ITV.SH
Kommunale Digitalisierung

# Standard:
# 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 | Standard: Einführung und Betrieb eines Informations-Sicherheits-Management-Systems (ISMS) |
| Version | 2.4.0 |
| Art | Standard/Richtlinie |
| Formatierung | SiKoSH_Styleguide.dotx (vs 2.4.0) |
| TLP | Clear |
| Dateiname | SiKoSH_Standard |
| veröffentlicht am | 02.12.2024 [aus DMS v1.7 – 02.12.2024] |

**. 4: Ihre Notizen**

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

# Inhalt

0 Überblick ..... 7
0.1 Zielsetzung von SiKoSH ..... 7
0.2 SiKoSH Standard – Zielpersonen ..... 7
0.3 Was ist SiKoSH? ..... 7
0.4 Zertifizierung ..... 8
0.5 Zentrale Aspekte, Komponenten und Begriffe ..... 8
1 Einführung ISMS ..... 11
1.1 Warum überhaupt ein ISMS? ..... 11
1.2 Warum SiKoSH? ..... 12
1.3 BSI IT-Grundschutz-Methodik und kommunales Grundschutzprofil ..... 12
1.4 Voraussetzungen für die erfolgreiche Anwendung von SiKoSH ..... 13
2 SiKoSH einführen ..... 14
2.1 Ziel von SiKoSH: Vermittler zwischen Theorie und Praxis ..... 14
2.2 Vorteile von SiKoSH ..... 16
3 Mit SiKoSH arbeiten ..... 17
3.1 SiKoSH Aktivitätsdiagramm ..... 17
3.2 Regelmäßig wiederkehrende Aufgaben ..... 18
3.3 Arbeiten mit den Quickchecks ..... 19
3.4 Tabellen „Übersicht Dokumente“ zu den SiKoSH Phasen ..... 19
4 SiKoSH Phase 1: Sicherheitsmanagement und Organisation ..... 21
4.1 Umsetzung Phase 1 ..... 21
4.2 Start: ISMS Arbeitsgruppe gründen ..... 21
4.3 Bestandsaufnahme Sicherheitsmanagement und Organisation ..... 22
4.4 Grundlagen schaffen ..... 22
4.5 Organisationsstruktur aufbauen ..... 23
4.6 Identitäts- und Berechtigungsmanagement ..... 24
4.7 Ziel SiKoSH Phase 1: Grundlegende ISMS-Struktur aufgebaut ..... 24
4.8 Übersicht: Dokumente zur SiKoSH Phase 1 ..... 25
5 SiKoSH Phase 2: Personal, Sensibilisierung und Schulung ..... 26
5.1 Sensibilisierung planen und starten ..... 26
5.2 Informationssicherheit lernen ..... 27
5.3 Sensibilisierung der Leitungsebene ..... 28
5.4 Übersicht: Dokumente der SiKoSH Phase 2 ..... 28

6 SiKoSH Phase 3: Standardregelungen ..... 29
6.1 Überblick ..... 29
6.2 Verankerung in der Organisation ..... 29
6.3 Internes Kontrollsystem, Nachhaltigkeit ..... 30
6.4 Übersicht: Dokumente der SiKoSH-Phase 3 ..... 31
7 SiKoSH Phase 4: Allgemeine Musterregelungen ..... 32
7.1 Überblick ..... 32
7.2 Übersicht: Dokumente der SiKoSH Phase 4 ..... 33
8 SiKoSH Phase 5: Technische Musterregelungen ..... 34
8.1 Überblick ..... 34
8.2 Übersicht: Dokumente der SiKoSH Phase 5 ..... 35
9 SiKoSH Phase 6: Regelungen für Verfahren ..... 37
9.1 Überblick ..... 37
9.2 Iteration – Zuordnung im Lebenszyklus ..... 37
9.3 Übersicht: Dokumente der SiKoSH Phase 6 ..... 37
10 SiKoSH Phase 7: Notfallmanagement ..... 39
10.1 Überblick ..... 39
10.2 Übersicht: Dokumente der SiKoSH-Phase 7 ..... 39
11 SiKoSH Ziel - Querschnittsprüfung ..... 40
11.1 Überblick ..... 40
11.2 Übersicht: Dokumente der SiKoSH-Querschnittsprüfung ..... 40
12 Sicherheitskonzept ..... 41
12.1 Was mit SiKoSH erreicht wird ..... 41
12.2 Empfehlung für das weitere Vorgehen ..... 41
12.3 IT-Strukturanalyse ..... 41
12.4 Bisher noch nicht berücksichtigte Basisanforderungen ..... 42
12.5 Standardabsicherung ..... 42
12.6 Risikomanagement ..... 42
12.7 Revision ..... 43
13 Anhang ..... 44
13.1 Index ..... 44
13.2 Glossar ..... 45

# Tabellen

Tabelle 1: Dokumente für den SiKoSH Kickoff 9
Tabelle 2: SiKoSH Phase 1 – Übersicht Dokumente 25
Tabelle 3: SiKoSH Phase 2 – Übersicht Dokumente 28
Tabelle 4: SiKoSH Phase 3 – Übersicht Dokumente 31
Tabelle 5: SiKoSH Phase 4 – Übersicht Dokumente 33
Tabelle 6: SiKoSH Phase 5 – Übersicht Dokumente 35
Tabelle 7: SiKoSH Phase 6 – Übersicht Dokumente 37
Tabelle 8: SiKoSH Phase 7 – Übersicht Dokumente 39
Tabelle 9: SiKoSH Schritt 9 – Querschnittsprüfung: Übersicht Dokumente 40

# Abbildungen

Abb. 1: Hierarchisch-analytisches Vorgehen ..... 14
Abb. 2: Beispiel: Theorie und Praxis in Schulsystemen ..... 15
Abb. 3: ISMS Komponenten ..... 16
Abb. 4: SiKoSH Aktivitätsdiagramm ..... 17
Abb. 5: PDCA-Methode der Einführung und des Betriebs eines ISMS ..... 18
Abb. 6: Aktivitätsdiagramm SiKoSH Phase 1 ..... 21
Abb. 7: Aktivitätsdiagramm SiKoSH Phase 2 ..... 26
Abb. 8: Lernkontinuum Informationssicherheit ..... 27
Abb. 9: Aktivitätsdiagramm SiKoSH Phase 3 ..... 29
Abb. 10: Aktivitätsdiagramm SiKoSH Phase 4 ..... 32
Abb. 11: Aktivitätsdiagramm SiKoSH Phase 5 ..... 34
Abb. 12: Aktivitätsdiagramm SiKoSH Phase 6 ..... 37
Abb. 13: Aktivitätsdiagramm SiKoSH Phase 7 ..... 39

# 0 Überblick

## 0.1 Zielsetzung von SiKoSH

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

Der hier vorliegende *„Standard: 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.

