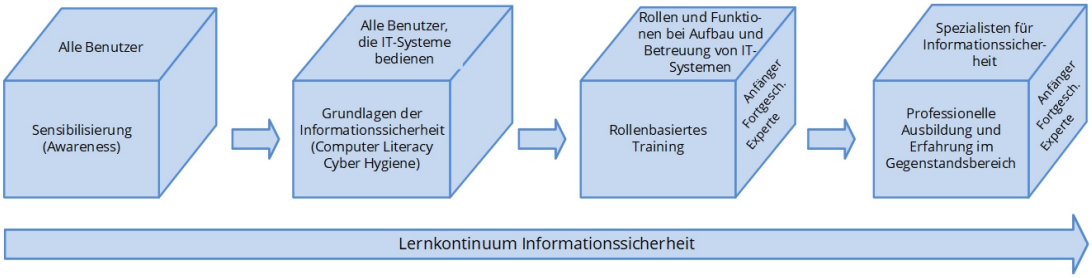
- **Mitarbeiter ermutigen**, Verdächtiges zu melden, ohne Angst vor Repressalien zu haben. Dies muss von den Vorgesetzten unterstützt und vorgelebt werden.
- Berücksichtigen, dass Mitarbeiter unter erhöhtem Arbeitsdruck schnell in **alte Verhaltensmuster** verfallen und dann eine erhöhte Risikobereitschaft aufweisen, um Arbeit vom Tisch zu bekommen. Wo immer möglich, sollte bereits in der Aufgabenstellung deutlich gemacht werden, dass die Sicherheitsthemen zur Aufgabenerledigung dazugehören.
- **Sensibilisierung** der Mitarbeiter ist eine **Aktivität**, die immer wieder **wiederholt** werden muss, die Bedrohungslage ändert sich ja ständig. Mit Schulungen alleine ist es nicht getan, es muss vor allem eine Veränderung des Verhaltens der Mitarbeitenden erreicht werden. Das ist leichter, wenn das Thema Informationssicherheit in Anweisungen, Prozessen, Vorgehensweisen und bei den Arbeitsaufträgen der Mitarbeiter immer eingebunden ist. Im Folgenden werden weitere Hilfsmittel aufgeführt, welche die Umsetzung von Maßnahmen zu den im Quickcheck 2: „Personal, Sensibilisierung und Schulung“ definierten Prüfpunkten erleichtern.

## 5.3 Informationssicherheit lernen

Schulung und Training Informationssicherheit und Datenschutz

Das National Institute of Standards and Technology NIST stellt fest, dass das Lernen von Informationssicherheit ein Kontinuum ist, das mit der Sensibilisierung für das Thema beginnt (Awareness), dann durch Training relevante Fähigkeiten und Fertigkeiten ausbildet und für definierte Personengruppen auch professionelle Ausbildung und Erfahrung im Gegenstandsbereich bedeutet.[17]

**Abb. 8: Lernkontinuum Informationssicherheit**




Sensibilisierung

Der Zweck von **Awareness**-Präsentationen besteht lediglich darin, die Aufmerksamkeit auf die Sicherheit zu lenken. Awareness-Präsentationen sollen Einzelpersonen in die Lage versetzen, IT-Sicherheitsprobleme zu erkennen und entsprechend zu reagieren

Training

**Training** zielt darauf ab, relevante und erforderliche Sicherheitsfähigkeiten und -kompetenzen zu vermitteln. Der wichtigste Unterschied zwischen Training und Sensibilisierung besteht darin, dass ein Training Fähigkeiten vermitteln soll, die es einer Person ermöglichen, eine bestimmte Funktion auszuführen, während bei der Sensibilisierung die Aufmerksamkeit einer Person auf ein Problem oder eine Reihe von Problemen gelenkt werden soll. Die im Training erworbenen Fähigkeiten bauen auf dem Fundament der Sensibilisierung auf, insbesondere auf den Grundlagen der Sicherheit und dem Material zur Vermittlung von Kenntnissen.[18]

Ausbildung

**Professionelle Ausbildung** integriert alle Sicherheitsfähigkeiten und -kompetenzen der verschiedenen funktionalen Spezialgebiete in einen gemeinsamen Wissensbestand und strebt danach, IT-Sicherheitsspezialisten und -fachleute hervorzubringen, die in der Lage sind, vorausschauend und proaktiv zu reagieren. Fachbezogene Aspekte zur Informationssicherheit sollten Teil jeder Ausbildung sein. Beispielsweise muss eine administrierende Person für die Sicherheitsaspekte seines oder ihres Systems ausgebildet werden. Ein zentralisiertes Knowhow auf wenige Spezialisten, wie den/die ISB, ist nicht umsetzbar. Jeder hat seinen Anteil an der Informationssicherheit zu leisten.

## 5.4 Sensibilisierung der Leitungsebene

Sensibilisierung Informationssicherheit und Datenschutz für die Leitungsebene in der öffentlichen Verwaltung

Klagen über zu geringe Motivation von Vorgesetzten und Top-Entscheidern, sich Fragen der Informationssicherheit zu widmen, gehören zur Folklore der Informationssicherheitsbeauftragten. Tatsächlich ist es so, dass die Geschäftsleitung den Fokus eher auf fachliche Themen

[17] NIST Special Publication 800-50, Building an Information Technology Security Awareness and Training Program

[18] Das Merkblatt „Melden von Sicherheits- und Datenschutzvorfällen“ aus Phase 1 erläutert, was ein Sicherheitsvorfall ist und wer bei der Feststellung oder dem Verdacht eines Sicherheitsvorfalls zu informieren ist

hat und das Ziel „Informationssicherheit und Datenschutz“ oft mit möglichst geringem Aufwand zu erreichen sucht.

Das hat betriebswirtschaftlich möglicherweise kurzfristig seinen Sinn, ist aber aus Sicht der Informationssicherheit und - im reuevollen Rückblick auf einen eingetretenen Sicherheitsvorfall - für die Behördenleitung gefährlich, die ja die Gesamtverantwortung trägt. In der Informationssicherheit zählt die Vorsorge und nicht die Reue.

## 5.5 Übersicht: Dokumente der SiKoSH Phase 2

Tabelle 3 zeigt die wichtigsten Dokumente der SiKoSH Phase 2. Registrierte SiKoSH-Anwender laden SiKoSH Dokumente mit einem Klick auf die entsprechende Formatanzeige in der Tabelle (.pdf, .docx, .dotx, .xlsx) zur weiteren Verwendung herunter.

