AG Handreichung ISLL

Handreichung zur Ausgestaltung der

Informationssicherheitsleitlinie in Kommunalverwaltungen

Version 3.0, veröffentlicht im Oktober 2024

Autorenschaft

Die vorliegende dritte Auflage der Handreichung zur Ausgestaltung der Informationssicherheitsleitlinie in Kommunalverwaltungen wurde von einer behördenübergreifenden Arbeitsgruppe erstellt:

Leitung der Arbeitsgruppe:

Markus Albert, Informationssicherheitsbeauftragter, FITKO (Föderale IT-Kooperation), Frankfurt a. M.,
E-Mail: markus.albert@fitko.de

Dr. Lutz Gollan, Fachbereichsleiter, Landesbetrieb Verkehr, Hamburg,
E-Mail: lutz.gollan@lbv.hamburg.de

Moritz Kienzle, Informationssicherheitsbeauftragter, Landkreis Rotenburg (Wümme),
E-Mail: moritz.kienzle@lk-row.de

Jens Lange, Informationssicherheitsbeauftragter, Stadt Kassel,
E-Mail: jens.lange@kassel.de

Heino Reinartz, Chief Information Security Officer, Stadt Eschweiler,
E-Mail: heino.reinartz@eschweiler.de

Mitglieder der Arbeitsgruppe:

Timo Bock, IT-Sicherheitskoordinator, Kommunale Dienste Göttingen (kAöR)

Thorsten Früchtnicht, Externer Sicherheitsbeauftragter, Zweckverband Kommunale Datenverarbeitung Oldenburg

Marianne Grofe-Juhlke, IT-Sicherheitsbeauftragte, Stadt Krefeld

Kathrin Heckmann, Informationssicherheitsbeauftragte, Landkreis Anhalt-Bitterfeld

Dirk Helbig, Stabsstellenleiter und CDO/CIO, Salzlandkreis

Olaf Kirsch, IT-Sicherheitsbeauftragter, Kreis Marburg-Biedenkopf

Jörg Naumann, Beauftragter für Informationssicherheit, Stadt Chemnitz

Maik Poburski, Informationssicherheitsbeauftragter, Landkreis Osnabrück

Jan Schrod, Informationssicherheitsbeauftragter, Kreis Mettmann

Frank Weidemann, Datenschutzbeauftragter, IT-Verbund Schleswig-Holstein (AöR)

Udo Zaudig, Chief Information Security Officer, Stadt Köln

Der IT-Planungsrat hat in seiner 16. Sitzung am 18. März 2015 im Beschluss 2015/05 erklärt, er halte die Handreichung „insbesondere in der Orientierungs- und Einstiegsphase der Entwicklung und Gestaltung von Informationssicherheitsleitlinien sowie für Aufbau und Betrieb kommunaler Informationssicherheits-Managementsysteme für geeignet und empfiehlt den Kommunalverwaltungen deren Anwendung.“

Eschweiler/Frankfurt/Hamburg/Kassel/Rotenburg (Wümme)
im Oktober 2024

Inhaltsverzeichnis

1. VORWORT

Die Bedrohungslage im Cyberraum ist weiterhin besorgniserregend. Täglich kommt es zu erfolgreichen Cyberangriffen oder weitreichenden IT-Sicherheitsvorfällen, die zu IT-Störungen und -Ausfällen führen und damit unser alltägliches Leben beeinträchtigen. Der kommunalen Ebene kommt dabei eine besondere Bedeutung zu. Viele Energie- und Wasserwerke, Krankenhäuser oder Entsorgungseinrichtungen werden von Städten und Gemeinden sowie Landkreisen betrieben. Sie alle sind zentral für eine funktionierende Gesellschaft. Gleiches gilt für die täglichen Verwaltungsdienstleistungen im Rathaus und auf dem Landratsamt. Sie sind für uns unerlässliche Grundlage des Miteinanders, des nachhaltigen Wirtschaftens und unseres Wohlergehens.