Ein **ISMS** besteht grundsätzlich aus:

- einer Aufbauorganisation (Rollenträger),
- einer Ablauforganisation (Prozesse/Verfahren),
- einem Regelwerk,
- und seiner Umsetzung.

## 0.2 SiKoSH Standard – Zielpersonen

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

## 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, 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 dem Anwender Vorlagen, Materialien, Hilfestellungen und Werkzeuge an die Hand.

… damit Informationssicherheits-Management machbar wird.

Dem **SikoSH-Standard** (auch SiKoSH-Framework genannt) liegt das *IT-Grundschutz-Profil Basis-Absicherung Kommunalverwaltung* der bundesweiten Arbeitsgruppe Kommunale Basisabsicherung (AG koBa) in der jeweils aktuellen Version zugrunde. Das IT-Grundschutzprofil Basis-Absicherung Kommunalverwaltung erleichtert den Einstieg in die Informationssicherheit und hilft die größten Schwachstellen aufzudecken.

SiKoSH erlaubt es, den gesetzlichen Verpflichtungen nachzukommen und eine sichere Informationsverarbeitung zu etablieren.

## 0.4 Zertifizierung

BSI Testat Basisabsicherung

SikoSH kann im Rahmen einer Zertifizierung hilfreich sein, da das BSI seit Einführung des IT-Grundschutz-Kompendiums auch ein *Testat nach der Basis-Absicherung*[1] anbietet.

## 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) enthält alle hoch-priorisierten Prüffragen der Quickchecks zu den sieben SiKoSH-Phasen. Die Querschnittsprüfung (QP) kann auch mit dem Start des SiKoSH-Prozesses als **Selbstauditierung** verwendet werden, um das allgemeine Sicherheitsniveau der Organisation festzustellen und eine informierte 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
- Phase 7: Notfallmanagement

### 0.5.3 Arten von SiKoSH Dokumenten und Materialien

SiKoSH Dokumentenarten

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

Standard und Richtlinien

Die Richtlinien fassen die Regelungen des SiKoSH Frameworks entsprechend den SiKoSH-Phasen in handhabbare Gruppen zusammen. Standard und Richtlinien sagen im Wesentlichen was gemacht werden muss, was gemacht werden soll, was nicht gemacht werden darf, etc., damit die definierten Sicherheitsziele erreicht werden.[2]

[1] 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

[2] https://datatracker.ietf.org/doc/html/rfc2119 für die in ISMS Frameworks verwendete Terminologie

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 Standard mit seinen Richtlinien spezifizierten Anforderungen aufwandsarm zu erreichen. Zu den Hilfsmitteln zählen Vorlagen, Anleitungen, Beispiele 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 schnellen Überblick über die Sicherheitslage geben und den Stand der Umsetzung des Standards mit seinen Richtlinien dokumentieren. Jede SiKoSH-Phase wird von einem Quickcheck eingeleitet: Sie enthalten Prüffragen zu den kommunalen Basisanforderungen, Verweise auf hilfreiche SiKoSH-Dokumente und – wie die Querschnittsprüfung (Querschnitts-Check) – auch als Selbstauditierung verstanden werden.

Sicherheitsdokumentation

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 das Sicherheitskonzept.

SiKoSH Styleguide

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

### 0.5.4 SiKoSH Start – Dokumente für den Kickoff

SiKoSH Anwender sollten sich mit diesen drei Dokumenten vertraut machen. Der Styleguide ist für alle Anwender wichtig, die SiKoSH Dokumente an ihre örtlichen Bedingungen anpassen wollen oder neue Dokumente im Stil von SiKoSH anfertigen wollen.

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 1: Dokumente für den SiKoSH Kickoff**

| Titel des Dokuments – Beschreibung |
|---|
| **„Standard – Einführung und Betrieb eines Informationssicherheitsmanagementsystems (ISMS)“** [↓.pdf ]<br>Hauptdokument des SiKoSH ISMS Frameworks mit Verweisen auf alle Richtlinien des Standards |
| **„Styleguide“** [↓.pdf \| .dotx ]<br>Anleitung für Bearbeitung und Erstellung von Dokumenten im SiKoSH Layout (mit MS Word Dokumentenvorlage) |
| **„Bearbeiten der Quickchecks“** [↓.pdf ]<br>Anleitung zum Umgang mit den SiKoSH Quickchecks |

### 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[3].

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[4] als Voraussetzung für die Nutzung ebenenübergreifender IT-Verfahren sowie die Verordnung zur Gewährleistung der IT-Sicherheit der im Portalverbund und zur Anbindung an den Portalverbund genutzten IT-Komponenten (ITSiV-PV)[5] genannt.

Grundlage der Digitalisierung von Verwaltungsverfahren (OZG)

Während die Leitlinie bei der Planung und Anpassung ebenenübergreifender IT-Verfahren den IT-Grundschutz des BSI vorsieht, unterscheidet die ITSiV-PV zwischen einer reinen Nachnutzung des OZG-Portalverbunds, hier ist die Basisabsicherung nach BSI-Standard 200-2 als Mindestsicherheitsstandard vorgeschrieben[6], und der Einbringung eigener OZG-Komponenten in den Portalverbund[7], hier gelten neben der Standardabsicherung nach dem BSI-Standard 200-2 noch weitere Anforderungen.

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). 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-

[3] 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)

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

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

[6] Mithin auch das Sicherheitsziel der kommunalen Basisabsicherung und von SiKoSH.

[7] Gilt auch bei Auftragsverarbeitung.

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 Grundschutz vorrangig an den aus der IT-Sicherheit bekannten Schutzzielen Verfügbarkeit, Integrität und Vertraulichkeit."

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) zu 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 funktionierendes ISMS nachweisen kann.

## 1.2 Warum SiKoSH?

SiKoSH ist ein „Do-it-Yourself ISMS"

Der SiKoSH-Standard 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 Einrichtung. SiKoSH begreift sich als *Do-it-Yourself ISMS* das durch Quickchecks, Mustervorlagen und viele andere Hilfsmittel den Weg zur Basisabsicherung nach BSI IT-Grundschutz leichtmacht.

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

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

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

- Kernabsicherung
- Standardabsicherung und
- Basisabsicherung.

Kernabsicherung

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

Standardabsicherung

Mit der **Standardabsicherung** 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 entspricht.

Basisabsicherung

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

Ziel von SiKoSH ist ein ISMS mit dem Sicherheitsniveau **Basisabsicherung**. An dieser Stelle sei deutlich darauf hingewiesen, dass die Basisabsicherung 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 Grundschutzprofil

Grundlage des SiKoSH-Standards ist das „IT-Grundschutzprofil BASIS-ABSICHERUNG KOMMUNALVERWALTUNG (kommunales Grundschutzprofil)“ der AG KoBA[8] in der jeweils aktuellen Version[9]. Das Kommunale Grundschutzprofil benennt dabei auf der Basis einer typischen Kommunalverwaltung die umzusetzenden BSI-Bausteine und die zur Umsetzung der Basisabsicherung erforderlichen Anforderungen .