→Aktivitätsdiagramm

**Tabelle 3: SiKoSH Phase 2 – Übersicht Dokumente**

| Titel des Dokuments – Beschreibung |
|---|
| **Quickcheck Phase 2 – Personal, Sensibilisierung und Schulung,**<br>**enthalten in „SiKoSH ISMS-Übersicht“** [↓.xslx]<br>Der Quickcheck der Phase 2 behandelt die kommunalen Basisanforderungen der BSI-Bausteine ORP.2 Personal und ORP.3 Sensibilisierung und Schulung zur Informationssicherheit. |
| **Richtlinie „Personal“**[↓.docx ]<br>Vorgaben, Best Practices und Muster für die Sensibilisierung und Schulung von Personal |
| **Konzept „Schulung und Sensibilisierung Informationssicherheit und Datenschutz“** [↓.docx ]<br>Grundlagen für den Aufbau einer Schulungs- und Trainingsumgebung |
| **Beispiel „Sensibilisierung Informationssicherheit und Datenschutz“** [↓.pdf ]<br>Grundlagen einer erfolgreichen Sensibilisierungskampagne am Beispiel der Landeshauptstadt Kiel |
| **Beispiel „Sensibilisierung Informationssicherheit und Datenschutz für die Leitungsebene in der öffentlichen Verwaltung“** [↓.pdf ]<br>Theoretische Grundlagen für die Behördenleitung und deren Umgang mit Informationssicherheit und Datenschutz |

# 6 SiKoSH Phase 3: Standardregelungen

## 6.1 Überblick

Aufgaben für Fachabteilungen

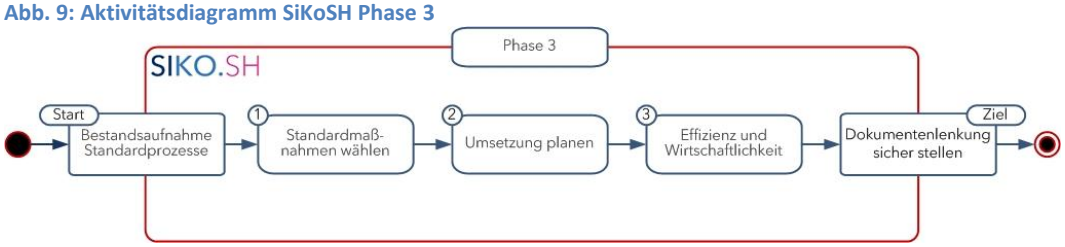
In der SiKoSH-Phase 3 werden zahlreiche Musterregelungen bereitgestellt, die wesentliche Aspekte des Sicherheitsmanagements aufgreifen. Die Verantwortung für die Ausarbeitung und Einführung dieser Regelungen liegt typischerweise nicht beim Informationssicherheitsbeauftragten (ISB), sondern in den jeweiligen Fach- oder Querschnittsabteilungen. Die Musterregelungen helfen dabei, typische sicherheitsbezogene Regelungsbedarfe zu verankern oder bereits vorhandene Regelungen auf Lücken zu prüfen und zu ergänzen.

In der SiKoSH Phase 3 werden folgende BSI-Grundschutz-Bausteine angewendet:

→Aktivitätsdiagramm

- CON.1 Kryptokonzept
- CON.2 Datenschutz
- CON.3 Datensicherungskonzept
- CON.9 Informationsaustausch
- OPS.1.1.1 Allgemeiner IT-Betrieb
- OPS.1.1.2 Ordnungsgemäße IT-Administration
- OPS.1.1.3 Patch- und Änderungsmanagement
- OPS.1.1.4 Schutz vor Schadprogrammen
- OPS.1.1.5 Protokollierung
- OPS.1.2.4 Telearbeit

Abb. 9: Aktivitätsdiagramm SiKoSH Phase 3




## 6.2 Übersicht: Dokumente der SiKoSH-Phase 3

→Aktivitätsdiagramm

Tabelle 4 zeigt die wichtigsten Dokumente der SiKoSH Phase 3. Registrierte SiKoSH-Anwender laden SiKoSH Dokumente mit einem Klick auf die entsprechende Formatanzeige in der Tabelle (.pdf, .docx, .dotx, .xlsx) zur weiteren Verwendung herunter.

Tabelle 4: SiKoSH Phase 3 – Übersicht Dokumente

| Titel des Dokuments – Beschreibung |
|---|
| **Quickcheck der Phase 3 – Standardregelungen,**<br>**enthalten in „SiKoSH ISMS-Übersicht“** [↓.xslx]<br>Der Quickcheck der Phase 3 behandelt ausgewählte Bausteine aus den Bereichen Konzeption und Vorgehensweisen. |

| Titel des Dokuments – Beschreibung |
| --- |
| **Richtlinie „Kryptografie“** [↓.docx]<br><br>Anforderungen zum Schutz von Vertraulichkeit, Integrität und Authentizität von Informationen. |
| **Konzept „Kryptografie“** [↓.docx]<br><br>Beschreibung der organisatorischen und technischen Umsetzung der kryptografischen Anforderungen. |
| **Hilfsmittel „Krypto-Inventar“** [↓.xslx]<br><br>Sämtliche veralteten Verfahren können hier mit ihrer Risikobewertung, ggf. Migrationsplanung und Verantwortlichkeit nachvollziehbar dokumentiert und regelmäßig kontrolliert werden. |
| **Richtlinie „Datenschutz“**<br><br>in Vorbereitung |
| **Konzept „Datenschutz“**<br><br>in Vorbereitung |
| **Richtlinie „Sicherer Informationsaustausch“** [↓.docx]<br><br>Für den sicheren Austausch dienstlicher Informationen müssen geeignete Kommunikations- und Austauschwege festgelegt und abhängig von Schutzbedarf, Empfängerkreis und Informationsart passende Schutzmaßnahmen berücksichtigt werden.<br><br>Die Richtlinie enthält die grundlegenden Regelungen für den sicheren Informationsaustausch und kann nach individueller Anpassung als verbindliche interne Regelung genutzt werden. |
| **Hilfsmittel „Sicherer Informationsaustausch“** [↓.docx]<br><br>Das ergänzende Hilfsmittel unterstützt dabei, die freigegebenen Kommunikations- und Austauschdienste sowie die zulässigen Übermittlungswege und erforderlichen Schutzmaßnahmen für unterschiedliche Informationsarten organisationsspezifisch festzulegen und für die Mitarbeitenden übersichtlich bereitzustellen. |
| **Richtlinie „Datensicherung“** [↓.docx]<br><br>Die Richtlinie legt die organisationsweit verbindlichen Mindestanforderungen an Datensicherung und Wiederherstellung fest. Sie behandelt unter anderem die Festlegung des Sicherungsbedarfs, Sicherungsverfahren und -intervalle, den Schutz und die Aufbewahrung von Sicherungskopien, Überwachung und Fehlerbehandlung, Wiederherstellungstests sowie extern erbrachte Sicherungsleistungen. |
| **Vorlage Datensicherungsplan** [↓.docx]<br><br>Mit der Vorlage können die Vorgaben der Richtlinie für ein konkretes IT-System oder eine sinnvoll gebildete Systemgruppe umgesetzt und dokumentiert werden. Erfasst werden insbesondere Sicherungsbedarf und Rahmenbedingungen, Sicherungsumfang und -verfahren, Aufbewahrung und Schutz der Sicherungskopien, Wiederherstellung, Zuständigkeiten und Wiederherstellungstests. Technische Details können weiterhin in Betriebshandbüchern, Runbooks oder anderen führenden Betriebsdokumentationen verbleiben und werden lediglich referenziert. |