Angriffe mit Ransomware (Verschlüsselungstrojaner) haben insbesondere in Kommunalverwaltungen und bei ihren IT-Dienstleistern auch in der jüngeren Vergangenheit schwerwiegende Folgen verursacht − Folgen nicht nur für die Kommunalverwaltungen selbst, sondern insbesondere auch für die Bürgerinnen und Bürger. Sozialleistungen können nicht oder verspätet ausgezahlt werden, Hochzeiten müssen verschoben werden, KFZ-Anmeldungen können nicht durchgeführt werden. Wenn wichtige bürgernahe Dienstleistungen ausfallen, bedeutet dies aber auch eine erhebliche Mehrbelastung für die Mitarbeiterinnen und Mitarbeiter. Zwar gibt es keine 100-prozentige Sicherheit, aber die Wahrscheinlichkeit für einen IT-Sicherheitsvorfall lässt sich schmälern und auch die schwerwiegenden Folgen mildern, wenn die richtigen Maßnahmen umgesetzt werden.

Ein wichtiger Baustein einer resilienten Cybernation Deutschland ist dabei ein strukturiertes Vorgehen zur Herstellung bzw. Aufrechterhaltung eines angemessenen Informationssicherheitsniveaus, idealerweise auf Grundlage eines Informationssicherheitsmanagement-Systems wie dem BSI-Grundschutz.

Aber unabhängig davon, welcher Standard eingesetzt wird: an erster Stelle steht jeweils das klare Bekenntnis der Behördenleitung zur Informationssicherheit und die Übernahme der Verantwortung für dieses Thema. Dieses Bekenntnis sollte durch eine Informationssicherheitsleitlinie der obersten Verwaltungsebene erfolgen.

Die vorliegende vollständig aktualisierte Handreichung zur Ausgestaltung der Informationssicherheitsleitlinie in Kommunalverwaltungen hilft dabei, sich dem Thema angemessen zu widmen. Das Bundesamt für Sicherheit in der Informationstechnik arbeitet eng mit den Kommunen zusammen und hofft, dass die Handreichung nicht nur einen Überblick über Sinn und Zweck, Vor- und Nachteile der verschiedenen Standards verschafft, sondern durch die Erläuterungen und Formulierungshilfen den Städten, Gemeinden und Landkreisen eine verlässliche Grundlage für die Förderung und Festigung der eigenen Informationssicherheit liefert.

Claudia Plattner

Präsidentin
Bundesamt für Sicherheit in der Informationstechnik

2. ZUSAMMENFASSUNG

Die Informationssicherheit in Kommunen ist eng mit deren Aufgabenerfüllung verbunden. Sie ist ein kritischer Schlüssel für verlässliches und nachvollziehbares Verwaltungshandeln. Über die letzten Jahrzehnte hat dabei die Sicherheit der Informationstechnik (IT) als Teilmenge der Informationssicherheit[1] einen bedeutenden Stellenwert eingenommen. Die Komplexität der IT, der hohe Grad der Vernetzung und die Abhängigkeit der Verwaltung von IT-gestützten Verfahren verlangen nach einer Systematisierung und Organisation der Informationssicherheit – nach einem Informationssicherheits-Managementsystem (ISMS). Die Grundlage für ein solches ISMS ist ein Bekenntnis der Behördenleitung zur Informationssicherheit. Dieses Bekenntnis wird durch eine Informationssicherheitsleitlinie (ISLL) verbrieft.

Planung, Umsetzung, Überprüfung und Verbesserung der Informationssicherheit dürfen nicht als Projekt angesehen werden, das nach einem festen Terminplan durchgeführt wird und die Zielstellung hat, einmalig für mehr Informationssicherheit zu sorgen. Vielmehr handelt es sich um einen stetigen Prozess zur Feststellung des aktuellen Sicherheitsniveaus und den daraus resultierenden Festlegungen zur Verbesserung. Die Einführung und Aufrechterhaltung dieses Sicherheitsprozesses ist Aufgabe der Behördenleitung. Sie muss den Sicherheitsprozess initiieren, steuern und auch überprüfen, ob die Sicherheitsziele in allen Bereichen umgesetzt werden. Nur wenn sie voll hinter den Sicherheitszielen und den damit verbundenen Aktivitäten steht, kann diese Aufgabe erfolgreich wahrgenommen werden. Dafür ist eine systematische Herangehensweise an einen kontinuierlichen Überwachungs- und Optimierungsprozess nötig, mit dem sowohl die Technik als auch die Beschäftigten und weitere Einflussfaktoren berücksichtigt werden.

