

22.05.2025 SiKoSH – Vorstellung der
Workshopergebnisse

ISMS - Aller Anfang ist leicht: Der geregelte
Einstieg in ein professionelles Informations-
sicherheitsmanagement



Zusammenfassung der Workshopergebnisse

Die Ausgangslage und 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

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).

Zusammenfassung der Workshopergebnisse

Risiko: Die Bedrohungslage

IT-Sicherheitsvorfälle in Kommunalverwaltungen



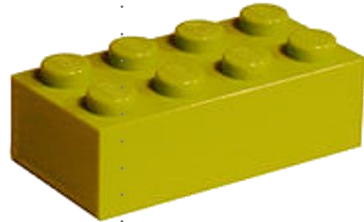
Quelle: <https://kommunaler-notbetrieb.de/uebersichtskarte>

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)

- > Warum hat nicht jede Behörde ein ISMS?
 - Komplex
 - Arbeitsalltag frisst einen auf
 - Ressourcen fehlen, der Verantwortliche für den Aufbau eines ISMS

Wer hilft dem ISB? SiKoSH



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



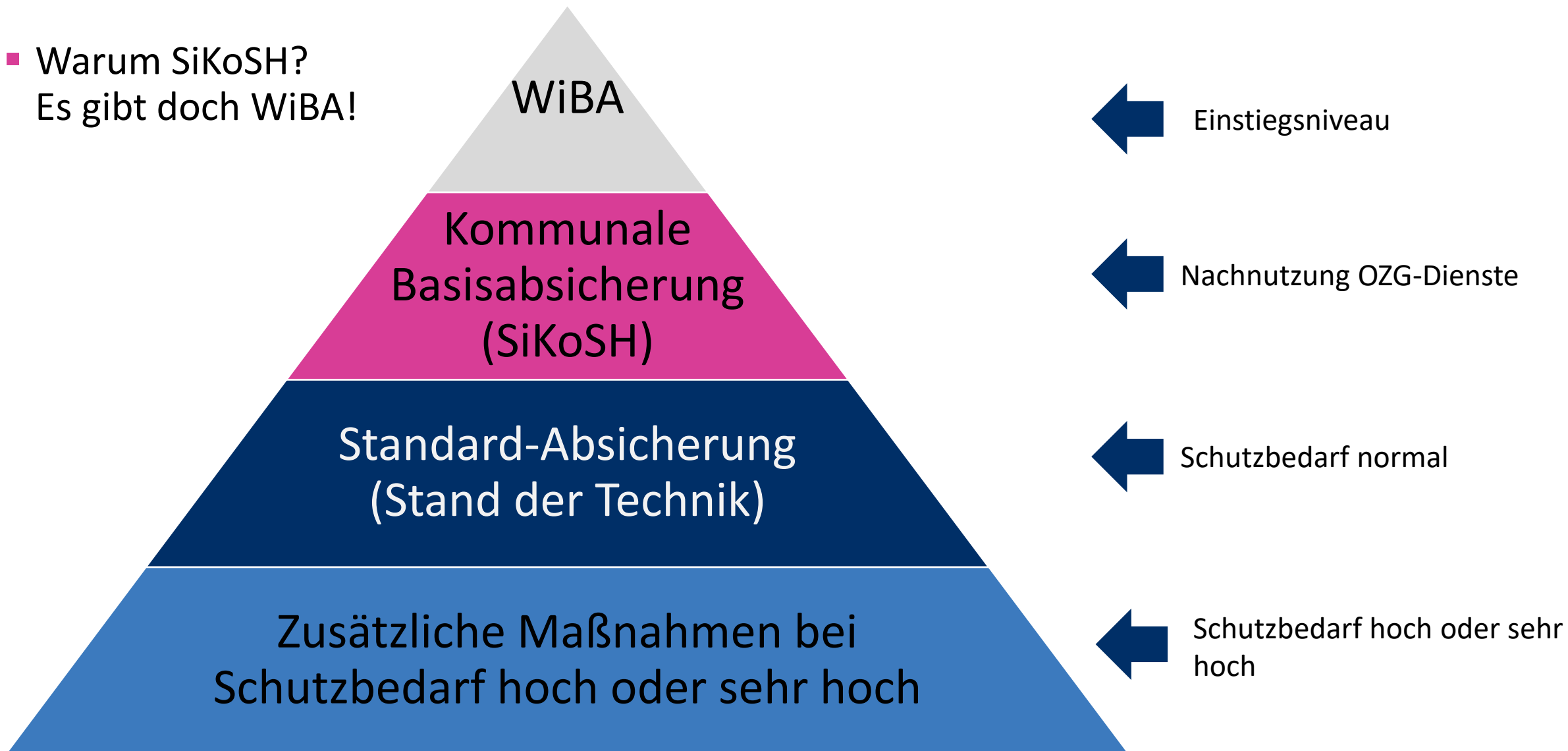
Das **IT-Grundschutzprofil „Basis-Absicherung Kommunalverwaltung“** wählt die für kommunale Einrichtungen nötigen Bausteine und kommunalen Basisanforderungen aus.