| Titel des Dokuments – Beschreibung |
| --- |
| **Beispiel Datensicherungsplan** [↓.docx]<br>Das vollständig ausgefüllte Beispiel zeigt, wie die Vorlage in der Praxis genutzt werden kann. Als fachliche Ausgangsbasis dient die Referenzarchitektur des IT-Grundschutz-Profils „Basis-Absicherung Kommunalverwaltung“, Version 4.0. Herangezogen werden insbesondere die dort beschriebenen Objekte „Allgemeiner Server“, „Terminal-Server“, „Virtualisierungshosts“ und „Dateiablage“. Die konkrete Ausgestaltung der Musterkommune mit Systemnamen, Sicherungsintervallen, Aufbewahrungsdauern und weiteren Betriebswerten ist fiktiv und dient ausschließlich der Veranschaulichung. Das Beispiel ist zugleich mit dem SiKoSH-Beispiel IT-Betriebshandbuch abgestimmt und verdeutlicht die Abgrenzung zwischen Datensicherungsplan und technischer Betriebsdokumentation. |
| **Richtlinie „Sicherer IT-Betrieb und Administration“** [↓.docx]<br><br>Ein sicherer und verlässlicher IT-Betrieb ist eine wesentliche Voraussetzung dafür, dass kommunale Aufgaben dauerhaft erfüllt und Informationen angemessen geschützt werden können. Einheitliche Vorgaben helfen, Fehlkonfigurationen, Bedienfehler, unkontrollierte Änderungen und Ausfälle zu vermeiden sowie administrative Tätigkeiten nachvollziehbar zu gestalten.<br><br>Die Richtlinie legt organisationsweite Mindestanforderungen für einen sicheren und ordnungsgemäßen IT-Betrieb fest. Sie behandelt unter anderem den Lebenszyklus von IT-Komponenten, sichere Konfigurationen, administrative Tätigkeiten, Überwachung, Wartung sowie die Erstellung und Pflege von IT-Betriebshandbüchern. |
| **H**ilfsmittel **„Vorlage IT-Betriebshandbuch“** [↓.docx]<br><br>Ein IT-Betriebshandbuch stellt sicher, dass das für den Betrieb benötigte Wissen nachvollziehbar dokumentiert und nicht ausschließlich an einzelne Personen gebunden ist. Dies erleichtert die Einarbeitung und Vertretung, unterstützt einen geregelten Betrieb und ermöglicht bei Störungen oder personellen Veränderungen ein schnelleres und zielgerichtetes Handeln.<br><br>Die Vorlage unterstützt Kommunen dabei, die für den sicheren Betrieb einer IT-Komponente, einer Komponentengruppe, eines Fachverfahrens oder eines IT-Services erforderlichen Informationen strukturiert zu dokumentieren. Dazu gehören insbesondere Zuständigkeiten, technische Abhängigkeiten, Konfigurationen sowie Betriebs-, Wartungs- und Wiederherstellungsaufgaben. |
| **Beispiel „IT-Betriebshandbuch“** [↓.docx]<br><br>Ein ausgefülltes Beispiel erleichtert den Einstieg in die Erstellung eigener IT-Betriebshandbücher und macht deutlich, welche Informationen in welcher Form dokumentiert werden können. Dadurch lassen sich Unklarheiten bei der Anwendung der Vorlage und mögliche Dokumentationslücken reduzieren.<br><br>Das vollständig ausgefüllte, fiktive Beispiel zeigt anhand einer Server- und Virtualisierungsinfrastruktur, wie die SiKoSH-Vorlage in der Praxis verwendet werden kann. Es dient als Orientierung und muss für den Einsatz an die tatsächlichen technischen und organisatorischen Gegebenheiten der jeweiligen Kommune angepasst werden. |
| **Richtlinie „Patch-, Änderungs- und Schwachstellenmanagement“** [↓.docx]<br><br>Anforderungen zu geregelten Prozessen für Änderungen, Sicherheitsupdates und den Umgang mit Schwachstellen mit dem Ziel IT-Systeme sicher und stabil zu betreiben. |
| **Konzept „Patch-, Änderungs- und Schwachstellenmanagement“** [↓.docx] |

| Titel des Dokuments – Beschreibung |
| --- |
| Beschreibung der organisatorischen und technischen Umsetzung der Anforderungen der Richtlinie Patch-, Änderungs- und Schwachstellenmanagement. |
| **„Hilfsmittel Schwachstellenregister“** [↓.xslx]<br><br>Hier können Schwachstellen erfasst und eingestuft werden sowie die umgesetzten Maßnahmen dokumentiert werden. |
| **Richtlinie „Schutz vor Schadprogrammen“** [↓.docx]<br><br>Diese Richtlinie regelt die organisatorischen und technischen Mindestanforderungen zum Schutz vor Schadprogrammen. |
| **Konzept „Schutz vor Schadprogrammen“** [↓.docx]<br><br>Dieses Konzept regelt die organisatorischen und technischen Mindestanforderungen zum Schutz vor Schadprogrammen. |
| **Richtlinie „Protokollierung“** [↓.docx ]<br><br>Eine angemessene Protokollierung ermöglicht es, technische Abläufe und sicherheitsrelevante Vorgänge nachzuvollziehen, Störungen und Sicherheitsvorfälle zu erkennen und deren Ursachen zu untersuchen. Gleichzeitig müssen Protokolldaten vor unberechtigtem Zugriff und Veränderung geschützt und rechtliche Anforderungen berücksichtigt werden.<br><br>Die Richtlinie legt die übergreifenden organisatorischen und technischen Mindestanforderungen an die Protokollierung fest. Sie regelt insbesondere Verantwortlichkeiten, die Auswahl zu protokollierender Ereignisse, die technische Einrichtung und Überprüfung der Protokollierung, Zeitsynchronisation, Schutz und Rechtevergabe, Auswertung und Alarmierung sowie Aufbewahrung und Löschung von Protokolldaten. |
| **Hilfsmittel Protokollierungsübersicht** [↓.docx ]<br><br>Das ergänzende SiKoSH-Hilfsmittel „Protokollierungsübersicht“ unterstützt dabei, die erforderlichen systemspezifischen Festlegungen strukturiert zu dokumentieren. Dazu gehören unter anderem Zweck und Umfang der Protokollierung, relevante Ereignisse, Verantwortlichkeiten, Speicher- und Übertragungswege, Zugriffsberechtigungen, Auswertung sowie Aufbewahrungs- und Löschfristen. Die Übersicht kann eigenständig oder als Bestandteil der Betriebsdokumentation geführt werden. |
| **Richtlinie „Mobiles Arbeiten“** [↓.docx ]<br><br>Beim mobilen Arbeiten werden dienstliche Informationen außerhalb der geschützten kommunalen Arbeitsumgebung verarbeitet. Dadurch entstehen besondere Risiken, etwa durch Einsichtnahme oder Mithören, den Verlust von Geräten und Unterlagen sowie die Nutzung fremder Netzwerke oder ungeeigneter Arbeitsorte. Einheitliche Vorgaben helfen, diese Risiken zu begrenzen und ermöglichen ein sicheres Arbeiten unabhängig vom jeweiligen Arbeitsort.<br><br>Die Richtlinie legt organisatorische Mindestanforderungen für den Schutz dienstlicher Informationen beim mobilen Arbeiten fest. Sie regelt insbesondere den Schutz vor Einsichtnahme und Mithören, den Umgang mit dienstlichen Informationen und Unterlagen, die Nutzung externer Zugänge und Netzwerke, den sicheren Transport sowie das Verhalten bei Verlust, Diebstahl und anderen Sicherheitsvorfällen. Technische Anforderungen an mobile Endgeräte werden in der separaten Richtlinie „Mobile Endgeräte“ behandelt. |

