

20.05.2025 ISMS – Aller Anfang ist leicht: Der geregelte Einstieg in ein professionelles Informationssicherheitsmanagement



Ein wenig Geschichte

Frank Weidemann | Projektleiter

Die Ausgangslage oder der „Schmerz“ 2015

- Fehlende oder lückenhafte Dokumentation der kommunalen Informationssicherheit
- Sicherheitsvorfälle
- Gesetzliche Dokumentationspflichten wie z. B. Fachrecht, DSGVO, Leitlinie des IT-PLR

Die Ausgangslage oder der „Schmerz“ heute

- Fehlende oder lückenhafte Dokumentation der kommunalen Informationssicherheit
- Aktuelle Sicherheitsvorfälle und eine verschärfte IT-Sicherheitslage
- Gesetzliche Dokumentationspflichten wie z. B. Fachrecht, DSGVO, Leitlinie IT-PLR, OZG, NIS 2.0

Grundlagen

Frank Weidemann | Projektleiter

Was ist eigentlich Informationssicherheit?

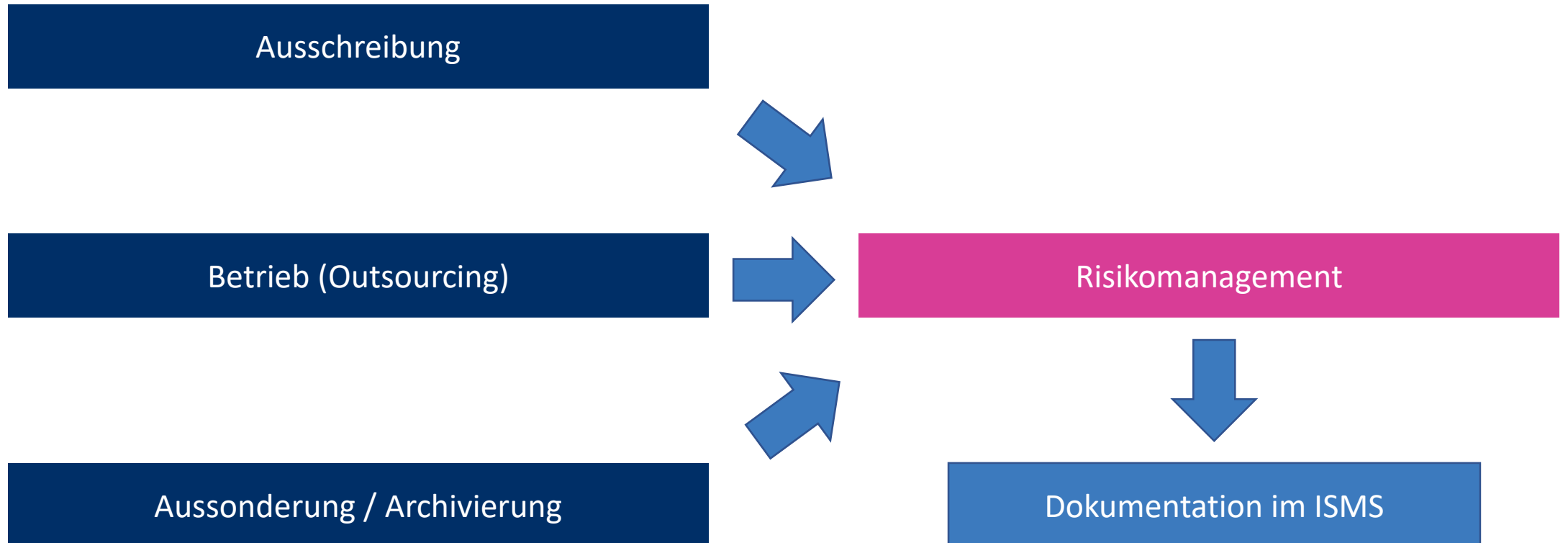
- Sicherstellung der **Schutzziele**
 - **Vertraulichkeit** (Datenschutz!)
 - **Verfügbarkeit** (SLA)
 - **und Integrität** (Schutz vor Manipulation) sicherstellen soll.
- Effektives **Risikomanagement**
 - Ziel ist die Minimierung der Restrisiken (Schadenshöhe*Eintrittswahrscheinlichkeit) auf ein vertretbares Maß (Risikoakzeptanz).

IT-Sicherheitsvorfälle in Kommunalverwaltungen



Quelle: <https://kommunaler-notbetrieb.de/uebersichtskarte>

Wie schütze ich mich vor unakzeptablen Risiken?



Risikovermeidung

Risiko reduzieren (Maßnahmen, TOMs)



Risikotransfer (Cyberversicherung)



Restrisiko akzeptieren



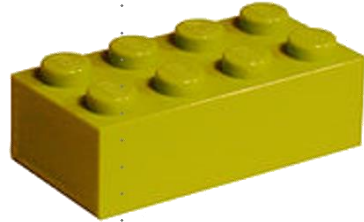
Quelle: BSI

Und was ist ein ISMS?

- Ein ISMS dient der Dokumentation
 - Der Aufbauorganisation (Rollenträger),
 - Der Ablauforganisation (Prozesse/Verfahren) und
 - Des Regelwerks (v.a. der technischen und organisatorischen Maßnahmen zur Risikominimierung)

SiKoSH

Frank Weidemann | Projektleiter



Die **BSI-IT-Grundschutzbausteine** definieren Anforderungen an die Informationssicherheit.