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

Der Faktencheck

- Warum SiKoSH?
Es gibt doch WiBA!



- 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

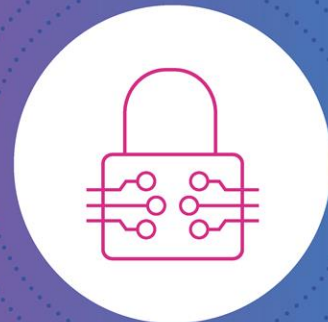


Standard:
Einführung und Betrieb eines Informations-
Sicherheits-Management-Systems (ISMS)



Aus der Praxis für die Praxis. Informationssicherheit ist Gemeinschaftsaufgabe.

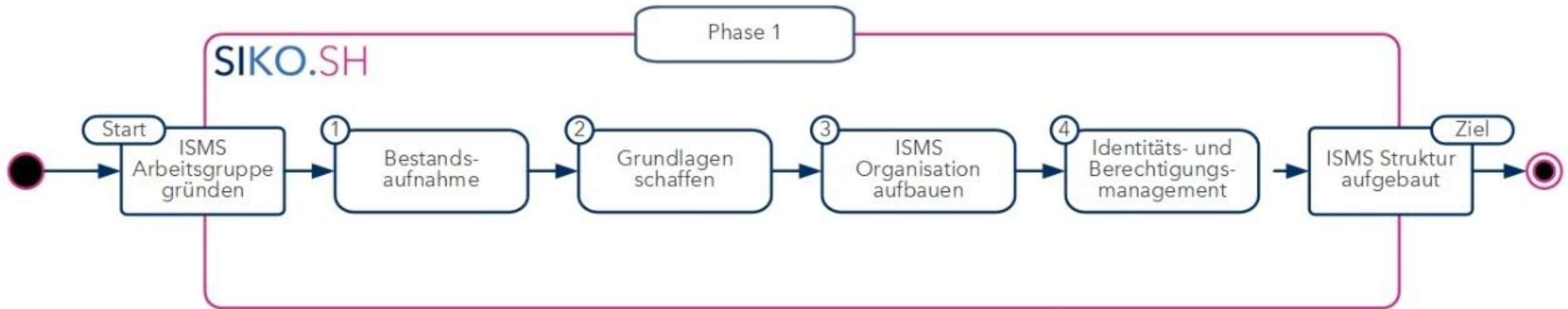
SIKO.SH
Sicherheit für Kommunen

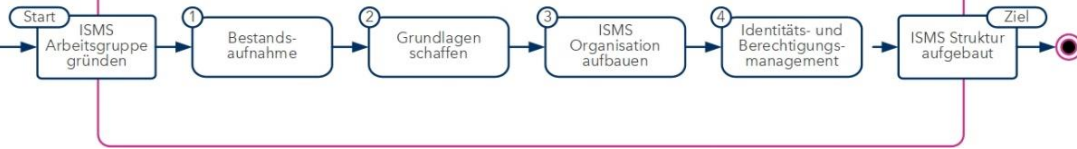


ISMS – Aller Anfang ist leicht: Der geregelte
Einstieg in ein professionelles
Informationssicherheitsmanagement

Part II: Workshop SiKoSH-Phase 1

Aus der Praxis für die Praxis. Informationssicherheit ist Gemeinschaftsaufgabe.