# 7 SiKoSH Phase 4: Allgemeine Musterregelungen

## 7.1 Überblick

In den Musterregelungen der SiKoSH-Phase 4 werden insbesondere die Aspekte **physikalische Infrastruktur (Gebäudesicherheit), Beschaffung und Entsorgung** und **Outsourcing** behandelt.

→Aktivitätsdiagramm

In der SiKoSH Phase 4 werden finden folgende BSI-Grundschutz-Bausteine angewendet:

- CON.6 Löschen und Vernichten
- INF.1 Allgemeines Gebäude
- INF.2 Rechenzentrum sowie Serverraum
- INF.5 Raum sowie Schrank für technische Infrastruktur
- INF.6 Datenträgerarchiv
- INF.7 Büroarbeitsplatz
- INF.8 Häuslicher Arbeitsplatz
- INF.9 Mobiler Arbeitsplatz
- INF.10 Besprechungs-, Veranstaltungs- und Schulungsräume
- INF.11 Allgemeines Fahrzeug
- INF.12 Verkabelung
- OPS.2.2 Cloud-Nutzung
- OPS.2.3 Nutzung von Outsourcing

Gebäudesicherheit

Der Bereich Gebäudesicherheit ist wegen seiner vielfältigen Schnittstellen zu vielen anderen Sicherheitsaspekten *von zentraler Bedeutung*. Die Prozesse der Entsorgung stehen in engem Zusammenhang mit dem Schutzziel „Vertraulichkeit“ der verarbeiteten Daten.

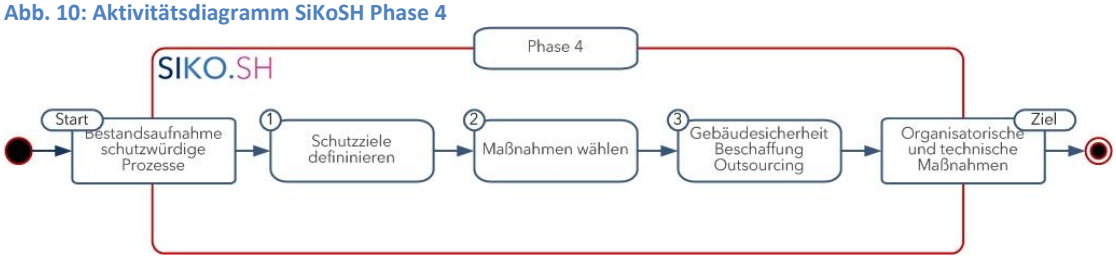
Cloud und Outsourcing

Der Themenbereich „Outsourcing von IT-Dienstleistungen“ muss selbstverständlich nur dann bearbeitet werden, wenn es Outsourcing von IT-Dienstleistungen gibt.

Beschaffung und Entsorgung

Der Bereich Beschaffung und Entsorgung definiert Sicherheitsanforderungen an Informationssysteme im Rahmen von Beschaffungs- und Aussonderungsvorgängen.

**Abb. 10: Aktivitätsdiagramm SiKoSH Phase 4**



## 7.2 Übersicht: Dokumente der SiKoSH Phase 4

→Aktivitätsdiagramm

Registrierte SiKoSH-Anwender laden SiKoSH Dokumente mit einem Klick auf die entsprechende Formatanzeige in der Tabelle (.pdf, .docx, .dotx, .xlsx) zur weiteren Verwendung herunter.

Tabelle 5 zeigt die wichtigsten Dokumente der SiKoSH Phase 4. Registrierte SiKoSH-Anwender laden SiKoSH Dokumente mit einem Klick auf die entsprechende Formatanzeige in der Tabelle (.pdf, .docx, .dotx, .xlsx) zur weiteren Verwendung herunter.