Die vorliegende Handreichung erläutert, wie ein ISMS aufgebaut und unterhalten werden kann, und sie beschreibt, wie eine dahinterstehende ISLL konzipiert und gestaltet werden kann.

Die Handreichung wurde von kommunalen Praktikerinnen und Praktikern erstellt und orientiert sich zum einen an den in Deutschland verbreiteten Standards zur Informationssicherheit und den Vorgaben, die der IT-Planungsrat als verfassungsrechtlich legitimiertes Gremium über seine Leitlinie zur Informationssicherheit erstellt hat. Zum anderen hat sie die kommunalen Realitäten im Blick und nimmt Rücksicht auf die Besonderheiten der Gebietskörperschaften.

[1] Vgl. Zilkens/Gollan, Datenschutz in der Kommunalverwaltung, 6. Aufl. 2023, Rn. 1369 ff.

3. EINLEITUNG

Bei der Einführung eines ISMS spielt die örtliche ISLL eine wesentliche Rolle. Der vorliegende Text enthält eine Hilfestellung zur Erarbeitung einer solchen ISLL. Kapitel 4 erörtert zunächst die wichtigsten Begriffe der Informationssicherheit. Im Kapitel 5 werden die gängigen ISMS-Standards vorgestellt, gefolgt (Kapitel 6) von der Erörterung der Leitlinie des IT-Planungsrats. In Kapitel 7 werden in der Praxis erprobte Mustertexte für eine kommunale ISLL präsentiert.

Die rechnergestützte Informationsverarbeitung stellt die öffentliche Verwaltung vor große Herausforderungen. Über die Jahre hinweg haben sich die technischen Möglichkeiten, aber auch die Anforderungen an die Informationstechnik (IT) stetig weiterentwickelt. Während anfänglich eine Nutzung der IT-Systeme nur durch wenige, spezialisierte Beschäftigte erfolgte, einfache digitale Nachrichten empfangen und versendet wurden und die Gefahren als beherrschbar galten, wachsen mittlerweile die Bedrohungen für die Informationssicherheit in den Kommunalverwaltungen. Diese ergeben sich u. a. aus der zunehmenden komplexen Vernetzung der Informationstechnik und der dazugehörigen Systeme. Neben den elementaren Gefährdungen und technischem Versagen spielen dabei Schwachstellen in IT-Systemen und Anwendungen, organisatorische Mängel, menschliche Fehlhandlungen, aber auch vorsätzliche, ggf. kriminelle Handlungen eine wesentliche Rolle.

Mit dem vorliegenden Dokument soll der Einstieg zum Aufbau eines ISMS in der Kommunalverwaltung unterstützt werden. Ein ISMS bietet Chancen, die geschilderten Bedrohungen strukturiert zu erkennen und ihnen angemessen zu begegnen. Das Dokument richtet sich in erster Linie an die Leitungsebene der Kommunalverwaltung und deren Informationsmanagement, durch die alle notwendigen Schritte zum Aufbau und Betrieb eines ISMS einzuleiten und im weiteren Verlauf zu überwachen sind.

Die Vorteile eines ISMS sind insbesondere:

- die organisierte und nachvollziehbare Abwehr von Bedrohungen der Informationssicherheit,
- die Sicherstellung der Erfüllung gesetzlicher Anforderungen, u. a. bei ebenenübergreifenden Verfahren und bei der Anbindung an das Verbindungsnetz,
- die Optimierung der Kosten beim IT-Einsatz,
- die planbare Nutzung der IT für alle Verwaltungsabläufe,
- die Minimierung der Risiken für den Umgang mit Informationen,
- die Steigerung des Vertrauens in der Öffentlichkeit und
- die Integration in das übergeordnete Managementsystem der Verwaltung.