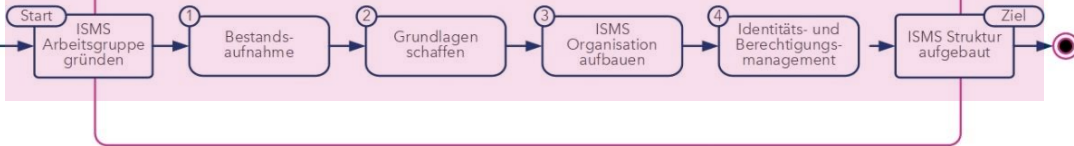




Wie fange ich an?

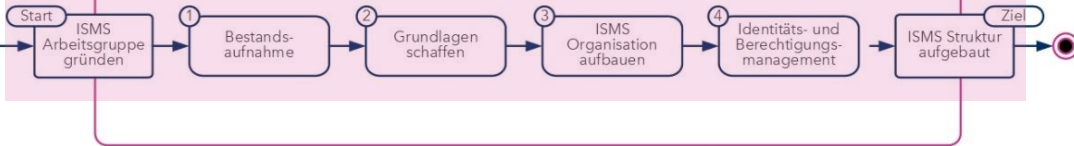
- Wo fange ich an?
- Wie erhalte ich die Dokumente?
- Welche Dokumente gibt es?
- Wie sind die Dokumente strukturiert?
- Mit welchem Dokument fange ich an?
- Wen kann ich benachrichtigen, wenn ich Fragen oder Anmerkungen habe?

Einstieg über www.sikosh.de und den dort erreichbaren SiKoSH-Standard



Genauere Betrachtung der Einzelschritte von Phase 1 und Vorstellung aller relevanten Hilfsmittel