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

Basisabsicherung und Testat

Die Beschränkung auf die Basisabsicherung 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.[10]

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-Standard 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 des Bundeslands11, DSGVO), IT-Grundschutz des BSI und einem grundsätzlichen Verständnis von Informationstechnik und Netzwerken ergänzt.

[8] https://info.it-sibe-forum.de/dokumente/it-grundschutz-profil
[9] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Hilfsmittel/Profile/Basis_Absicherung_Kommunalverwaltung.html
[10] Vgl. Nr. 5.2 des kommunalen Grundschutzprofils
[11] In Schleswig-Holstein s. http://www.gesetze-rechtsprechung.sh.juris.de

# 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.

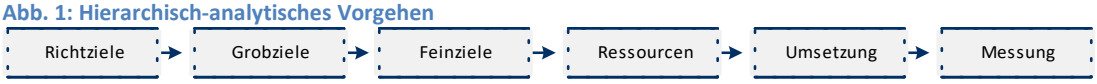
Sicherheitskultur

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

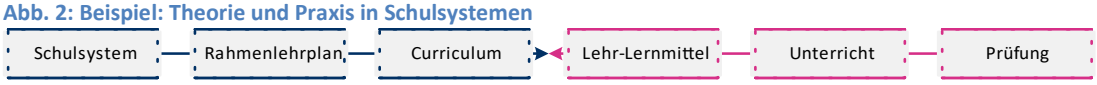



Das hierarchisch-analytische Vorgehen kennen wir aus allen Lebensbereichen. Nehmen wir das Schulsystem als Beispiel:
Das Schulsystem setzt eine bestimmte Vorstellung davon um, wie man die nachwachsende Generation mit den notwendigen Fähigkeiten und Fertigkeiten für z.B. ein erfolgreiches Leben ausstatten 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, das 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

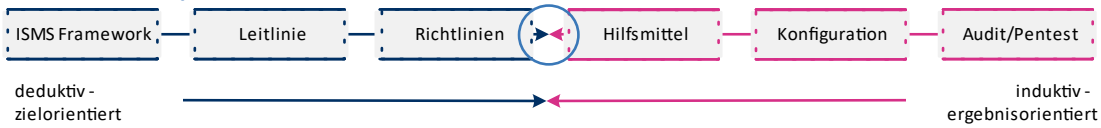
mit Dokumentation verbringen und ein Zertifikat ist für ihn nur dann wichtig, wenn es verlangt wird. Das sind sehr unterschiedliche Perspektiven und Herangehensweisen.

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 Grundschutzprofil Kommunale Basisabsicherung 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 kommunale Praktiker, die SiKoSH-Anwendern mit Rat und Tat zur Seite stehen.

## 2.2 Vorteile von SiKoSH

SiKoSH hat im Vergleich zu anderen Vorgehensmodellen diese Vorteile:

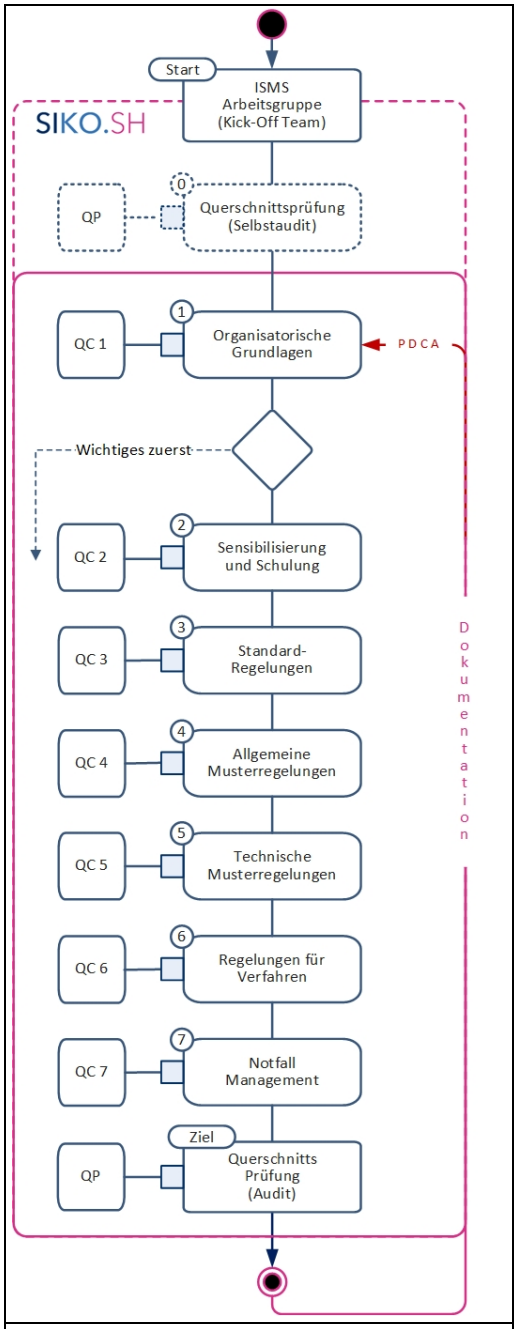
- SiKoSH wurde mit Blick auf Anforderungen und Gegebenheiten kommunaler Einrichtungen entwickelt.
- SiKoSH ist als Einstiegsframework leicht zu handhaben und mit **geringerem Ressourcenaufwand** umsetzbar.
- SiKoSH ergänzt andere etablierte ISMS Frameworks - wie z.B. BSI IT-Grundschutz, ISO/IEC 27001 - 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) 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 feststellt. 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 Dokumentation eines Sicherheitskonzepts (siehe Kap. 12 auf Seite 41) 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 – 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

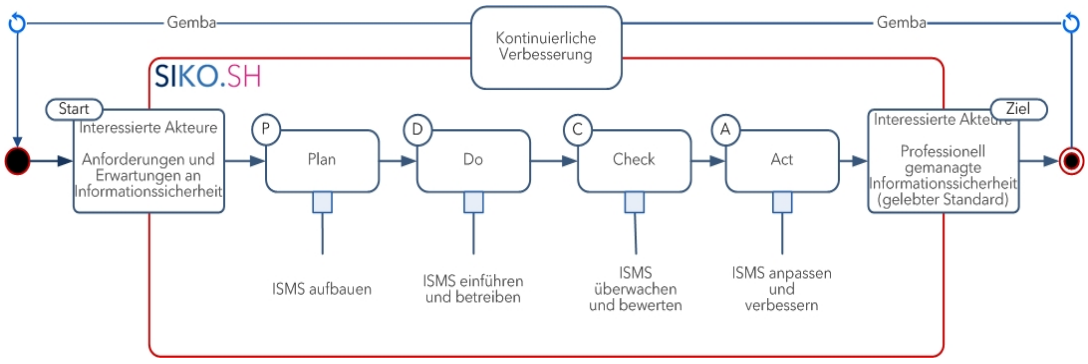
PDCA

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 Basisanforderungen. 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 Basisanforderungen.