4. BEGRIFFE

4.1. INFORMATIONSSICHERHEIT

Informationssicherheit kann als der Zustand beschrieben werden, in dem die drei Grundwerte **Vertraulichkeit, Integrität und Verfügbarkeit** von Informationen durch angemessene Maßnahmen gewährleistet sind. Dabei umfasst die Informationssicherheit den Schutz von jeglichen Informationen (einschließlich personenbezogene Daten, amtliche Geheimhaltungsstufen[2], Amts-, Betriebs- und Geschäftsgeheimnisse) jeglicher Art und Herkunft, unabhängig davon, ob sie auf Papier oder digital gespeichert sind.

Die Begriffe Informationssicherheit, IT-Sicherheit und Cybersicherheit werden sehr häufig synonym verwendet. In der vorliegenden Handreichung wird der Begriff Informationssicherheit verwendet, um zu verdeutlichen, dass elektronische wie auch nicht-elektronische Informationen zu schützen sind, die z. B. auch in Aktenform vorliegen können.

Vertraulichkeit	Integrität	Verfügbarkeit
Zugang zu Informationen nur für Befugte Es gibt klar festgelegte Berechtigungen, welche Personen auf welche Informationen (z. B. Daten mit normalem oder hohem Schutzbedarf, allgemeine Informationen oder Verschlusssachen) zugreifen dürfen.	Unversehrtheit und Korrektheit von Informationen Die Informationen sind vollständig und richtig; unautorisierte Änderungen gespeicherter oder übertragener Daten werden ausgeschlossen bzw. erkannt.	Informationen bei Bedarf bereitstellen IT-Systeme, Anwendungen und Informationen sind verfügbar, wenn sie gebraucht werden.

Abbildung 1: Grundwerte der Informationssicherheit

4.2. INFORMATIONSSICHERHEITSKONZEPT VS. -KONZEPTION

Ein **Sicherheitskonzept** ist das zentrale Dokument des Sicherheitsprozesses einer Organisation. Darin wird systematisch beschrieben, durch welche Maßnahmen die Sicherheitsziele der Organisation zu erreichen sind. Alle Sicherheitsmaßnahmen auf operationaler Ebene werden von diesem Dokument abgeleitet.

Die Erstellung einer **Sicherheitskonzeption** ist eine der zentralen Aufgaben des Informationssicherheits-Managements. Damit werden die erforderlichen Sicherheitsmaßnahmen identifiziert, die im Sicherheitskonzept und seinen Teilkonzepten dokumentiert werden. Die Erstellung einer Sicherheitskonzeption ist im BSI-Standard 200-2 IT-Grundschutz-Methodik beschrieben.

Die Sicherheitsorganisation und das Sicherheitskonzept müssen nach Planung und Umsetzung einer Prüfung unterzogen werden. Dabei werden die Eignung und Effizienz der umgesetzten Maßnahmen und eine eventuelle Veränderung der Rahmenbedingungen (z. B. Organisationsziele oder Gesetze) betrachtet.

[2] Beispielsweise „VERSCHLUSSSACHE – VERTRAULICH“ oder „GEHEIM“.

Für einige Kommunen in Deutschland ist es gemäß der jeweiligen Landesgesetzgebung verpflichtend, über ein Informationssicherheitskonzept zu verfügen. So müssen z. B. gemäß § 14 Sächsisches Informationssicherheitsgesetz staatliche Stellen zur Erreichung und Aufrechterhaltung eines angemessenen Informationssicherheitsniveaus die jeweils geltenden Standards und das jeweils geltende IT-Grundschutz-Kompendium des Bundesamtes für Sicherheit in der Informationstechnik BSI berücksichtigen. In Bayern müssen die Kommunen nach Art. 43 Abs. 1 Bayerisches Digitalgesetz über ein Informationssicherheitskonzept verfügen. Dieses kann dort über das niedrigschwellige „LSI-Siegel“ (Landesamt für Sicherheit in der Informationstechnik) erstellt werden.[3]

Für die meisten der sogenannten ebenenübergreifenden Verfahren werden explizit Informationssicherheitskonzepte gefordert und deren Umsetzung geprüft.