ISM-Basis	Prüfpunkte	Priorität	Status	Bewertung	SIKO-SH Hilfmittel		
1 Sind Formulare und Verantwortlichkeiten vorliegend	ISMETAT 11	Die Behörde/Behörden hat die Gesamtverantwortung für Informationssicherheit deutlich erkennbar für alle Beteiligten übernommen. Die Behörde/Behörden hat den Informationssicherheitsprozess vor, in dem Sie ihn initiiert, steuert und festlegt, ausgearbeitet werden.	Normal	Unbewertet	0	Informationssicherheit für die Behörde/Behörden	
	ISMETAT 12	Für die Zuständigkeiten und Verantwortlichkeiten sind Verantwortliche definiert, die mit den erforderlichen Kompetenzen und mögliche Funktionen innehaben.	Normal	Unbewertet	0	Betriebshandbuch - allgemeiner Teil	
	ISMETAT 13	Die Behörde/Behörden hat eine Verantwortung über den Stand der Informationssicherheit und hat insbesondere über diese eine Strategie für Informationssicherheit festgelegt und dokumentiert.	Normal	Unbewertet	0	ISMS-Betrieb	
	ISMETAT 14	Es werden strategische Vorgaben erarbeitet und organisatorische Rahmenbedingungen geschaffen, um den Informationsprozess und dessen Umsetzung mit Informationen innerhalb aller Fachaufgaben der Behörde zu ermöglichen. Aktualität und Abgrenzung sind überprüfbar.	Hoch	Unbewertet	0	Informationssicherheitsleitlinie	
	ISMETAT 15	Die Informationssicherheitsleitlinie wird erstellt und durch die Behörde/Behörden unterstützt und in Kraft gesetzt. Wichtigen Aspekte der Sicherheitsstrategie werden der Organisationsstruktur für Informationssicherheit, die Sicherheit Ziele, die festzulegen sind festgelegt. Die Sicherheitsziele und die Struktur der Sicherheitsziele zu den Aufgaben der Behörde/Behörden sind in allen Mitarbeiter/innen bekannt und wird regelmäßig aktualisiert.	Hoch	Unbewertet	0	Informationssicherheitsleitlinie	
	ISMETAT 16	Die Informationssicherheitsleitlinie wird erstellt und durch die Behörde/Behörden unterstützt und in Kraft gesetzt. Wichtigen Aspekte der Sicherheitsstrategie werden der Organisationsstruktur für Informationssicherheit, die Sicherheit Ziele, die festzulegen sind festgelegt. Die Sicherheitsziele und die Struktur der Sicherheitsziele zu den Aufgaben der Behörde/Behörden sind in allen Mitarbeiter/innen bekannt und wird regelmäßig aktualisiert.	Normal	Unbewertet	0	Informationssicherheitsleitlinie	
	2 Sind aktuelle Prozesse und Strukturen beschaffen	ISMETAT 17	Es wurde eine Informationssicherheitsbeauftragter (ISB) (normal) bestellt zur Förderung der Informationssicherheit in der Behörde/Behörden und der Förderung der Sicherheitsprozesse.	Normal	Unbewertet	0	Bestellung eines ISB
		ISMETAT 18	Der oder die ISB wird bei allen größeren Projekten eingebunden und hat bei Bedarf das I-Bestellrecht an die ISB. Sollte ein kleinerer ISB-Sicherheitsbeauftragter bestellt worden sein, ist eine geeignete Vernetzung (Problemlösung, Projektleitung, Kundenkontakt) für die Informationssicherheit bzw. ein Informationssicherheitsbeauftragter zu gewährleisten. Die Aufgaben und Verantwortlichkeiten sind im Rahmen der Bestellung eindeutig definiert.	Normal	Unbewertet	0	Bestellung eines ISB
		ISMETAT 19	Es wurde eine eigene Organisationsstruktur für die Informationssicherheit bzw. ein Informationssicherheitsbeauftragter zu gewährleisten. Die Aufgaben und Verantwortlichkeiten sind im Rahmen der Bestellung eindeutig definiert.	Normal	Unbewertet	0	ISMS-Organisation
		ISMETAT 20	Die Informationssicherheitsleitlinie wird erstellt und durch die Behörde/Behörden unterstützt und in Kraft gesetzt. Wichtigen Aspekte der Sicherheitsstrategie werden der Organisationsstruktur für Informationssicherheit, die Sicherheit Ziele, die festzulegen sind festgelegt. Die Sicherheitsziele und die Struktur der Sicherheitsziele zu den Aufgaben der Behörde/Behörden sind in allen Mitarbeiter/innen bekannt und wird regelmäßig aktualisiert.	Normal	Unbewertet	0	ISMS-Organisation
		ISMETAT 21	Für die gesamte Informationsverarbeitung sind ausreichende und angemessene Sicherheitsmaßnahmen festgelegt und regelmäßig aktualisiert.	Normal	Unbewertet	0	ISMS-Organisation
		ISMETAT 22	Die Sicherheitsmaßnahmen zur Informationsverarbeitung werden in Sicherheitskonzepten dokumentiert und regelmäßig aktualisiert.	Normal	Unbewertet	0	ISMS-Betrieb
	3 Ist der Sicherheitsprozess mit den Organisationsstrukturen verknüpft	ISMETAT 23	Alle Mitarbeiter/innen werden in Themen der Informationssicherheit miteinbezogen und regelmäßig über Gefährdungen und Sicherheitsmaßnahmen informiert.	Hoch	Unbewertet	0	Quickchecks
		ISMETAT 24	Alle Mitarbeiter/innen sind in der Lage (z.B. durch Schulungen) Sicherheit aktiv mitzugestalten.	Hoch	Unbewertet	0	SIKOSH Phase 2
		ISMETAT 25	Sicherheitsrichtlinien und dazugehörige Regelungen werden zielgruppenspezifisch erstellt und in geeigneter Weise bekanntgegeben.	Normal	Unbewertet	0	ISMS-Organisation
		ISMETAT 26	Die Informationssicherheitsleitlinie wird erstellt und durch die Behörde/Behörden unterstützt und in Kraft gesetzt. Wichtigen Aspekte der Sicherheitsstrategie werden der Organisationsstruktur für Informationssicherheit, die Sicherheit Ziele, die festzulegen sind festgelegt. Die Sicherheitsziele und die Struktur der Sicherheitsziele zu den Aufgaben der Behörde/Behörden sind in allen Mitarbeiter/innen bekannt und wird regelmäßig aktualisiert.	Normal	Unbewertet	0	ISMS-Organisation
		ISMETAT 27	Es ist sicherzustellen, dass der Informationssicherheitsprozess einen Einfluss auf alle relevanten Entscheidungsfindungen und Prozesse aller Institutionen hat.	Normal	Unbewertet	0	ISMS-Organisation
		ISMETAT 28	Die Informationssicherheitsleitlinie wird erstellt und durch die Behörde/Behörden unterstützt und in Kraft gesetzt. Wichtigen Aspekte der Sicherheitsstrategie werden der Organisationsstruktur für Informationssicherheit, die Sicherheit Ziele, die festzulegen sind festgelegt. Die Sicherheitsziele und die Struktur der Sicherheitsziele zu den Aufgaben der Behörde/Behörden sind in allen Mitarbeiter/innen bekannt und wird regelmäßig aktualisiert.	Normal	Unbewertet	0	ISMS-Organisation
ISMETAT 29		Eine Abklärung der Fachbereiche untereinander in Sachen Sicherheit und Risikomanagement ist sicherzustellen.	Niedrig	Unbewertet	0	ISMS-Organisation	