Eine Sonderrolle spielt der Quickcheck „Querschnittsprüfung“. Er enthält zusammenfassende Prüffragen über alle Phasen-Quickchecks. Mit der Querschnittsprüfung bekommt der/die SiKoSH-Anwender:in einen soliden Überblick über den Stand der Informationssicherheit seiner Einrichtung.

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

SiKoSH hilft dabei die kommunale Basisabsicherung nach Maßgabe des „IT-Grundschutz-Profil: Basis-Absicherung Kommunalverwaltung“[12] umzusetzen.

Änderungen in der BSI IT-Grundschutz-Methodik werden in den SiKoSH-Standard übernommen, aktuell ist hier ein jährlicher Revisionszyklus geplant.

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-Gundschutzprofil: Basis-Absicherung-Kommunalverwaltung geändert haben.

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

**SiKoSH Phase 1 – Übersicht Dokumente**

| Titel des Dokuments – Beschreibung |
|---|
| **„QC 1 – Sicherheitsmanagement und Organisation“** [↓.xslx]<br>Der Quickcheck 1 (QC 1) behandelt die kommunalen Basisanforderungen der BSI-Bausteine ISMS.1 (Sicherheitsmanagement), ORP.1 (Organisation), ORP.4 (Identitäts- und Berechtigungsmanagement) und ORP.5 (Compliance Management). |
| **„Informationssicherheit für Behördenleitungen“** [↓.pdf \| .docx ]<br>Ein Onepager, der kurz und knapp die Ziele der Informationssicherheit und des Datenschutzes beschreibt. |

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

Ist ein Dokument noch nicht auf die gerade gültige Hauptversion des Standards 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 „SiKoSH Phase 3 – Übersicht Dokumente“.

SiKoSH Phase 3 – Übersicht Dokumente

| Titel des Dokuments – Beschreibung |
| --- |
| **„QC 3 – Standardregelungen“** [↓.xlsx ]<br>Der Quickcheck 3 (QC 3) behandelt ausgewählte Bausteine aus den Bereichen Konzeption und Vorgehensweisen. |

Ein Klick auf ↓ neben dem ausgegrauten Link im Standard ruft das Dokument *„Referenztabelle SiKoSH vs 2.4.0 auf Vorversionen“* auf, die Sie auf die entsprechende Vorversion leitet.

# 4 SiKoSH Phase 1: Sicherheitsmanagement und Organisation

## 4.1 Umsetzung Phase 1

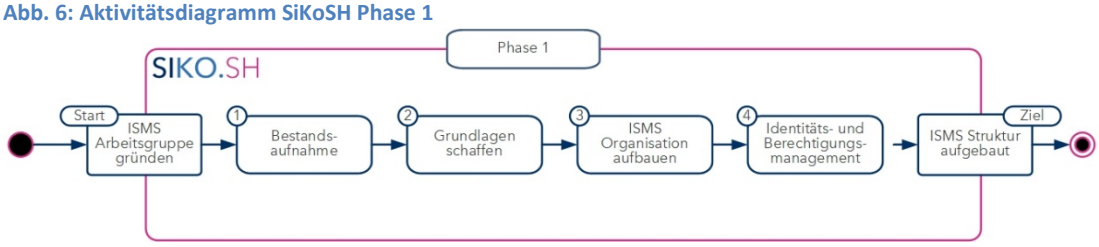
→Aktivitätsdiagramm

Die im SiKoSH-Standard 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:r 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

Quickcheck Phase 1

Die initiale Bestandsaufnahme mit dem Quickcheck 1 dient insbesondere dem Aufbau des ISMS hinsichtlich der Aufbau- und Ablauforganisation.

Nachdem der aktuelle Umsetzungsstand nach Maßgabe des Quickchecks 1: „Sicherheitsmanagement und Organisation“ festgestellt ist, sollten alle Prüfpunkte entsprechend Bearbeitungsstatus und Priorität abgearbeitet werden.

Nicht vollständig erfüllte Prüfpunkte sollten, frei nach dem *Pareto-Prinzip*, zu etwa zu 80% erfüllt sein bzw. Maßnahmen eingeleitet werden, die zur Erfüllung des Prüfpunktes im gewünschten Maße führen. Die Umsetzung der korrespondierenden Anforderungen wird durch die nachfolgend in dieser Vorgehensweise referenzierten Hilfsmittel erleichtert.

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 auch die Durchführung des Quickchecks „Querschnittsprüfung“. Erst wenn eine SiKoSH-Phase mit den jeweiligen Quickchecks befriedigend abgeschlossen ist, sollte mit der Umsetzung der nächsten SiKoSH-Phase begonnen 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/die später bestellte:n 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 ISLL Musterleitlinie 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 / eines ISB (siehe ISMS-Betrieb, Anlage 2

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-Organisation" 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:

- 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

ISMS Betrieb

Die Richtlinie „ISMS-Betrieb“ 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.

SiKoSH Styleguide ISMS-Betrieb

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

## 4.6 Identitäts- und Berechtigungsmanagement

Identitäts- und Berechtigungsmanagement

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

## 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.

Mitarbeiter sind der Schlüssel zur Informationssicherheit

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.

## 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 |
|---|
| **„QC 1 – Sicherheitsmanagement und Organisation“** [↓.xslx]<br>Der Quickcheck 1 (QC 1) behandelt die kommunalen Basisanforderungen der BSI-Bausteine ISMS.1 (Sicherheitsmanagement), ORP.1 (Organisation), ORP.4 (Identitäts- und Berechtigungsmanagement) und ORP.5 (Compliance Management). |
| **„Informationssicherheit für Behördenleitungen“** [↓.pdf \| .docx ]<br>Ein Onepager, der kurz und knapp die Ziele der Informationssicherheit und des Datenschutzes beschreibt. |
| **„Informationssicherheitsleitlinie“** [↓.pdf \| .docx ]<br>Muster einer Informationssicherheitsleitlinie zur individuellen Anpassung an die Bedürfnisse der Behörde |
| **„Bestellung des / der Informationssicherheitsbeauftragte:n“** [↓.pdf \| .docx ]<br>Formular zur ISB-Bestellung |
| **„ISMS-Betrieb“** [↓.pdf \| .docx ]<br>Vorgaben, Best Practice und Muster für den Betrieb eines ISMS |
| **„ISMS-Organisation“** [↓.pdf \| .docx ]<br>Die Richtlinie regelt die Aufbauorganisation für den erfolgreichen Betrieb eines ISMS |
| **„Identitäts- und Berechtigungsmanagement“** [↓.pdf \| .docx ]<br>Diese Richtlinie regelt den Zugriff auf schützenswerte Ressourcen einer Behörde. |
| **„Melden von Sicherheits- und Datenschutz-Vorfällen“** [↓.pdf \| .docx ]<br>Ein Meldeformular für Vorfälle. |
| **„Betriebshandbuch – allgemeiner Teil“** [↓.pdf \| .docx ]<br>Diese Vorlage für ein Betriebshandbuch (BHB) hilft der Behörde Anforderungen des BSI IT-Grundschutzes sowie etwaiger datenschutz-rechtlichen Anforderungen im Hinblick auf die Dokumentation von Fachverfahren zu gewährleisten. Hier werden grundlegende Dinge wie eine Liste der Verantwortlichen vor die Klammer gezogen. Die phasenspezifischen BHB (wie z. B. für die Verfahrensdokumentation) sind der jeweiligen SiKoSH-Phase zugeordnet. |
| **„QC QP – Querschnittsprüfung“** [↓.xslx]<br>Der Quickcheck Querschnittsprüfung enthält die wichtigsten Prüfpunkte der Quickchecks der 7 SiKoSH-Phasen. Er zeigt somit auf, wo vordringlich noch nachgebessert werden muss (siehe Kap. 11 - SiKoSH Ziel - Querschnittsprüfung) |