Das **IT-Grundschutzprofil „Basis-Absicherung Kommunalverwaltung“** wählt die für kommunale Einrichtungen nötigen Bausteine und kommunalen Basisanforderungen aus.



Die **SiKoSH-Methodik** setzt die kommunalen Basisanforderungen der ausgewählten Bausteine effizient, praxisorientiert und wirksam um.

- Warum SiKoSH? Ich muss IT-Grundschutz machen.

INSTITUT FÜR INFORMATIK
DER LUDWIG-MAXIMILIANS-UNIVERSITÄT MÜNCHEN



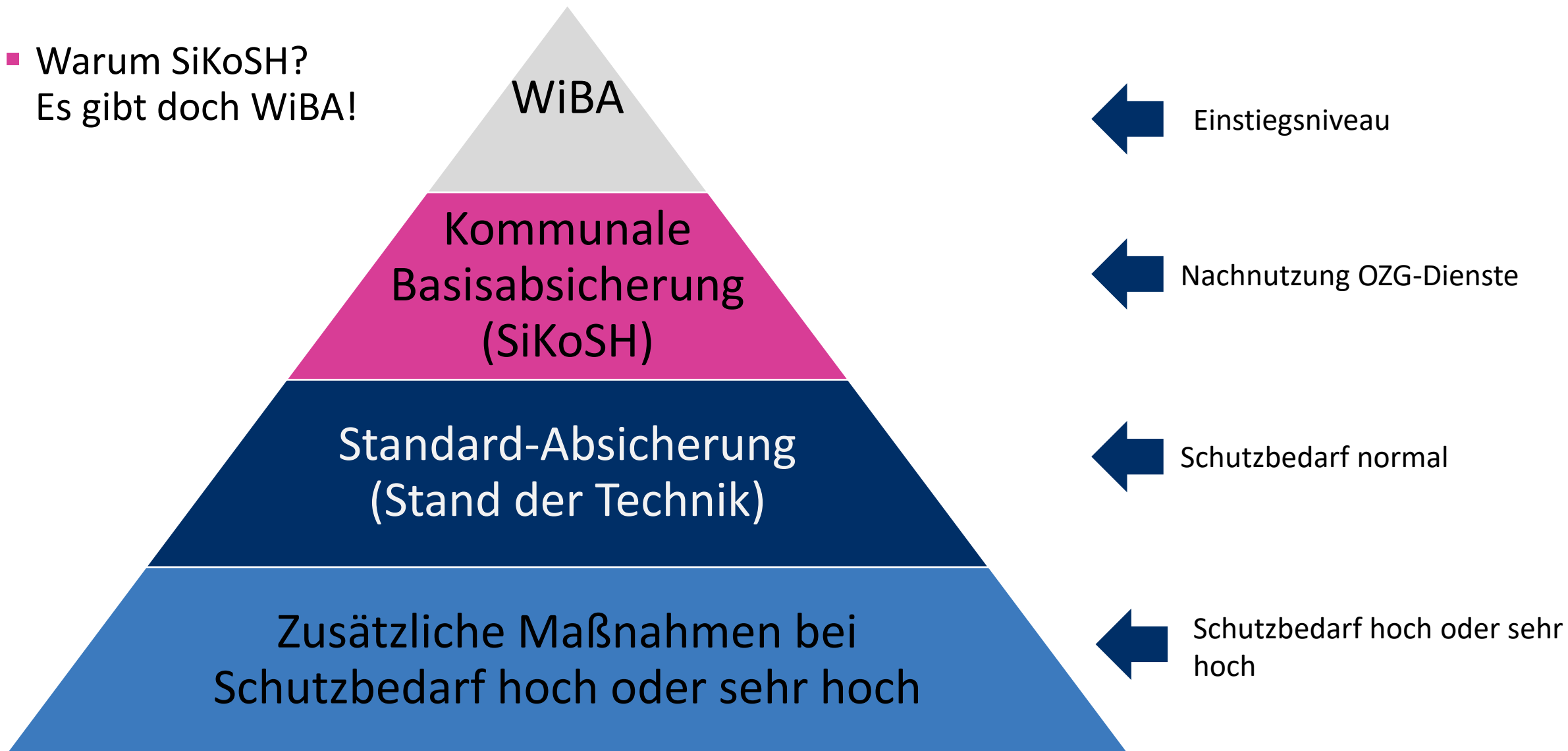
Bachelorarbeit

Vergleich zweier Frameworks für
Informationssicherheits-
managementsysteme
in kommunalen Einrichtungen

Maximilian Wiegand

Der Faktencheck

- Warum SiKoSH?
Es gibt doch WiBA!