4.3. INFORMATIONSSICHERHEITS-ORGANISATION

Die **Informationssicherheits-Organisation** (IS-Organisation) ist eine speziell mit Aufgaben zur Informationssicherheit betraute Einheit der Behörde. Sie stellt keine eigenständige Organisationseinheit dar, sondern setzt sich aus Beteiligten der bestehenden Organisationseinheiten zusammen. Die IS-Organisation sollte mindestens aus einer verantwortlichen Führungskraft der Behördenleitung sowie einer auf Informationssicherheit fachlich spezialisierten Person bestehen. In der Leitlinie zur Informationssicherheit einer Kommune sollte die konkrete Organisation vorgegeben und die erforderlichen Rollen und Aufgaben festgelegt werden.

4.4. INFORMATIONSSICHERHEITS-MANAGEMENTSYSTEM

Das **Informationssicherheits-Managementsystem** (ISMS) definiert, organisiert und dokumentiert alle Anforderungen zum Umgang mit Informationen an die Behörde und deren Umsetzungsstand. Es umfasst die Organisationsstrukturen und Geschäftsprozesse, die genutzte IT-Infrastruktur sowie Bedrohungsszenarien, welche allesamt einem ständigen Wandel unterworfen sind. Ein angemessenes Sicherheitsniveau wird nur durch eine kontinuierliche, ganzheitliche Betrachtung des gesamten Informationsflusses sowie aller daran Beteiligten gewährleistet.

Die Behördenleitung muss diesen Sicherheitsprozess initiieren. Dabei dient das ISMS als organisatorischer Rahmen für den Sicherheitsprozess und damit zur Schaffung und Aufrechterhaltung eines angemessenen Niveaus der Informationssicherheit in der gesamten Organisation sowie zur regelmäßigen Überprüfung der Sicherheitsziele und Steuerung aller damit verbundenen Maßnahmen. Es ist maßgeblich für den Erfolg dieser Aufgabe, dass die Behördenleitung hinter den Sicherheitszielen und den damit verbundenen Aktivitäten steht und dies dokumentiert wird.

Zur Implementierung eines ISMS haben sich mehrere gängige de-facto-Standards etabliert (s. Kapitel 5). Diese sehen verschiedene Maßnahmen und Hilfsmitteln vor, mit denen die Bestimmung des aktuellen Sicherheitsniveaus, die Festlegung der für die Organisation angemessenen Anforderungen und Ziele und die Steuerung des Sicherheitsprozesses vorgenommen werden können.

Das aus dem Qualitätsmanagement bekannte „PDCA-Modell“ (engl. „Plan, Do, Check, Act“ – „Planen, Umsetzen, Prüfen, Verbessern“) hat sich in der Praxis für diesen kontinuierlichen Verbesserungsprozess bewährt.