# 5 SiKoSH Phase 2: Personal, Sensibilisierung und Schulung

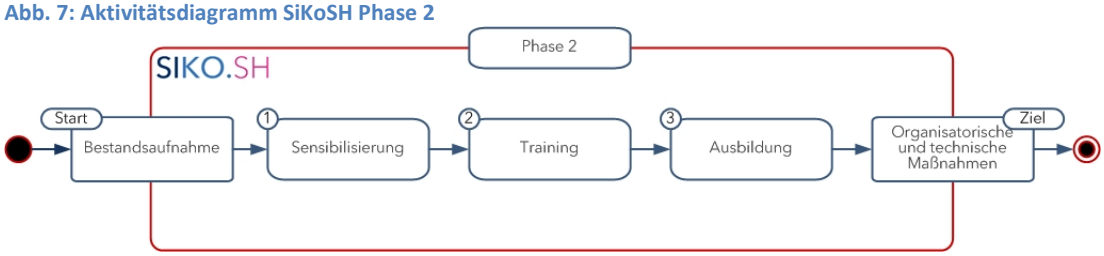
→Aktivitätsdiagramm

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.

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 Sensibilisierung planen und starten

Internationale Erfahrungen mit Sensibilisierung, Schulung und Training von Organisationen und individuellen Benutzern belegen, dass „Informationssicherheit“ ein abstraktes Konzept ist, das nur schwer gelernt werden kann. Andererseits zeigt die tägliche Praxis, dass Sicherheitsbedrohungen nicht ausschließlich technisch abgefedert werden können. Im Gegenteil, fast alle Angriffe auf die IT-Infrastruktur brauchen die (unfreiwillige) Mitarbeit von Benutzern für den Erfolg (bestes Beispiel sind Schadprogramme wie z. B. Locky oder Emotet).

Wissen reicht nicht

**Es genügt in der Regel nicht**, die Kenntnisse im Bereich Schadensmöglichkeiten, Schadvektoren und Verhalten zu erweitern. Mitarbeiter – und Benutzer ganz allgemein – 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.

Im Rahmen durchzuführender Sensibilisierungskampagnen sollten insbesondere nachfolgende Ratschläge beachtet werden:

- **Mitarbeiter ermutigen**, Verdächtiges zu melden, ohne Angst vor Repressalien zu haben. Dies muss von den Vorgesetzten unterstützt und vorgelebt werden.
- Berücksichtigen, dass Mitarbeiter unter erhöhtem Arbeitsdruck schnell in **alte Verhaltensmuster** verfallen und dann eine erhöhte Risikobereitschaft aufweisen, um 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

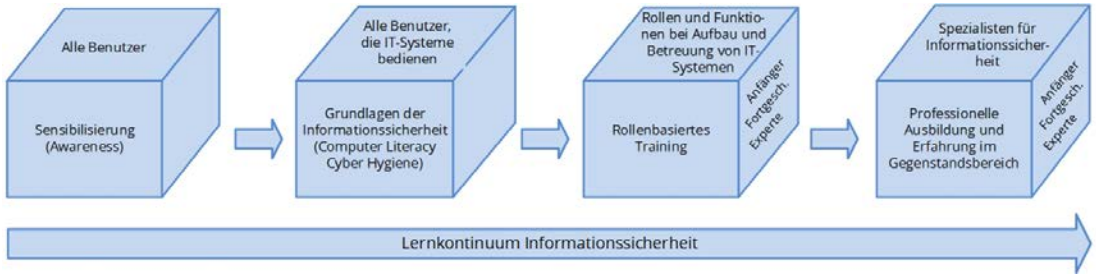
nicht getan, es muss eine Veränderung des Verhaltens der Mitarbeiter erreicht werden. Das ist leichter, wenn das Thema Informationssicherheit in Anweisungen, Prozessen, Vorgehensweisen und bei den Arbeitsaufträgen der Mitarbeiter immer eingebunden ist. Im Folgenden werden weitere Hilfsmittel aufgeführt, welche die Umsetzung von Maßnahmen zu den im Quickcheck 2: „Personal, Sensibilisierung und Schulung“ definierten Prüfpunkten erleichtern.

## 5.2 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.[13]

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.[14]

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.

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

[14] Das Merkblatt „Verhalten bei Sicherheitsvorfällen“ erläutert, was ein Sicherheitsvorfall ist und wer bei der Feststellung oder dem Verdacht eines Sicherheitsvorfalls zu informieren ist

## 5.3 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 die Prosperität der Einrichtung als wichtigstes Ziel ansieht und das Ziel „Informationssicherheit und Datenschutz“ oft mit möglichst geringem Aufwand zu erreichen sucht.

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

## 5.4 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 |
|---|
| **„QC 2 – Personal, Sensibilisierung und Schulung“** [↓.xslx]<br>Der Quickcheck 2 (QC 2) behandelt die kommunalen Basisanforderungen der BSI-Bausteine ORP.2 Personal und ORP.3 Sensibilisierung und Schulung zur Informationssicherheit. |
| **„Personal, Sensibilisierung und Schulung“** [↓.pdf \| .docx ]<br>Richtlinie mit Regelungen für das Personalmanagement, sowie Sensibilisierung und Schulung der Mitarbeitenden in Fragen der Informationssicherheit. |
| **„Sensibilisierung für Informationssicherheit und Datenschutz für die Leitungsebene in der öffentlichen Verwaltung“** [↓.pdf \| .docx ]<br>Argumentationshilfen für den Umgang mit Informationssicherheit und Datenschutz |
| **„Konzept: Schulung und Training für Informationssicherheit und Datenschutz“** [↓.pdf \| .docx ]<br>Grundlagen für den Aufbau einer Schulungs- und Trainingsumgebung |
| **„Beispiel: Sensibilisierung Informationssicherheit und Datenschutz“** [↓.pdf \| .docx ]<br>Grundlagen einer erfolgreichen Sensibilisierungskampagne am Beispiel der Landeshauptstadt Kiel |