Tabelle 5: SiKoSH Phase 4 – Übersicht Dokumente

| Titel des Dokuments – Beschreibung |
|---|
| **Quickcheck Phase 4 – Allgemeine Musterregelungen,**<br>**enthalten in „SiKoSH ISMS-Übersicht“** [↓.xslx]<br>Der Quickcheck der Phase 4 behandelt ausgewählte Bausteine aus den Bereichen Konzeption und Vorgehensweise, Betrieb und Infrastruktur. |
| **Richtlinie „Löschen und Vernichten“ [**↓ .docx]<br>Die Richtlinie legt die Anforderungen an das sichere Löschen und Vernichten von Informationen und Datenträgern fest. Sie berücksichtigt dabei gesetzliche Aufbewahrungs- und Archivierungspflichten und regelt insbesondere Verantwortlichkeiten, Lösch- und Vernichtungsverfahren sowie deren Nachweis. |
| **Hilfsmittel „Aufbewahrungs- und Löschregister“ [**↓ .docx]<br>Dieses die Richtlinie Löschen und Vernichten ergänzende Hilfsmittel unterstützt Kommunen bei der Erfassung und Verwaltung von Aufbewahrungsfristen, Archiventscheidungen und Löschregelungen. Es enthält beispielhafte Registereinträge für typische kommunale Aufgabenbereiche sowie eine Vorlage zur Festlegung geeigneter Lösch- und Vernichtungsverfahren. Die Musterangaben sind organisationsspezifisch anzupassen und fachlich zu prüfen. |
| **Richtlinie „Physische Sicherheit“ [**↓ .docx]<br>Die Richtlinie legt verbindliche Mindestanforderungen an die physische Sicherheit von Gebäuden, Räumen und technischer Infrastruktur fest. Sie behandelt insbesondere Zutritt und Verschluss, Brandschutz, Stromversorgung, Verkabelung sowie den Schutz besonders sicherheitsrelevanter Bereiche. |
| **Konzept „Sicherheitskonzept Gebäudenutzung“ [↓ .docx]**<br>Das IT-Grundschutz-Profil „Basis-Absicherung Kommunalverwaltung“ berücksichtigt mit INF.1.A9 ausdrücklich die Anforderung an ein Sicherheitskonzept für die Gebäudenutzung, einschließlich eines IT-bezogenen Brandschutzkonzepts.<br>Die ergänzende Vorlage unterstützt Kommunen bei der standortbezogenen Umsetzung und Dokumentation dieser Anforderungen. Sie enthält strukturierte Eingabefelder für Verantwortlichkeiten, Schutz- und Sicherheitsbereiche, Zutrittsregelungen, technische Schutzmaßnahmen sowie Prüf- und Wartungsmaßnahmen. Die farbliche Kennzeichnung unterscheidet zwischen Pflichtangaben, bedingt erforderlichen und optionalen Angaben. |
| **Beispiel „Sicherheitskonzept Gebäudenutzung“ [↓ .docx]** |

| **Titel des Dokuments – Beschreibung** |
| --- |
| Ein vollständig ausgefülltes Beispiel für ein fiktives Rathaus veranschaulicht die praktische Anwendung der Konzeptvorlage „Sicherheitskonzept Gebäudenutzung“. Die Beispielangaben dienen der Orientierung und müssen an die tatsächlichen örtlichen und organisatorischen Gegebenheiten angepasst werden. |
| **„Sichere Cloud-Nutzung“** [↓.pdf \| .docx ]<br>Diese Richtlinie beschreibt den Umgang mit Dienstleistern und Dienstleistungen aus den Bereichen Outsourcing und Clouddienste. |

# 8 SiKoSH Phase 5: Technische Musterregelungen

## 8.1 Überblick

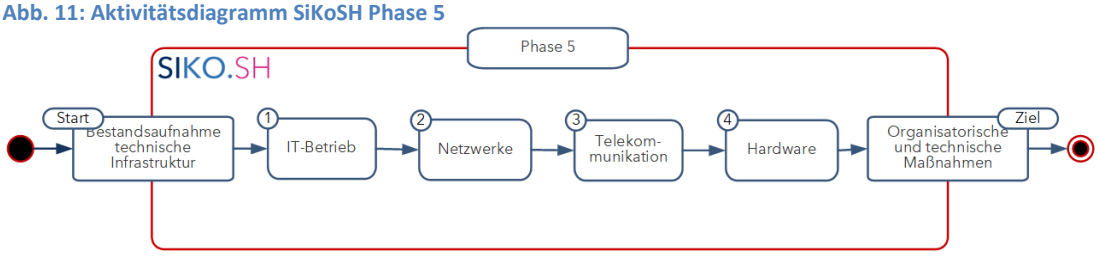
→Aktivitätsdiagramm

Technische Musterregelungen und die dazugehörigen Quickchecks beziehen sich insbesondere auf die interne und externe IT-Infrastruktur und deren Administratoren.

In SiKoSH werden folgende BSI-Grundschutz-Bausteine angewendet:

- OPS.1.2.5 Fernwartung
- NET.1.1 Netzarchitektur und –design
- NET.1.2 Netzmanagement
- NET.2.1 WLAN-Betrieb
- NET.2.2 WLAN-Nutzung
- NET.3.1 Router und Switches
- NET.3.2 Firewall
- NET.3.3 VPN
- NET.4.1 TK-Anlagen
- NET.4.2 VoIP
- NET.4.3 Faxgeräte und Faxserver
- SYS.1.1 Allgemeiner Server
- SYS.1.2.3 Windows-Server
- SYS.1.5 Virtualisierung
- SYS.1.9 Terminal-Server
- SYS.2.1 Allgemeiner Client
- SYS.2.2.3 Clients unter Windows
- SYS.2.5 Client-Virtualisierung
- SYS.2.6 Virtual Desktop Infrastructure
- SYS.3.1 Laptop
- SYS.3.2.1 Allgemeine Smartphones und Tablets
- SYS.3.3 Mobiltelefon
- SYS.4.1 Drucker, Kopierer und Multifunktionsgeräte
- SYS.4.5 Wechseldatenträger

Abb. 11: Aktivitätsdiagramm SiKoSH Phase 5



## 8.2 Übersicht: Dokumente der SiKoSH Phase 5

Registrierte SiKoSH-Anwender laden SiKoSH Dokumente mit einem Klick auf die entsprechende Formatanzeige in der Tabelle (.pdf, .docx, .dotx, .xlsx) zur weiteren Verwendung herunter.

→Aktivitätsdiagramm

Tabelle 6 zeigt die wichtigsten Dokumente der SiKoSH Phase 5. Registrierte SiKoSH-Anwender laden SiKoSH Dokumente mit einem Klick auf die entsprechende Formatanzeige in der Tabelle (.pdf, .docx, .dotx, .xlsx) zur weiteren Verwendung herunter.