Vorschau und Feedback zur Weiterentwicklung von SiKoSH

2 Regelungen ISMS

Die folgenden Regelungen (R.0) behandeln die kommunalen Basis-Anforderungen, die sich aus dem IT-Grundschutz-Kompendium und dem IT-Grundschutz-Profil "Basis-Absicherung Kommunalverwaltung" für den Baustein ISMS.1 ergeben (Anforderungen A1 - A9).

Es wird empfohlen, die Anforderungen des IT-Grundschutz-Kompendiums mit den tatsächlichen Gegebenheiten der anwendenden Institution abzugleichen und bei Bedarf die Regelungen dieser Richtlinie entsprechend zu ergänzen oder abzuändern. Dabei wird von einer Organisation ohne ISMS bzw. mit einem geringen Reifegrad eines ISMS ausgegangen. Sofern bereits Teile der untenstehenden Regelungen umgesetzt sind, besteht keine zwingende Notwendigkeit, die unten beschriebenen Umsetzungsformen zu verwenden. An den bereits eingeführten, ähnlichen Prozessen kann festgehalten werden, sofern diese eine adäquate Zielsetzung beinhalten.

- R.1 Gemäß Informationssicherheitsleitlinie liegt der Fokus im ersten Aufbau Schritt zunächst auf dem Sicherheitsniveau Basis-Absicherung. Die Anforderungen aus den SiKoSH Quickchecks (basierend auf dem IT-Grundschutz-Profil Basis-Absicherung Kommunalverwaltung) sind umzusetzen.
- R.2 Informationssicherheit ist in alle Geschäftsprozesse und Fachaufgaben zu integrieren. Zusätzlich ist die oder der ISB an allen sicherheitsrelevanten Entscheidungen zu beteiligen.
- R.3 Alle Mitarbeitenden werden in den Sicherheitsprozess integriert. Dafür werden sie über Hintergründe, für sie relevante Gefährdungen und durch die Planung von Sicherheitsmaßnahmen informiert. Zusätzlich werden sie bei der Planung von Sicherheitsmaßnahmen und der Gestaltung organisatorischer Regelungen frühzeitig beteiligt, um die Akzeptanz und Praktikabilität zu steigern.
- R.4 Sicherheitsmaßnahmen sind dann angemessen, wenn Sie unter Betrachtung der Wirtschaftlichkeit das Restrisiko für die Bedrohung der Schutzziele der Informationssicherheit auf ein akzeptables (vertretbares) Maß reduzieren.
- R.5 Die Dokumentation der Basis-Anforderungen erfolgt durch die SiKoSH-Quickchecks [Toolbasiert].
- R.6 Weitere zu dokumentierende Bestandteile des Sicherheitskonzepts sind:

Informationssicherheit für Behördenleiter
Informationssicherheitsleitlinie

IT-Grundschutz-Profil Basis-Absicherung Kommunalverwaltung

Risikomanagement

SiKoSH-Quickchecks

- Risiken gemäß Anlage 4 (Excel-Datei „Anlage 4 ISMS-Betrieb (Risikoliste).xlsx“)
- Ausnahmen gemäß Anlage 5 (Excel-Datei „Anlage 5 ISMS-Betrieb (Ausnahmeliste).xlsx“)