# 6 SiKoSH Phase 3: Standardregelungen

## 6.1 Überblick

Aufgaben für Fachabteilungen

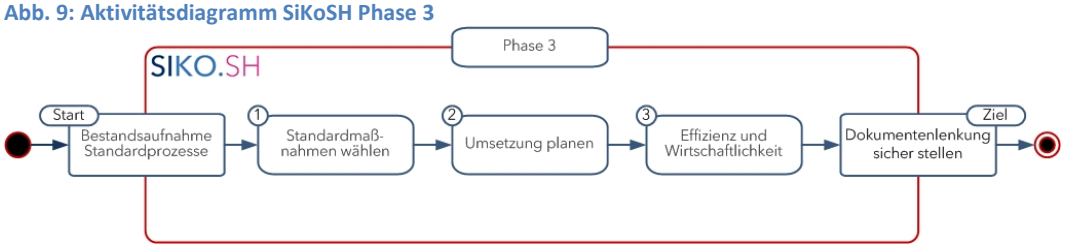
In der SiKoSH-Phase 3 werden zahlreiche Musterregelungen bereitgestellt, die wesentliche Aspekte des Sicherheitsmanagements aufgreifen. Die Verantwortung für die Ausarbeitung und Einführung dieser Regelungen liegt typischerweise nicht beim Informationssicherheitsbeauftragten (ISB), sondern in den jeweiligen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

→Aktivitätsdiagramm

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

- CON.1 Kryptokonzept
- CON.2 Datenschutz
- CON.3 Datensicherungskonzept
- CON.9 Informationsaustausch
- 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 Verankerung in der Organisation

Richtlinie Informationssicherheits- und Datenschutzmanagement

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.

Effizienz des ISMS

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).

Wirtschaftlichkeit des ISMS

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 Standard 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]

## 6.3 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.).

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.

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

## 6.4 Übersicht: Dokumente der SiKoSH-Phase 3

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.

→Aktivitätsdiagramm

Tabelle 4: SiKoSH Phase 3 – Übersicht Dokumente

| Titel des Dokuments – Beschreibung |
|---|
| **„QC 3 – Standardregelungen“** [↓.xslx]<br>Der Quickcheck 3 (QC 3) behandelt ausgewählte Bausteine aus den Bereichen Konzeption und Vorgehensweisen. |
| **„Betriebshandbuch-Prozesse“** [↓.pdf \| .docx ]<br>Hilfsmittel für die Dokumentation des laufenden IT-Betriebs. |
| **„Datensicherung“** [↓.pdf \| .docx ]<br>Regelungen für einen redundanten Datenbestand (Backup) zur Sicherstellung der zeitnahen Wiederaufnahme des Betriebs, wenn Teile des operativen Datenbestands verloren gehen. |
| **„Bürokommunikationssysteme (BKS)“** [↓.pdf \| .docx ]<br>Diese Richtlinie regelt den grundsätzlichen und fachverfahrensunabhängigen Umgang mit Verwaltungs-IT und damit zusammenhängenden Aspekten wie Informationsaustausch und Telearbeit. |
| **„Kryptografie“** [↓.pdf \| .docx ]<br>Diese Richtlinie regelt die Voraussetzungen für den Einsatz kryptografischer Vorgänge und behandelt den Einsatz von Krypto-Technologie zur Verschlüsselung digitaler Daten. |
| **„Datenschutz“** [↓.pdf \| .docx ]<br>Diese Richtlinie regelt die Umsetzung von technischen und organisatorischen Maßnahmen (TOM) zur Umsetzung der Gewährleistungsziele des Datenschutzrechts |
| **„Patch- und Änderungsmanagement“** [↓.pdf \| .docx ]<br>Diese Richtlinie legt Rahmenbedingungen für das Patchen von Infrastruktur- und Fachanwendungskomponenten sowie den Bezug von sicherheitsrelevanten Meldungen (z.B. über ein CERT) fest. Dies umfasst Verantwortlichkeiten sowie Fristen für das Einspielen von Patches in Abhängigkeit der Kritikalität etwaiger Fehler oder Lücken der jeweiligen Komponenten. Die Kritikalität wird hier ebenfalls definiert. |
| **„Protokollierung“** [↓.pdf \| .docx ]<br>Diese Richtlinie behandelt die Protokollierungsanforderungen aus der Sicht von Informationssicherheit und Datenschutz |
| **„Schutz vor Schadsoftware“** [↓.pdf \| .docx ]<br>Diese Richtlinie definiert Anforderungen und Regelungen an Virenschutzlösungen und Virenschutz-Managementprozesse. |

# 7 SiKoSH Phase 4: Allgemeine Musterregelungen

## 7.1 Überblick

→Aktivitätsdiagramm

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

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.2.2.2 Cloud-Nutzung
- OPS.2.2.3 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.

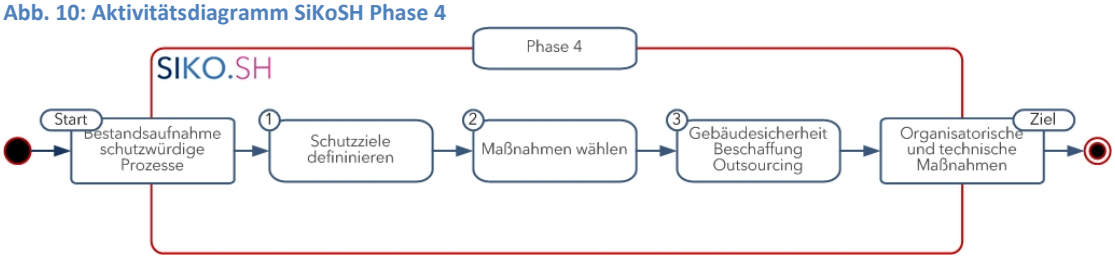
Cloud und Outsourcing

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

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.