Tabelle 6: SiKoSH Phase 5 – Übersicht Dokumente

| Titel des Dokuments – Beschreibung |
|---|
| **Quickcheck Phase 5 – Technische Musterregelungen,**<br>**enthalten in „SiKoSH ISMS-Übersicht“** [↓.xslx]<br>Der Quickcheck der Phase 5 behandelt ausgewählte Bausteine aus den Bereichen Betrieb, Netze und Kommunikation sowie IT-Systeme. |
| **Hilfsmittel „Fernzugriff und Fernwartung“** [↓.pdf \| .docx ]<br>**Anlage „Vereinbarung“** [↓.pdf \| .docx ]<br>Diese Richtlinie dient der Dokumentation der Aufgaben und Tätigkeiten, die mit dem Betrieb, der Administration von Hard- und Softwarekomponenten und der Fernwartung von Verfahren verbunden sind. |
| **Richtlinie „Netzarchitektur und Netzwerkmanagement“** [↓.pdf \| .docx ]<br>Zuverlässiges Netzmanagement ist Grundvoraussetzung für den sicheren und effizienten Betrieb moderner Netze. Dazu ist es erforderlich, dass das Netzmanagement alle Netzkomponenten umfassend integriert. Außerdem müssen geeignete Maßnahmen umgesetzt werden, um die Netz-Kommunikation und -infrastruktur zu schützen. |
| **Richtlinie „WLAN“** [↓.pdf \| .docx ]<br>Die Richtlinie beschreibt grundsätzliche Anforderungen, die beachtet und erfüllt werden müssen, wenn WLANs aufgebaut und betrieben werden. |
| **Richtlinie „Netzwerkkomponenten“** [↓.docx]<br>Diese Richtlinie unterstützt bei der Umsetzung der kommunalen Basisanforderungen, die sich aus den BSI-Bausteinen NET.3.1 (Router und Switches), NET.3.2 (Firewalls) und NET.3.3 (VPN) ergeben. |
| **Richtlinie „Serversicherheit“** [↓.pdf \| .docx ]<br>Diese Richtlinie behandelt die bestehenden Anforderungen für Planung und Konzeption, Beschaffung und Betrieb von Servern. |
| **Richtlinie „Virtualisierung“** [↓.pdf \| .docx ]<br>Diese Richtlinie regelt die Voraussetzungen für den Betrieb von Virtualisierungsumgebungen in der anwendenden Behörde. |
| **Richtlinie „Multifunktionsgeräte“** [↓.pdf \| .docx ] |

| Titel des Dokuments – Beschreibung |
| --- |
| Diese Richtlinie regelt die Einsatzrahmenbedingungen für Multifunktionsgeräte (typischerweise Multifunktionsdrucker). Es umfasst Vorgaben zu Aufstellort und Authentisierung sowie der Administration der Geräte. |
| **Richtlinie „Penetrationstests“** [↓.pdf \| .docx ]<br><br>Diese Richtlinie regelt die Voraussetzungen für alle Penetrationstests im Kontext der anwendenden Behörde.<br><br>Hinweis: Penetrationstests sind nicht Gegenstand der kommunalen Basisabsicherung; von daher wird diese Richtlinie nicht mehr weitergepflegt. |
| **Richtlinie „Webserverbetrieb“** [↓.pdf \| .docx ]<br><br>Mit dieser Sicherheitsrichtlinie erfüllt die anwendende Institution die nach BSI Grundschutz Baustein 5.4 Webserver bestehenden Anforderungen zur Strukturierung von Sicherheitsmaßnahmen für die Planung und Konzeption, die Beschaffung, die Umsetzung, den Betrieb und die Notfallvorsorge für Webserver.<br><br>Hinweis: Webserver sind nicht Gegenstand der kommunalen Basisabsicherung; von daher wird diese Richtlinie nicht mehr weitergepflegt. |

# 9 SiKoSH Phase 6: Regelungen für Verfahren

## 9.1 Überblick

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

→Aktivitätsdiagramm

In der SiKoSH Phase 6 werden folgende BSI-Bausteine angewendet:

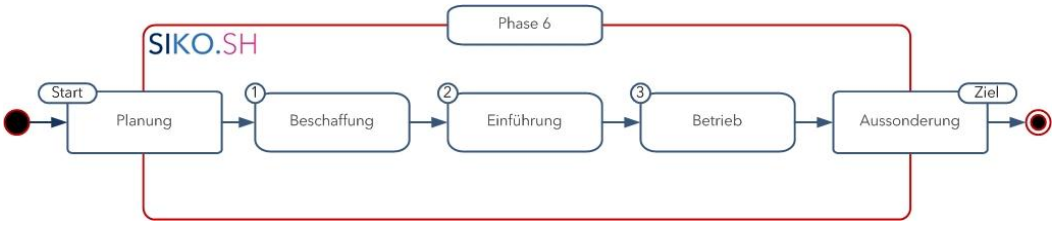
- APP.1.1 Office-Produkte
- APP.1.2 Webbrowser
- APP.2.1 Allgemeiner Verzeichnisdienst
- APP.2.2 Active Directory Domain Services
- APP.3.3 Fileserver
- APP.5.3 Allgemeiner E-Mail-Client und -Server
- APP.6 Allgemeine Software

## 9.2 Iteration – Zuordnung im Lebenszyklus

Fachverfahren bzw. IT-Komponenten durchlaufen idealtypisch folgende Lebensphasen:

Fachverfahren

Abb. 12: Aktivitätsdiagramm SiKoSH Phase 6




## 9.3 Übersicht: Dokumente der SiKoSH Phase 6

Tabelle 7 zeigt die wichtigsten Dokumente der SiKoSH Phase 6. Registrierte SiKoSH-Anwender laden SiKoSH Dokumente mit einem Klick auf die entsprechende Formatanzeige in der Tabelle (.pdf, .docx, .dotx, .xlsx) zur weiteren Verwendung herunter.

→Aktivitätsdiagramm

Tabelle 7: SiKoSH Phase 6 – Übersicht Dokumente

| Titel des Dokuments – Beschreibung |
|---|
| **Quickcheck Phase 6 – Regelungen für Verfahren,**<br>**enthalten in „SiKoSH ISMS-Übersicht“** [↓.xslx]<br>Der Quickcheck der Phase 6 behandelt ausgewählte Anwendungsbausteine. |
| **„Betriebshandbuch – Verfahren“** [↓.pdf \| .docx ]<br>Dieses BHB dient der Beschreibung von Verfahren. |
| **„Rollen und Rechte“** [↓.pdf \| .docx ]<br>Diese Richtlinie behandelt Anforderungen an Standardsoftware auf Client-Rechnern. |

# 10 SiKoSH Phase 7: Notfallmanagement

## 10.1 Überblick

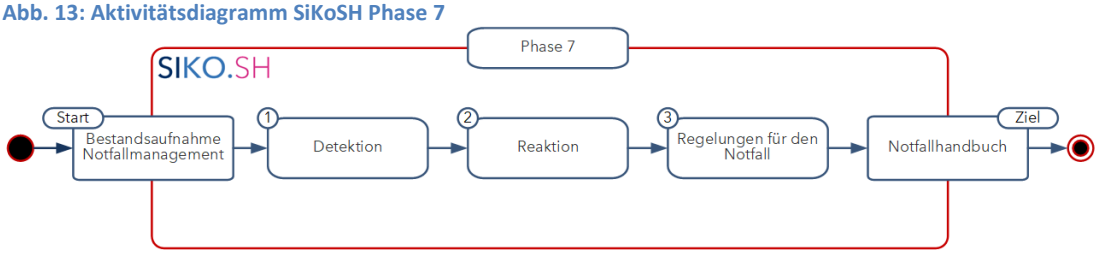
→Aktivitätsdiagramm

Die Notfallvorsorge wird sinnvollerweise am Ende der Dokumentation eines Fachverfahrens oder anderer IT-Komponenten geplant und umgesetzt.