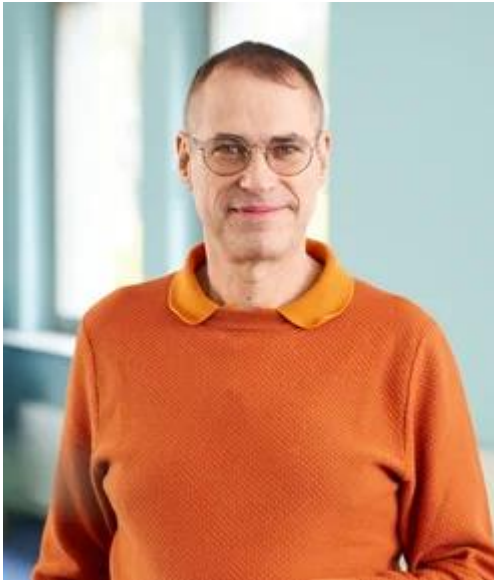


- IT-Grundschutz ist doch gar nicht vorgeschrieben!
 - DSGVO (Art. 32 - TOMs)
 - OZG (§ 5 – Mindestsicherheitsstandards im Portalverbund)
 - IT-Sicherheitsgesetz (KRITIS)
 - Fachrecht (z. B. BMG)
 - Grundsatz der Ordnungsmäßigkeit der Verwaltung

- Ein ISMS aufzubauen ist viel zu kompliziert!

SiKoSH

- ist einfaches Einstiegsframework – speziell für kommunale Anwender
- führt wie ein Kochbuch durch die ISMS Umsetzungsphasen
- hat wie ein Kochbuch viele Hilfsmittel, zusätzliche Anleitungen und Vorlagen
- beinhaltet konkrete Handlungs-Anweisungen zur Gewährleistung von Informationssicherheit und Datenschutz
- Berücksichtigt die Bedingungen des kommunalen Arbeitsalltags



Frank Weidemann

Projektleitung SiKoSH

Frank.weidemann@itvsh.de

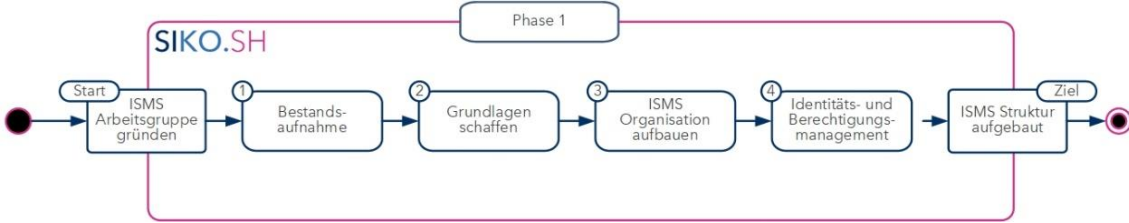
SIKO.SH
Sicherheit für Kommunen



ISMS – Aller Anfang ist leicht: Der geregelte Einstieg in ein professionelles Informationssicherheitsmanagement

Part II: Workshop SiKoSH-Phase 1

Aus der Praxis für die Praxis. Informationssicherheit ist Gemeinschaftsaufgabe.



Agenda

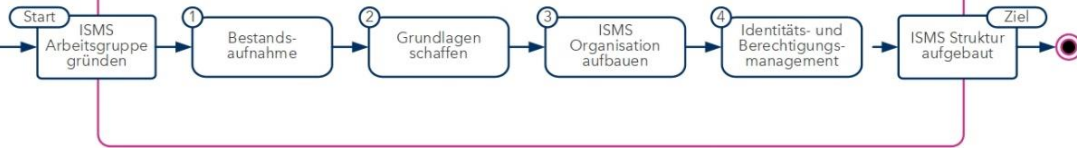
- Kick-off SiKoSH
- Start: Bildung der temporären Arbeitsgruppe
- Bestandsaufnahme
- Grundlagen schaffen
- ISMS Organisation aufbauen
- Identitäts- und Berechtigungsmanagement
- Ziel: ISMS Struktur aufgebaut

Organisatorisches:

- Information zu Räumlichkeiten
- Pausen
- Mittagszeit (12:00 - 12:45 Uhr)
- Fragen jederzeit willkommen und gewünscht
- Falls zu tiefgehende/abschweifende Diskussion entsteht, möchten wir ein Signal ausmachen um mit dem geplanten Programm fortzufahren.

Wer bin ich?





Kickoff SiKoSH - FAQ:

- Wo fange ich an?
- Wie erhalte ich die Dokumente?
- Welche Dokumente gibt es?
- Wie sind die Dokumente strukturiert?
- Mit welchem Dokument fange ich an?
- Wen kann ich benachrichtigen, wenn ich Fragen oder Anmerkungen habe?

ITV.SH | Wir sind | Was wir tun | Infotext | News | Events | OZG-Shop | EA.SH | EN | Q

Informationssicherheit

Home → Was wir tun → Wir beraten → Informationssicherheit

Wir beraten

- Digitaler Ankerung
- Informationssicherheit**
- SiKoSH Glossar
- Schulträgerberatung

SiKoSH Standard

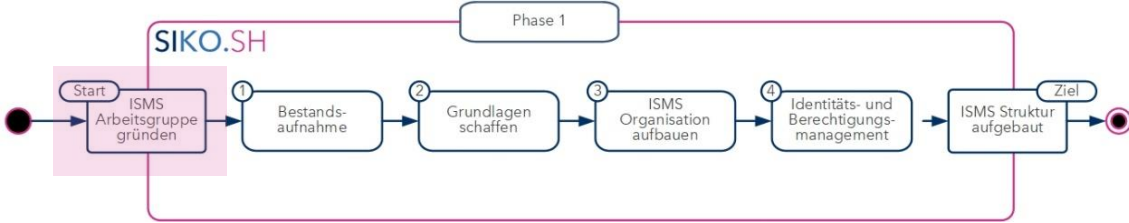
SiKoSH Standard (PDF, 1 MB)