→Aktivitätsdiagramm

Tabelle 5: SiKoSH Phase 4 – Übersicht Dokumente

| Titel des Dokuments – Beschreibung |
|---|
| **„QC 4 – Allgemeine Musterregelungen“** [↓.pdf \| .xlsx ]<br>Der Quickcheck 4 (QC 4) behandelt ausgewählte Bausteine aus den Bereichen Konzeption und Vorgehensweise, Betrieb und Infrastruktur. |
| **„Gebäudesicherheit“** [↓.pdf \| .docx ]<br>Die Richtlinie legt grundsätzliche Aspekte der Raum- und Gebäudesicherheit (Einsatz von Sicherheitszonen, Einsatz eines Zutrittskontrollsystems, Raumsicherheit etc.) fest. |
| **„Beschaffung und Entsorgung“** [↓.pdf \| .docx ]<br>Diese Richtlinie dient als Unterstützung bei der Spezifikation der Sicherheitsanforderungen an Informationssysteme im Rahmen von Beschaffungs- und Aussonderungsvorgängen. |
| **„Nutzung von Cloud und Outsourcing“** [↓.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

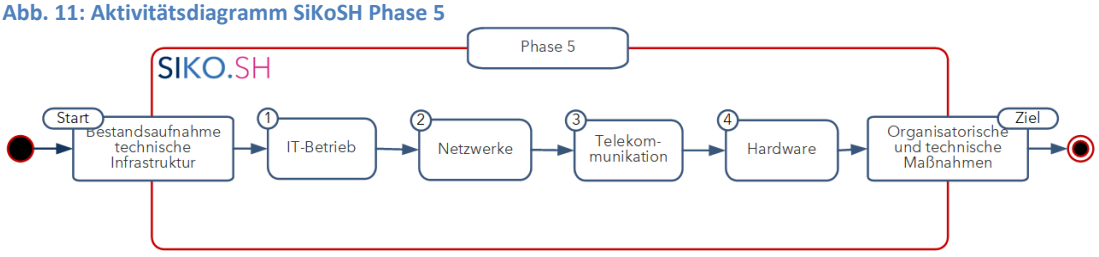
→Aktivitätsdiagram

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

In der SiKoS folgende BSI Grundschutz-Bausteine angewendet:

- OPS.1.1.1 Allgemeiner IT-Betrieb
- OPS.1.1.2 Ordnungsgemäße IT-Administration
- 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

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.

→Aktivitätsdiagramm

Tabelle 6: SiKoSH Phase 5 – Übersicht Dokumente

| Titel des Dokuments – Beschreibung |
|---|
| **„QC 5 – Technische Musterregelungen“** [↓.pdf \| .xlsx ]<br>Der Quickcheck 5 (QC 5) behandelt ausgewählte Bausteine aus den Bereichen Betrieb, Netze und Kommunikation sowie IT-Systeme. |
| **„Client-Sicherheit“** [↓.pdf \| .docx ]<br>Diese Richtlinie behandelt die bestehenden Anforderungen für Planung und Konzeption, Beschaffung und Betrieb von Clients. |
| **„Sicherheit für mobile Endgeräte“** [↓.pdf \| .docx ]<br>Diese Richtlinie behandelt die bestehenden Anforderungen für Planung und Konzeption, Beschaffung und Betrieb von mobilen Endgeräten. |
| **„Betriebshandbuch „Clientmanagement“** [↓.pdf \| .docx ]<br>Diese Vorlage dient zur detaillierten Beschreibung des Clientmanagements. |
| **„IT-Betrieb und IT-Administration“** [↓.pdf \| .docx ]<br>Diese Richtlinie dient der Dokumentation der Aufgaben und Tätigkeiten, die mit dem Betrieb und der Administration von Hard- und Softwarekomponenten vonVerfahren verbunden sind. |
| **„Multifunktionsgeräte“** [↓.pdf \| .docx ]<br>Diese Richtlinie regelt die Einsatzrahmenbedingungen für Multifunktionsgeräte (typischerweise Multifunktionsdrucker). Es umfasst Vorgaben zu Aufstellort und Authentisierung sowie der Administration der Geräte. |
| **„TK, VoIP und Fax“** [↓.pdf \| .docx ]<br>Diese Richtlinie regelt Telekommunikation, Voice over IP und Fax. |
| **„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. |
| **„Netzwerkkomponenten“** [↓.pdf \| .docx ]<br>Diese Richtlinie beschreibt Anforderungen an den Betrieb von Routern, Switches und Firewalls. |
| **„WLAN“** [↓.pdf \| .docx ]<br>Die Richtlinie beschreibt grundsätzliche Anforderungen, die beachtet und erfüllt werden müssen, wenn WLANs aufgebaut und betrieben werden. |

| Titel des Dokuments – Beschreibung |
| --- |
| **„Serversicherheit“** [↓.pdf \| .docx ]<br>Diese Richtlinie behandelt die bestehenden Anforderungen für Planung und Konzeption, Beschaffung und Betrieb von Servern. |

# 9 SiKoSH Phase 6: Regelungen für Verfahren

## 9.1 Überblick

→Aktivitätsdiagramm

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.

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

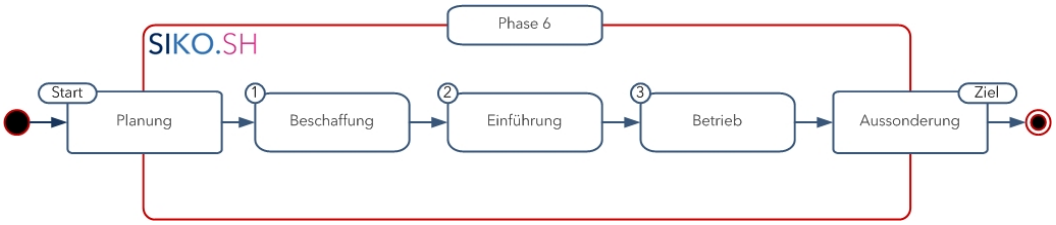
- APP.1.1 Office-Produkte
- APP.1.2 Webbrowser
- APP.2.1 Allgemeiner Verzeichnisdienst
- APP.2.2 Active Directory Domain Services
- APP.3.3 Fileserver
- APP.5.3 Allgemeiner E-Mail-Client und -Server
- APP.6 Allgemeine Software

## 9.2 Iteration – Zuordnung im Lebenszyklus

Fachverfahren

Fachverfahren bzw. IT-Komponenten durchlaufen idealtypisch folgende Lebensphasen:

Abb. 12: Aktivitätsdiagramm SiKoSH Phase 6




## 9.3 Übersicht: Dokumente der SiKoSH Phase 6

→Aktivitätsdiagramm

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.

Tabelle 7: SiKoSH Phase 6 – Übersicht Dokumente

| Titel des Dokuments – Beschreibung |
|---|
| **„QC 6 – Regelungen für Verfahren“** [↓.xlsx ]<br>Der Quickcheck 6 (QC 6) behandelt ausgewählte Anwendungsbau-steine. |
| **„Betriebshandbuch – Verfahren“** [↓.pdf \| .docx ]<br>Dieses BHB dient der Beschreibung von Verfahren. |
| **„Office Produkte und Webbrowser“** [↓.pdf \| .docx ]<br>Diese Richtlinie behandelt Anforderungen an Standardsoftware auf Client-Rechnern. |
| **„Administration von Verzeichnisdiensten“** [↓.pdf \| .docx ] |

| Titel des Dokuments – Beschreibung |
| --- |
| Diese Richtlinie beschreibt grundlegende Regelungen für den sicheren Umgang mit Verzeichnisdiensten |
| **„Fileserver“** [⭳.pdf \| .docx ]<br><br>Diese Richtlinie behandelt Anforderungen für den sicheren Einsatz von Fileservern. |
| **„E-Mail“** [⭳.pdf \| .docx ]<br><br>Diese Richtlinie regelt den Schutz von Informationen, die mit E-Mail-Clients bzw. auf E-Mail-Servern verarbeitet werden. |
| **„Software“** [⭳.pdf \| .docx ]<br><br>Diese Richtlinie regelt Sicherheitsanforderungen, die zu erfüllen sind, damit Softwareverfahren über den gesamten Lebenszyklus hin sicher eingesetzt werden können. |