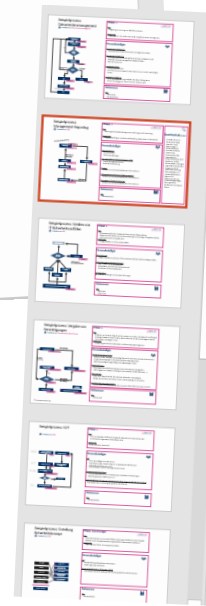
R.7 Die Sicherheitsdokumentation ist anschlussbezogen – jedoch spätestens jährlich – hinsichtlich Aktualität und Vollständigkeit zu prüfen.

R.8 Alle Mitarbeitende sind für das Thema Informationssicherheit zu sensibilisieren und regelmäßig zu schulen.

Hinweis: Sensibilisierung und Schulung wird in SiKoSH Phase 2 genauer betrachtet.

R.9 Zwischen ISB und Behördenleitung haben regelmäßige (mindestens alle [XX] Wochen) sowie anschlussbezogene Besprechungen stattzufinden, in denen über den Stand der Informationssicherheit und mögliche Risiken und Konsequenzen aufgrund fehlender Sicherheitsmaßnahmen informiert wird. Über die durchgeführten Besprechungen sind Protokolle anzufertigen und abzuliegen.

Hinweis: Dafür gibt es ein SiKoSH-Beispielprozess: Management-Reporting



Beispielprozess: Management-Reporting

Prozessowner: ISB

vereinfachte Darstellung:



Phase: 1

- Ziel:**
- Beratung der Behördenleitung zur aktueller Lage und Entwicklung
- Zuordnung:**
- Aufgabe des ISB gem. Leitlinie und Bestellung, Beschreiben in Richtlinie IS

Prozessbeteiligte

- Behördenleitung**
- Wird informiert
 - Trifft Entscheidungen
- Informationssicherheitsbeauftragte/-r (ISB)**
- Erstellt Managementbericht
 - Berät Behördenleitung
- IT-Leiter**
- Zuliefern von sicherheitsrelevanten Informationen
- IT-Sicherheitskoordinatoren (falls vorhanden)**
- Zuliefern von sicherheitsrelevanten Informationen
- Dienstleister / Outsourcingpartner**
- Zuliefern von sicherheitsrelevanten Informationen

Referenzen

- BSI:**
- Standard 200-1

Berichtsinhalt, u.a.:

- Aktueller Status im Sicherheitsprozess
- Überblick neuer Bedrohungen / Sicherheitslücken
- Compliance-Status
- Auswertung Sicherheitsvorfälle
- Ergebnisse von Sicherheitsanalysen (z.B. Revisionen, Audits, Risikoanalysen, Übungen)
- Ergebnisse aus laufenden Programmen (z.B. Awareness, Schulung)
- Rückmeldungen von Kunden/Mitarbeitern
- Eigene KPI's
- Ressourcenplanung
- Entscheidungsvorlagen
- Status geplanter Maßnahmen aus letztem Bericht

- Die vorgestellten neuen Hilfsmittel (Beispielprozesse, erweiterter Quickcheck,..) wurden als hilfreich angesehen
- Für die weitere Überarbeitung von SiKoSH wurde das Thema Notfall als wichtig angesehen
- Auch wenn man sich schon mal selbst mit SiKoSH beschäftigt hat, war der Workshop beim Zugang und Verständnis sehr hilfreich
- Teilnehmende wünschen sich einen regelmäßigen Austausch und weitere Workshops

Vielen Dank für die Teilnahme

Sprechen Sie uns gerne im Anschluss oder in der restlichen Zeit des ITV.SH-Forums an!



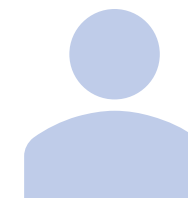
Andreas Haase

IT-Sicherheitsberater
Dataport



Lutz Seemann

IT-Sicherheitsberater
Dataport



Frank Weidemann

Projektleitung SiKoSH
ITV.SH

frank.weidemann@itvsh.de