SiKoSH - Das IT-Sicherheitskonzept für Schleswig-Holstein

SiKoSH (Sicherheit für Kommunen in Schleswig-Holstein) hilft beim Aufbau eines professionellen Informations-Sicherheits-Managements-Systems auf der Grundlage des BSI-Grundschutzprofils „Basisabsicherung Kommunalverwaltung“ und legt den Fokus auf die Anforderungen, die aus kommunaler Sicht primär umgesetzt werden müssen. SiKoSH liefert dabei nicht nur den Fahrplan für den Aufbau des ISMS, sondern auch zahlreiche Richtlinien und viele Hilfsmittel, die an die örtlichen Gegebenheiten angepasst werden. Die erforderliche Sicherheitsdokumentation entsteht dabei wie von selbst.

Basisabsicherung mit SiKoSH - praxisorientiert und kostenfrei!

SiKoSH ist ein ISMS-Framework, das durch den IT-Verbund Schleswig-Holstein (ITV.SH)



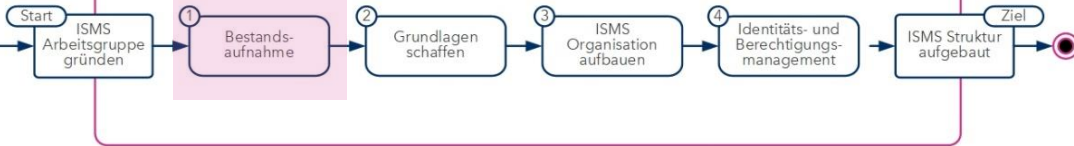
ISMS Arbeitsgruppe gründen



- Teilnehmende bilden gemeinsam die ISMS Arbeitsgruppe

FAQ

- Welche Rollen benötige ich für den Start eines ISMS?
- Wie groß sollte die Arbeitsgruppe sein?



Bestandsaufnahme

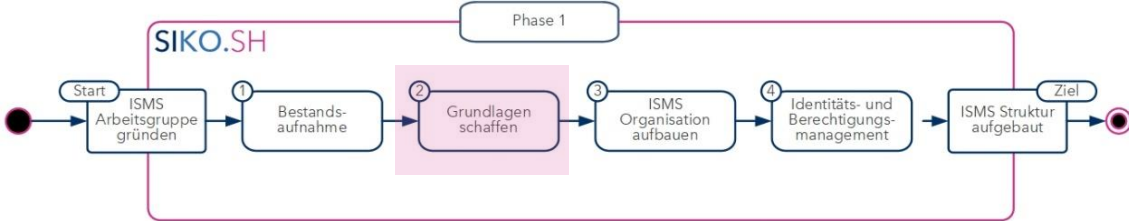
- Durchführen Quickcheck 1

FAQ

- Welche (SiKoSH) Hilfsmittel kann ich nutzen?
- Wen muss ich befragen?
- Muss ich meine Ergebnisse dokumentieren?
- Kann ich auf bereits vorhandene Regelungen verweisen?
- Reicht es aus, wenn die Anforderungen geregelt sind?