# 10 SiKoSH Phase 7: Notfallmanagement

## 10.1 Überblick

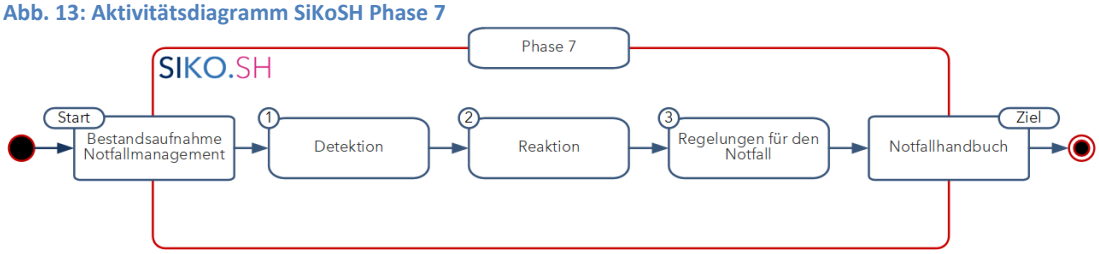
Die Notfallvorsorge wird sinnvollerweise am Ende der Dokumentation eines Fachverfahrens oder anderer IT-Komponenten geplant und umgesetzt.

→Aktivitätsdiagramm

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

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.

→Aktivitätsdiagramm

Tabelle 8: SiKoSH Phase 7 – Übersicht Dokumente

| Titel des Dokuments – Beschreibung |
|---|
| **„QC 7 – Notfallmanagement“** [↓.xlsx ]<br>Der Quickcheck 7 ermöglicht die Dokumentation der Notfallbewältigung in einem Notfallhandbuch. |
| **„Detektion und Reaktion“** [↓.pdf \| .docx ]<br>Diese Richtlinie regelt Anforderungen zur rechtzeitigen Erkennung von sicherheitsrelevanten Ereignissen, zur Behandlung von Sicherheitsvorfällen und zu grundlegenden Vorsorgemaßnahmen im Rahmen der IT-Forensik. |
| **„Notfallhandbuch“** [↓.pdf \| .docx ]<br>Das Notfallhandbuch trifft Regelungen für eine IT-Notfallsituation und hilft den Notfallverantwortlichen im Krisenfall bei einer effektive Krisenbewältigung. |

# 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 erste 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 Abarbeitung Querschnittsprüfung hat das ISMS seine erste Iteration durchlaufen. Die Querschnittsprüfung kann auch im ersten Jahr der Einführung des ISMS z. B. einmal im Quartal neu bearbeitet werden. Idealerweise sollte dann ein deutlicher Fortschritt bei der Umsetzung der Prüfpunkte erkennbar sein.

## 11.2 Übersicht: Dokumente der SiKoSH-Querschnittsprüfung

Tabelle 9zeigt 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 |
|---|
| **„QC QP – Querschnittsprüfung“** [↓.xslx]<br>Der Quickcheck Querschnittsprüfung enthält die wichtigsten Prüfpunkte der Quickchecks der vorangegangen 7 Phasen. Er zeigt somit auf, wo vordringlich noch nachgebessert werden muss. |
| **„Bearbeiten der Quickchecks“** [↓.pdf ]<br>Anleitung zum Umgang mit den SiKoSH Quickchecks |

# 12 Sicherheitskonzept

## 12.1 Was mit SiKoSH erreicht wird

Kommunale Basisabsicherung

Wenn alle Phasen mit ihren im kommunalen Grundschutzprofil bzw. in den SiKoSH-Quickchecks aufgeführten kommunalen Basisanforderungen bearbeitet sind, hat SiKoSH sein Projektziel „kommunale Basisabsicherung“ 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 Standardabsicherung 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-Standards bereits hohe fachliche Anforderungen. Der Einsatz eines Werkzeugs zur Unterstützung wird empfohlen[16]

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[17]

## 12.3 IT-Strukturanalyse

→Aktivitätsdiagramm

Im Grundschutzprofil Basisabsicherung 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 Allgemeinen sinnvoll, zuerst die produktiven Anwendungen und Daten zu ermitteln.

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

[17] 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/)

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 Basisanforderungen

Aus der durchgeführten IT-Strukturanalyse können die BSI-Bausteine ermittelt werden, die bisher noch nicht berücksichtigt worden sind. In der Hauptsache geht es darum, noch fehlende Basisanforderungen 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 Basisanforderungen auch die in den BSI-Bausteinen aufgeführten Standardanforderungen.

Einige Standardanforderungen gehören bereits zum Grundschutzprofil Basisabsicherung 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[18].

## 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.

Die Schutzbedarfsfeststellung ist Grundlage für die Umsetzung des Datenschutzrechts

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

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

### 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 Standardabsicherung 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 Index

Awareness ..... 27
Basisabsicherung ..... 13
  BSI ..... 13
  Testat ..... 13
Basis-Absicherung ..... 8
BSI IT-Grundschutz ..... 12
Do-it-Yourself ISMS ..... 12, 16
Fachverfahren
  Lebensphasen ..... 37
Gemba ..... 18
Grundschutzprofil
  kommunales ..... 13
Informationssicherheit
  Lernkontinuum ..... 27
Informationssicherheitsleitlinie ..... 22
ISMS
  Bestandteile ..... 7
ISO/IEC 27001 ..... 12
Lernkontinuum Informationssicherheit ..... 27
Organisationsverantwortung ..... 11
Outsourcing von IT-Dienstleistungen ..... 32
Pareto-Prinzip ..... 22
PDCA-Methode ..... 18
PDCA-Zyklus ..... 10
Querschnittsprüfung ..... 8, 40
Quick Win ..... 16, 19
Rechnungshöfe des Bundes und der Länder
  Mindestanforderungen ..... 11
Risikoakzeptanz ..... 43
Risikoreduktion ..... 43
Risikotransfer ..... 43
Risikovermeidung ..... 43
Selbstauditierung ..... 8, 9, 18
Sensibilisierung ..... 27
Sicherheitskonzept ..... 41
Sicherheitskultur ..... 14
Training ..... 27
Vorgehen
  hierarchisch-analytisches ..... 14
Vorgehensmodell
  vereinfachtes ..... 12

## 13.2 Glossar

Das vollständige SiKoSH Glossar gibt es bei https://www.sikosh.de/sikosh-glossar