In der SiKoSH Phase 7 werden folgende BSI-Grundschutz-Bausteine angewendet:

- DER.1 Detektion von sicherheitsrelevanten Ereignissen
- DER.2.1 Behandlung von Sicherheitsvorfällen
- DER.2.2 Vorsorge für die IT-Forensik

Abb. 13: Aktivitätsdiagramm SiKoSH Phase 7




## 10.2 Übersicht: Dokumente der SiKoSH-Phase 7

→Aktivitätsdiagramm

Tabelle 8 zeigt die wichtigsten Dokumente der SiKoSH Phase 7. Registrierte SiKoSH-Anwender laden SiKoSH Dokumente mit einem Klick auf die entsprechende Formatanzeige in der Tabelle (.pdf, .docx, .dotx, .xlsx) zur weiteren Verwendung herunter.

Tabelle 8: SiKoSH Phase 7 – Übersicht Dokumente

| Titel des Dokuments – Beschreibung |
|---|
| **Quickckeck Phase 7 – Notfallmanagement,**<br>**enthalten in „SiKoSH ISMS-Übersicht“** [↓.xslx]<br>Der Quickcheck der Phase 7 ermöglicht die Dokumentation der Notfallbewältigung in einem Notfallhandbuch. |
| **„Notfallhandbuch“** [↓.pdf \| .docx ]<br>Das Notfallhandbuch trifft Regelungen für eine IT-Notfallsituation und hilft den Notfallverantwortlichen im Krisenfall bei einer effektive Krisenbewältigung. |
| **Hilfsmittel „Notfallmanagement“** [↓.pdf]<br>Obwohl der Baustein DER.4 kein Teil des Profils Kommunalverwaltung ist, bietet SiKoSH ein optionales Hilfsmittel für die Umsetzung eines Notfallmanagements. |

# 11 SiKoSH Ziel - Querschnittsprüfung

## 11.1 Überblick

→Aktivitätsdiagramm

Nach der Bearbeitung der sieben SiKoSH-Phasen wird im letzten Schritt mit der Bearbeitung des SiKoSH-Quickchecks „Querschnittsprüfung“ der Erfolg der ISMS-Einführung bewertet. Die Querschnittsprüfung liefert eine kennzahlenbasierte Messung des Erfolgs der ISMS-Einführung und weist auf noch offene Prüfpunkte hin, die im weiteren Verlauf der ISMS-Inbetriebnahme bearbeitet werden müssen. Mit der Querschnittsprüfung hat das ISMS seine erste Iteration durchlaufen. Die Kennzahlen und Grafiken der ISMS-Übersicht können für die Darstellung des ISMS-Umsetzungsstatus und Fortschritt für den Management-Report an die Behördenleitung genutzt werden.

## 11.2 Übersicht: Dokumente der SiKoSH-Querschnittsprüfung

Tabelle 9 zeigt die wichtigsten Dokumente der Querschnittsprüfung. Registrierte SiKoSH-Anwender laden SiKoSH Dokumente mit einem Klick auf die entsprechende Formatanzeige in der Tabelle (.pdf, .docx, .dotx, .xlsx) zur weiteren Verwendung herunter.

Tabelle 9: SiKoSH Schritt 9 – Querschnittsprüfung: Übersicht Dokumente

| Titel des Dokuments – Beschreibung |
|---|
| **Querschnittsprüfung (QP),**<br>**enthalten in „SiKoSH ISMS-Übersicht“** [↓.xslx]<br>Die Querschnittsprüfung berechnet nach Bearbeitung der Quickchecks den tatsächlichen Erfüllungsgrad des ISMS und stellt diesen im Vergleich zur initialen Selbsteinschätzung dar. Aus den Ergebnissen kann abgelesen werden, wo vordringlich noch nachgebessert werden muss.<br>Die zusätzlichen Tabellenblätter *Auswertung QP, Auswertung Phasen, Kennzahlen* und *Pivot Auswertung* dienen dem Aufzeigen des Fortschritts mit der Bearbeitung der SiKoSH Vorgehensweise und können für den Managementbericht an die Behördenleitung genutzt werden. |
| **Hilfsmittel „Bearbeiten der ISMS-Übersicht“** [↓.pdf]<br>Anleitung zum Umgang mit der ISMS-Übersicht |

# 12 Sicherheitskonzept

## 12.1 Was mit SiKoSH erreicht wird

Kommunale Basis-Absicherung

Wenn alle Phasen mit ihren im kommunalen IT-Grundschutz-Profil bzw. in den SiKoSH-Quickchecks aufgeführten kommunalen Basisanforderungen bearbeitet sind, hat SiKoSH sein Projektziel „kommunale Basis-Absicherung“ erreicht.

Auch wenn das vermutlich mit einer beachtlichen Kraftanstrengung verbunden war, ist die Arbeit an dieser Stelle leider immer noch nicht zu Ende.

Zum einen verlangt der PDCA-Zyklus ein ständiges Nachbessern des Status quo, zum anderen ist – abhängig von der Kritikalität der betriebenen IT-Infrastrukturen und -Verfahren – grundsätzlich mindestens die Standard-Absicherung nach BSI IT-Grundschutz anzustreben.

Das gehört aber nicht mehr zu dem Projektauftrag von SiKoSH. Nachfolgend wird das weitere Vorgehen kurz skizziert.

## 12.2 Empfehlung für das weitere Vorgehen

Standardabsicherung
Die Erstellung eines Sicherheitskonzepts stellt auch nach den Vorgaben des SiKoSH-Leitfadens bereits hohe fachliche Anforderungen. Der Einsatz eines Werkzeugs zur Unterstützung wird empfohlen[19]

Das Sicherheitskonzept ist das Hauptdokument im Sicherheitsprozess der Organisation. Es stellt die Klammer dar für die in den SiKoSH-Phasen erstellten Dokumente. Das Sicherheitskonzept dient der Dokumentation der Sicherheitsstrategie und des Umsetzungsstands der Sicherheitsmaßnahmen.

Durch die Umsetzung und Dokumentation der kommunalen Basisanforderungen mit SiKoSH und seinen Hilfsmitteln ist ein grundlegender Schritt in Richtung Erstellung eines Sicherheitskonzepts nach dem BSI-Standard 200-2 getan.

Für das Sicherheitsniveau „Standardabsicherung“ fehlen aber noch

- IT-Strukturanalyse
- Bisher nicht berücksichtigte Basisanforderungen
- Standardanforderungen
- Risikomanagement
- ggf. zusätzliche Anforderungen[20]

## 12.3 IT-Strukturanalyse

→Aktivitätsdiagramm

Im IT-Grundschutz-Profil Basis-Absicherung Kommunalverwaltung wird eine Modell-Kommune mit ihren sicherheitsrelevanten Assets (z. B. Gebäude, IT-Infrastrukturen und Verfahren) behandelt.