Informationssicherheit / ISMS						Priorität	Status	Bewertung	SiKoSH-Hilfsmittel
ISID	ISID Klasse	Prüf-Prüfpunkte							
1 Sind Formale und Verantwortlichkeiten geregelt?									
ISMS1A1	11	Die Behörde/Instanz hat die Gesamtverantwortung für Informationssicherheit deutlich erkennbar für alle Beteiligten übernommen. Die Behörde/Instanz hat den Informationssicherheitsprozess vor, in dem Sie ihn initiiert, steuert und überwacht, festgelegt.	Hoch	Unbeantwortet	0	Informationssicherheit für die Behörde/Instanz			
	12	Für alle Zuständigkeitsbereiche sind Verantwortliche definiert, die mit den erforderlichen Kompetenzen und Ressourcen ausgestattet werden.	Normal	Unbeantwortet	0	Betriebshandbuch - allgemeine Teil			
	13	Die Behörde/Instanz lässt sich regelmäßig über den Stand der Informationssicherheit und hier insbesondere über mögliche Risiken informieren.	Normal	Unbeantwortet	0	ISMS-Betrieb			
ISMS1A2	14	Die Behörde/Instanz hat den Sicherheitsprozess initiiert und etabliert. Hierzu hat sie angemessene Sicherheitsziele sowie eine Strategie für Informationssicherheit festgelegt und dokumentiert.	Hoch	Unbeantwortet	0	Informationssicherheitsleitlinie			
	15	Es wurden konkrete Vorgaben erarbeitet und geeignete Rahmenbedingungen geschaffen, um den ordnungsgemäßen und sicheren Umgang mit Informationen innerhalb aller Fachaufgaben der Behörde zu ermöglichen.	Hoch	Unbeantwortet	0				
	16	Die Sicherheitsziele und Strategien der Behörde werden von der Behörde/Instanz verantwortet und regelmäßig auf Aktualität und Angemessenheit hin überprüft.	Normal	Unbeantwortet	0				
ISMS1A3	16	Eine Informationssicherheitsleitlinie wurde erstellt und durch die Behörde/Instanz genehmigt und in Kraft gesetzt.	Hoch	Unbeantwortet	0	Informationssicherheitsleitlinie			
	17	Die Informationssicherheitsleitlinie beschreibt den Stellenwert der Informationssicherheit, die Sicherheitsziele, die wichtigsten Aspekte der Sicherheitsstrategie sowie die Organisationsstruktur für Informationssicherheit. Ein klarer Geltungsbereich ist festgelegt. Die Sicherheitsziele und der Bezug der Sicherheitsziele zu den Aufgaben der Behörde/Instanz sind festgelegt. Die Informationssicherheitsleitlinie ist allen Mitarbeitenden bekannt und wird regelmäßig aktualisiert.	Normal	Unbeantwortet	0				
	18		Normal	Unbeantwortet	0				
2 Sind adäquate Prozesse und Strukturen geschaffen?									
ISMS1A4	2.1	Es wurde eine Normative Informationssicherheitsbeauftragter (ISB) formal bestellt zur Förderung der Informationssicherheit in der Institution und Mitsteuerung des Sicherheitsprozesses.	Hoch	Unbeantwortet	0	Bestellung eines ISB			
	2.2	Die oder der ISB ist mit angemessenen Ressourcen ausgestattet und kann bei Bedarf direkt Bericht an die Behörde/Instanz einbringen.	Normal	Unbeantwortet	0				
ISMS1A5	2.4	Die oder der ISB wird bei allen größeren Projekten sowie bei der Einführung neuer Anwendungen und IT-Systeme einbezogen.	Hoch	Unbeantwortet	0				
	2.4	Sollte ein externer IT-Sicherheitsbeauftragter bestellt worden sein, ist eine geeignete Vertragsgestaltung (Pflichten, Haftung, Verantwortlichkeit, Kündigung) vorgenommen worden.	Hoch	Unbeantwortet	0				
ISMS1A6	2.5	Es wurde eine eigene Organisationsstruktur für die Informationssicherheit bzw. ein Informationssicherheitsamt gebildet. Rollen und Aufgaben sind klar definiert, ausreichend Personalausstattung ist zur Verfügung.	Normal	Unbeantwortet	0	ISMS-Organisation			
	2.6	Kommunikations- und Informationspflichten innerhalb des Informationssicherheitsamtes sind beschrieben.	Normal	Unbeantwortet	0				
	2.7	Die Aktualität der Organisationsstruktur für Informationssicherheit wird regelmäßig geprüft.	Normal	Unbeantwortet	0				
3 Ist der Sicherheitsprozess in der Organisation verankert?									
ISMS1A7	3.1	Für die gesamte Informationsverarbeitung sind ausführliche und angemessene Sicherheitsmaßnahmen festgelegt und dokumentiert.	Hoch	Unbeantwortet	0	ISMS-Betrieb			
	3.2	Die Sicherheitsmaßnahmen zur Informationsverarbeitung werden in Sicherheitskonzepten dokumentiert und regelmäßig aktualisiert.	Normal	Unbeantwortet	0	Quickcheck 2			
ISMS1A8	3.3	Alle Mitarbeitenden werden in Themen der Informationssicherheit miteinbezogen und regelmäßig über Gefährdungen und Sicherheitsmaßnahmen informiert.	Hoch	Unbeantwortet	0	SIKO.SH Phase 2			
	3.4	Alle Mitarbeitenden sind in der Lage (z. B. durch Schulungen) Sicherheit aktiv mitzugestalten.	Normal	Unbeantwortet	0				
	3.5	Sicherheitsrichtlinien und dazugehörige Regelungen werden zielgruppenspezifisch erstellt und in geeigneter Weise bekanntgegeben.	Normal	Unbeantwortet	0				
	3.6	Die Mitarbeitenden sind sich der Konsequenzen bei Verletzung der Sicherheitsvorgaben bewusst.	Normal	Unbeantwortet	0				
ISMS1A9	3.7	Die Informationssicherheit ist in alle Entscheidungsprozesse sowie in Entscheidungen integriert.	Hoch	Unbeantwortet	0				
	3.8	Es ist sichergestellt, dass das Informationsrisikomanagement Einfluss auf alle relevanten Entscheidungen und Prozesse einer Institution nehmen kann.	Normal	Unbeantwortet	0	ISMS-Organisation			
	3.9	Eine Abstimmung der Arbeitsteilung untereinander in Sachen Sicherheit und Risikomanagement ist sichergestellt.	Niedrig	Unbeantwortet	0				

Informationssicherheit / ISMS						eigene Umsetzung			SiKoSH	
ISID	Prüfpunkte	Prüf-Prüfpunkte	Status	Reaktion	Verantwortlich/Ansprechperson	Verantwortlich/Ansprechperson	Maßnahmen/Anforderungen	SiKoSH-Hilfsmittel		
ISMS 1.001 (TA1-TA4)	11	Die Behörde/Instanz hat die Gesamtverantwortung für Informationssicherheit deutlich erkennbar für alle Beteiligten übernommen. Die Behörde/Instanz hat den Informationssicherheitsprozess vor, in dem Sie ihn initiiert, steuert und überwacht, festgelegt.	Nach	Unbeantwortet			Maßnahme: Zielsetzung: Die Behörde/Instanz hat die Gesamtverantwortung für Informationssicherheit deutlich erkennbar für alle Beteiligten übernommen. Die Behörde/Instanz hat den Informationssicherheitsprozess vor, in dem Sie ihn initiiert, steuert und überwacht, festgelegt.	SiKoSH-Hilfsmittel: Informationssicherheit für die Behörde/Instanz		
ISMS 1.002 (TA1)	12	Für alle Zuständigkeitsbereiche sind Verantwortliche definiert, die mit den erforderlichen Kompetenzen und Ressourcen ausgestattet werden.	Normal	Unbeantwortet			Maßnahme: Zielsetzung: Für alle Zuständigkeitsbereiche sind Verantwortliche definiert, die mit den erforderlichen Kompetenzen und Ressourcen ausgestattet werden.	SiKoSH-Hilfsmittel: Informationssicherheit für die Behörde/Instanz		
ISMS 1.003 (TA1)	13	Die Behörde/Instanz lässt sich regelmäßig über den Stand der Informationssicherheit und hier insbesondere über mögliche Risiken informieren.	Normal	Unbeantwortet			Maßnahme: Zielsetzung: Die Behörde/Instanz lässt sich regelmäßig über den Stand der Informationssicherheit und hier insbesondere über mögliche Risiken informieren.	SiKoSH-Hilfsmittel: Informationssicherheit für die Behörde/Instanz		
ISMS 1.004 (TA1)	14	Die Behörde/Instanz hat den Sicherheitsprozess initiiert und etabliert. Hierzu hat sie angemessene Sicherheitsziele sowie eine Strategie für Informationssicherheit festgelegt und dokumentiert.	Nach	Unbeantwortet			Maßnahme: Zielsetzung: Die Behörde/Instanz hat den Sicherheitsprozess initiiert und etabliert. Hierzu hat sie angemessene Sicherheitsziele sowie eine Strategie für Informationssicherheit festgelegt und dokumentiert.	SiKoSH-Hilfsmittel: Informationssicherheit für die Behörde/Instanz		
ISMS 1.005 (TA1)	15	Es wurden konkrete Vorgaben erarbeitet und geeignete Rahmenbedingungen geschaffen, um den ordnungsgemäßen und sicheren Umgang mit Informationen innerhalb aller Fachaufgaben der Behörde zu ermöglichen.	Nach	Unbeantwortet			Maßnahme: Zielsetzung: Es wurden konkrete Vorgaben erarbeitet und geeignete Rahmenbedingungen geschaffen, um den ordnungsgemäßen und sicheren Umgang mit Informationen innerhalb aller Fachaufgaben der Behörde zu ermöglichen.	SiKoSH-Hilfsmittel: Informationssicherheit für die Behörde/Instanz		
ISMS 1.006 (TA1)	16	Die Sicherheitsziele und Strategien der Behörde werden von der Behörde/Instanz verantwortet und regelmäßig auf Aktualität und Angemessenheit hin überprüft.	Normal	Unbeantwortet			Maßnahme: Zielsetzung: Die Sicherheitsziele und Strategien der Behörde werden von der Behörde/Instanz verantwortet und regelmäßig auf Aktualität und Angemessenheit hin überprüft.	SiKoSH-Hilfsmittel: Informationssicherheit für die Behörde/Instanz		
ISMS 1.007 (TA1)	17	Eine Informationssicherheitsleitlinie wurde erstellt und durch die Behörde/Instanz genehmigt und in Kraft gesetzt.	Nach	Unbeantwortet			Maßnahme: Zielsetzung: Eine Informationssicherheitsleitlinie wurde erstellt und durch die Behörde/Instanz genehmigt und in Kraft gesetzt.	SiKoSH-Hilfsmittel: Informationssicherheitsleitlinie		
ISMS 1.008 (TA1)	18	Die Informationssicherheitsleitlinie beschreibt den Stellenwert der Informationssicherheit, die Sicherheitsziele, die wichtigsten Aspekte der Sicherheitsstrategie sowie die Organisationsstruktur für Informationssicherheit. Ein klarer Geltungsbereich ist festgelegt. Die Sicherheitsziele und der Bezug der Sicherheitsziele zu den Aufgaben der Behörde/Instanz sind festgelegt. Die Informationssicherheitsleitlinie ist allen Mitarbeitenden bekannt und wird regelmäßig aktualisiert.	Normal	Unbeantwortet			Maßnahme: Zielsetzung: Die Informationssicherheitsleitlinie beschreibt den Stellenwert der Informationssicherheit, die Sicherheitsziele, die wichtigsten Aspekte der Sicherheitsstrategie sowie die Organisationsstruktur für Informationssicherheit. Ein klarer Geltungsbereich ist festgelegt. Die Sicherheitsziele und der Bezug der Sicherheitsziele zu den Aufgaben der Behörde/Instanz sind festgelegt. Die Informationssicherheitsleitlinie ist allen Mitarbeitenden bekannt und wird regelmäßig aktualisiert.	SiKoSH-Hilfsmittel: Informationssicherheitsleitlinie		