Die Strukturanalyse erfasst die relevanten IT-Objekte und ihre Beziehungen untereinander

Im Rahmen einer Strukturanalyse werden die Daten, Informationen und Anwendungen ermittelt und die betroffenen IT-Systeme, Räume, Gebäude und Netze erfasst. Dabei ist es im

[19] Eine (nicht abschließende) Liste marktüblicher Werkzeuge finden Sie auf den Webseiten des BSI.

[20] Die BSI-Mitarbeiterin Isabel Münch zeigt in ihrem Beitrag „Scheinriese Sicherheitskonzept“, dass man sich vor einem Sicherheitskonzept nicht fürchten muss. Der größte Teil der Arbeit ist mit der durch die Arbeit mit SiKoSH entstandenen Sicherheitsdokumentation schon geschafft (https://www.kes-informationssicherheit.de/artikel/scheinriese-sicherheitskonzept/)

Allgemeinen sinnvoll, zuerst die produktiven Anwendungen und Daten zu ermitteln. Ausgehend von den Anwendungen können dann die weiteren relevanten Zielobjekte erfasst werden.

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

Sinnvoll sind weiterhin Netzpläne oder Architekturskizzen, die in das Sicherheitskonzept eingepflegt werden. So erhält ein fachkundiger Dritter einen besseren Eindruck und ein besseres Verständnis des Sicherheitskonzepts. Eine Strukturanalyse in Interviewform bei verantwortlichen IT-Leitern, Administratoren und weiteren Ansprechpartnern ist ein geeignetes Mittel, um ein Gefühl für die IT-Architektur zu entwickeln, die der Strukturanalyse zugrunde liegt.

## 12.4 Bisher noch nicht berücksichtigte Basis-Anforderungen

Aus der durchgeführten IT-Strukturanalyse können die Bausteine des IT-Grundschutz-Kompendiums ermittelt werden, die bisher noch nicht berücksichtigt worden sind. In der Hauptsache geht es darum, noch fehlende Basis-Anforderungen zu dokumentieren und umzusetzen.

## 12.5 Standardabsicherung

Der BSI-Standard 200-2 nennt bereits alle Absicherungsmaßnahmen, die für einen normalen Schutzbedarf erforderlich sind. Dazu gehören neben den Basis-Anforderungen auch die in den Bausteinen des IT-Grundschutz-Kompendiums aufgeführten Standard-Anforderungen.

Einige Standard-Anforderungen gehören bereits zum IT-Grundschutz-Profil Basis-Absicherung Kommunalverwaltung. Jetzt ist es an der Zeit, sich um die noch fehlenden Standardmaßnahmen zu kümmern.

Die im IT-Grundschutz-Kompendium aufgeführten Basis- und Standard-Anforderungen stellen zusammengenommen den Stand der Technik dar[21].

## 12.6 Risikomanagement

### 12.6.1 Schutzbedarfsfeststellung

Informationssicherheit und Datenschutz agieren risikobasiert. Sie akzeptieren, dass eine 100%-ige Sicherheit sowohl technisch als auch wirtschaftlich illusorisch ist und sehen somit eine Risikobehandlung anhand des festgestellten *Schutzbedarfs* vor.

[21] Vgl. BSI-Standard 200-2 Seite 18

Die Schutzbedarfsfeststellung ist auch Grundlage für die Umsetzung des Datenschutzrechts und für das Notfallmanagement

Der Schutzbedarf orientiert sich an den möglichen Schäden, die mit einer Beeinträchtigung der Geschäftsprozesse verbunden sind und umfasst auch die personenbezogenen Daten von Betroffenen innerhalb und außerhalb der Behörde.

Im Rahmen einer *Schutzbedarfsfeststellung* eines Informationsverbundes wird die Schadenshöhe für die drei Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit festgelegt.

### 12.6.2 Risikoanalyse

Risikoanalyse und Datenschutz-Folgenabschätzung gehen Hand in Hand

Die Risikoanalyse ist im BSI-Standard 200-3 beschrieben. Alle Objekte mit hohen Schutzbedarfen (im Datenschutz hohes Risiko für die Rechte und Freiheiten natürlicher Personen) 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. Die Risikoanalyse kann die ggf. datenschutzrechtlich erforderliche Datenschutz-Folgenabschätzung ersetzen, wenn die Risiken auch aus Sicht der betroffenen Person bewertet werden.

### 12.6.3 Risikobehandlung

Risikoanalyse

Die Behördenleitung entscheidet auf Grundlage der Risikoanalyse, wie mit den Risiken umgegangen werden soll.

Mögliche Methoden der Behandlung von Risiken sind:

Risikovermeidung

- Von einer IT, die nicht betrieben wird, geht auch kein Risiko aus. Allerdings müssen Behörden ihren gesetzlichen Auftrag erfüllen und insofern existiert nur wenig Spielraum hinsichtlich einer Risikovermeidung.

Risikoreduktion

- Durch die Umsetzung weiterer über die Standard-Absicherung herausgehende Maßnahmen (zusätzliche Maßnahmen) kann eine Reduzierung des Risikos erreicht werden. Diese sind entsprechend auch im Sicherheitskonzept zu dokumentieren.

Risikotransfer

- Hier wird der mögliche Schaden auf einen Dritten (Versicherer) übertragen. Hierbei ist zu beachten, dass immaterielle Schäden (wie z. B. Rufschäden) nicht abgesichert sind. Der Datenschutz schließt gar eine Übertragung von Schäden aufgrund von Datenschutzverletzungen auf Dritte generell aus.

Risikoakzeptanz

- Verbleibende Restrisiken, die nicht durch eine der vorstehenden Risikobehandlungsmethoden vollständig behandelt werden können, müssen letztlich akzeptiert werden. Dazu sind diese im Sicherheitskonzept deutlich zu benennen. Die Behördenleitung signalisiert durch ihre Unterschrift die Übernahme der Verantwortung für die identifizierten Restrisiken.

## 12.7 Revision

Der Vollständigkeit halber sei an dieser Stelle nochmals erwähnt, dass ein regelmäßiger Revisionszyklus (PDCA) eingehalten werden sollte. Die Revision dient der Feststellung, ob sich im IT-Verbund behandlungsbedürftige Änderungen ergeben haben, sei es aufgrund neuer sicherheitssensitiver Assets oder aufgrund wesentlicher Änderungen bei bestehenden sicherheitssensitiven Assets.

# 13 Anhang

## 13.1 Glossar

Das vollständige SiKoSH Glossar gibt es bei https://itvsh.de/was-wir-tun/it-sicherheit/sikosh-glossar.