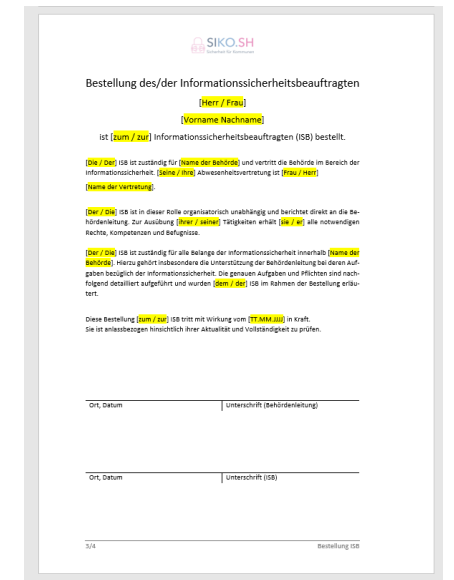
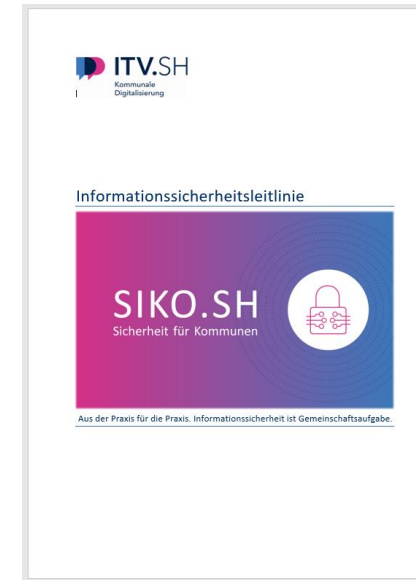


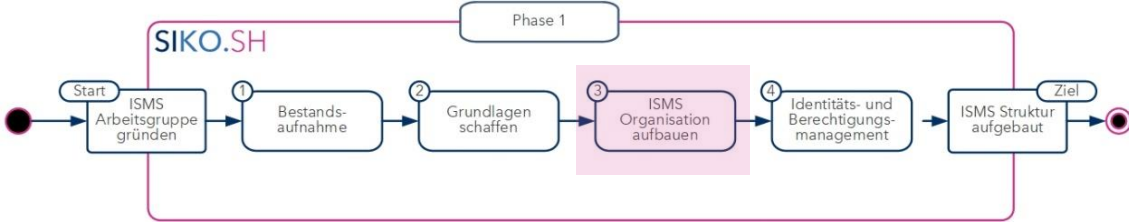
Grundlagen schaffen:

- Rückendeckung der Behördenleitung (Informationssicherheit_fuer_Behoerdenleitungen)
- Leitlinie
- Bestellung ISB

FAQ

- Welche (SiKoSH) Hilfsmittel kann ich nutzen?
- Warum ist es so wichtig die Informationssicherheit so hoch aufzuhängen?
- Welche Aufgaben hat ein ISB?





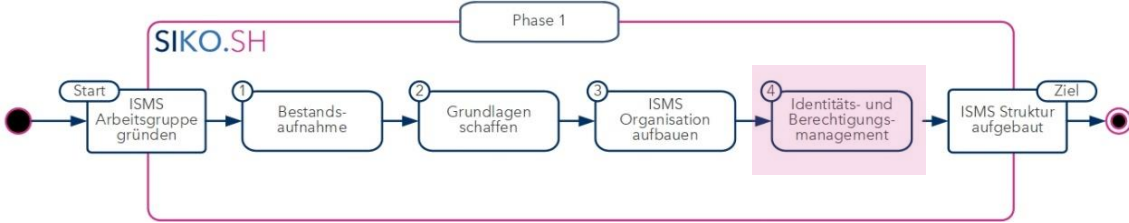
ISMS Organisation aufbauen:

- Aufbauorganisation: Richtlinie ISMS-Organisation
- Ablauforganisation: Richtlinie ISMS-Betrieb
- Vorlage: Melden von Sicherheitsvorfällen

FAQ

- Welche Rollen werden benötigt und was muss dabei beachtet werden?
- Wo werden Verantwortlichkeiten und Aufgaben dokumentiert?
- Welche Aufgaben müssen kontinuierlich bearbeitet werden?
- Welche Prozesse müssen dafür etabliert werden?





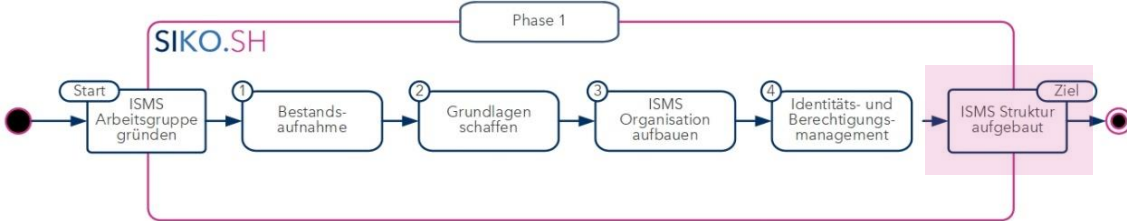
Identitäts- und Berechtigungsmanagement:

- Richtlinie „Identitäts- und Berechtigungsmanagement“

FAQ

- Welche Vorgaben zur Authentisierung sind notwendig?
- Wie soll der Prozess zur Berechtigungsvergabe aussehen?
- Wo und von wem müssen die Vorgaben eingehalten werden?



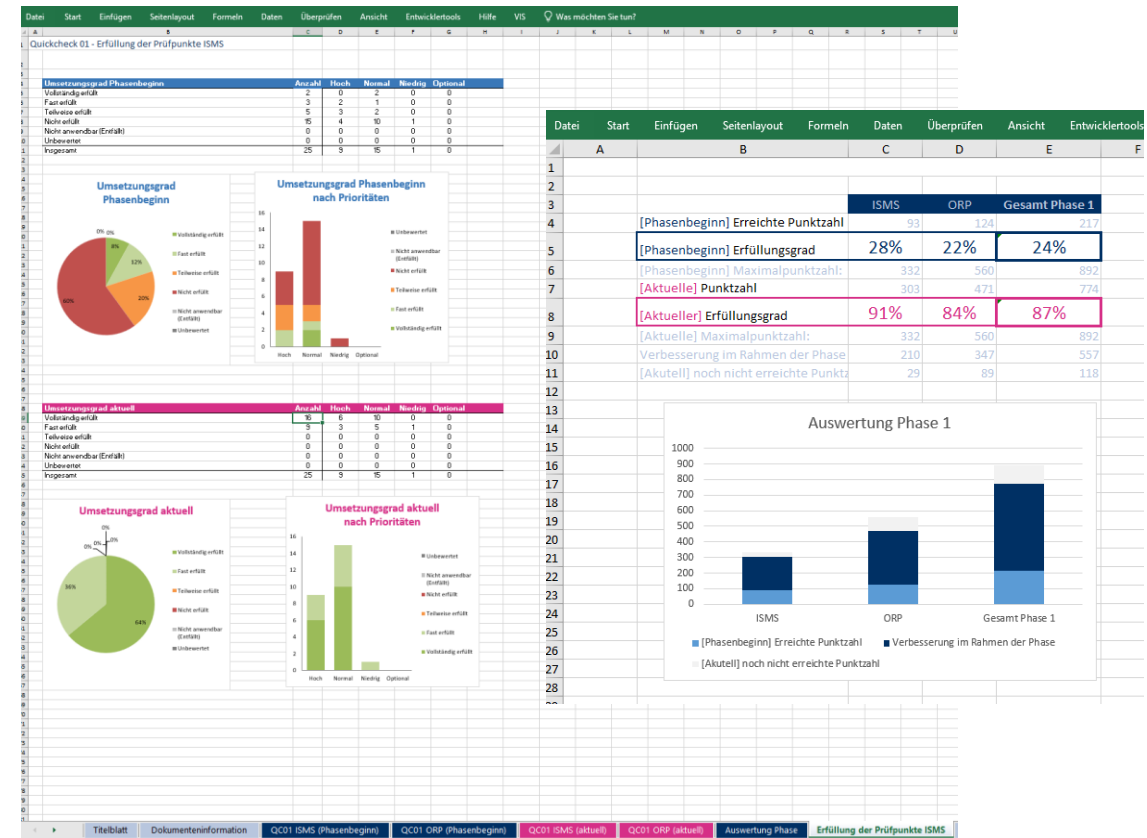


ISMS Struktur aufgebaut:

- Auswertung der abgehakten Punkte im Quickcheck
- Nächste Schritte: Übergang in Phase 2

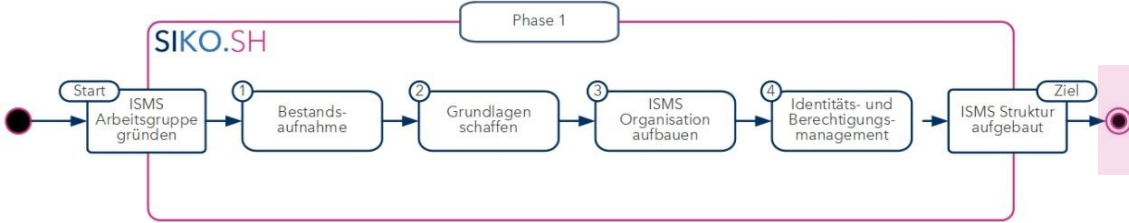
FAQ

- Wann ist es sinnvoll in die Phase 2 zu starten?



FAQ

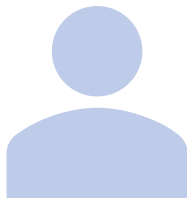
- Was habe ich selbst anpassen müssen?
- Was war nicht verständlich?



Abschluss:

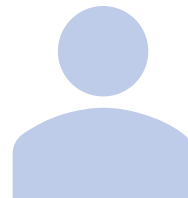
- War der Inhalt des Workshops hilfreich?
- Welche Hilfsmittel von SiKoSH sind besonders nützlich?
- Wo fehlen noch weitere Hilfsmittel?

Vielen Dank für die Teilnahme am Workshop



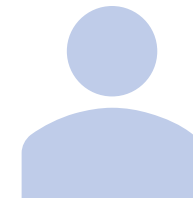
Andreas Haase

IT-Sicherheitsberater
Dataport



Lutz Seemann

IT-Sicherheitsberater
Dataport



Frank Weidemann

PL SiKoSH
ITV.SH