[3] https://www.lsi.bayern.de/kommunen/siegel_kommunale_it_sicherheit/

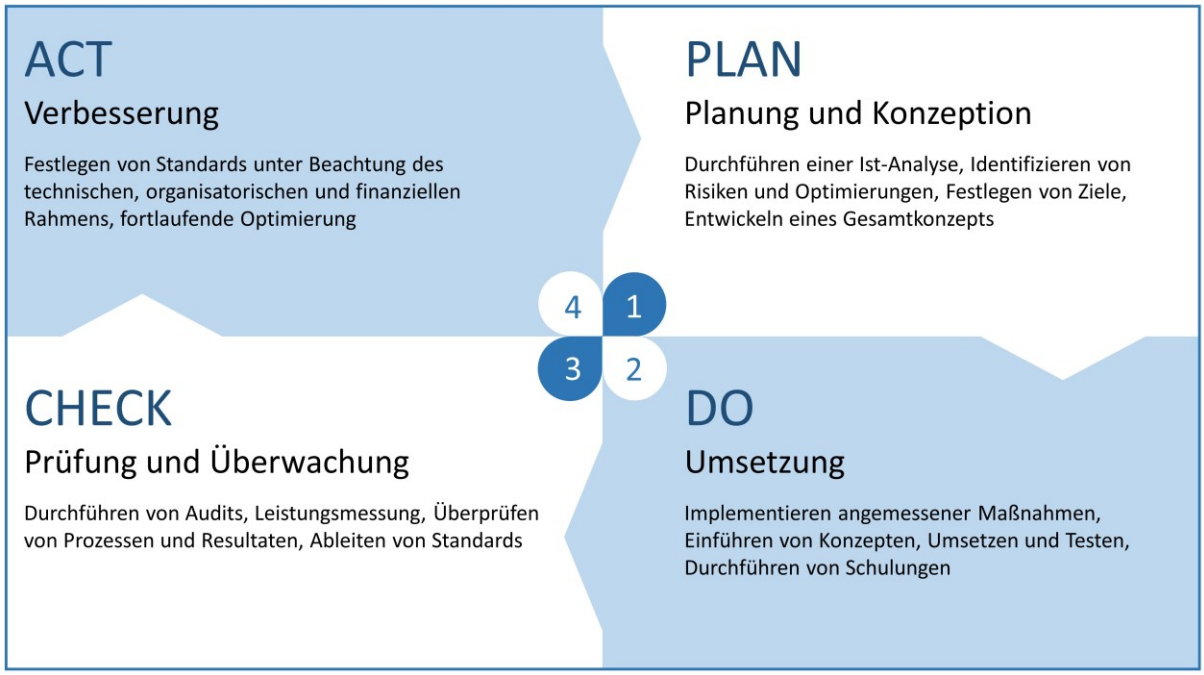

Abbildung 2: PDCA-Modell zur Einführung eines ISMS

5. AUSGEWÄHLTE STANDARDS FÜR EIN ISMS

Ein ISMS soll für die Behörde ein angemessenes Niveau an Informationssicherheit bewirken, was durch eine Zertifizierung des ISMS bestätigt werden kann, jedoch nicht zwingend erfolgen muss. Auch ohne eine Zertifizierung ermöglicht das Arbeiten nach einem anerkannten ISMS-Standard, dass alle relevanten Aspekte der Informationssicherheit beachtet werden und dies transparent dokumentiert wird. Aus diesem Grund werden nachfolgend wesentliche Standards zum Aufbau eines zertifizierbaren ISMS dargestellt. Die Aufstellung erhebt keinen Anspruch auf Vollständigkeit. Die für eine Zertifizierung notwendigen Schritte und möglichen Kosten werden nicht betrachtet. Die abschließende Gegenüberstellung (siehe Kapitel 5.6) soll die Vorzüge, aber auch die Unterschiede verdeutlichen. Auch wenn keine Zertifizierung angestrebt wird, bilden die genannten Standards die Grundlage zum erfolgreichen Betrieb eines ISMS.

5.1. ISO/IEC 2700X-NORMENREIHE

Die laufend erweiterte Normenreihe ISO 2700x[4] ist eine Sammlung internationaler Standards für den Aufbau und den Betrieb eines ISMS. Der zugrundeliegende Standard wurde ursprünglich auf Basis von Best-Practice-Empfehlungen für die Industrie entwickelt. Ein einheitliches Mindestsicherheitsniveau wird durch die Reihe nicht vorgegeben. Die in den zugehörigen Standards formulierten Maßnahmen haben empfehlenden Charakter. Bei der Anwendung der ISO 27001 legt die anwendende Organisation das Sicherheitsniveau individuell unter Berücksichtigung bestehender und möglicher Risiken fest.

Zusammenfassend lässt sich sagen, dass der „Hauptstandard“, die Norm ISO 27001, die Anforderungen an die Einführung, Umsetzung, Dokumentation und Verbesserung eines ISMS formuliert. Es ist möglich, sich nach ISO/IEC 27001 zertifizieren zu lassen und dadurch die Wirksamkeit seines ISMS nachzuweisen. Im Standard ISO 27002 werden die o. g. Anforderungen aufgegriffen und spezifiziert. ISO 27002 kann daher als Leitfaden für die praktische Umsetzung angesehen werden.

Die Reihe beinhaltet weitere Normen (in Summe ca. 38), die Unterstützung bieten durch u. a. Implementierungsrichtlinien, Risikomanagementmodelle und Kennzahlensysteme.

Die Normenreihe muss käuflich erworben werden.

5.2. IT-GRUNDSCHUTZ

Einen weiteren Standard hat das BSI in der Reihe 200[5] beschrieben. Dieser ist Teil des BSI IT-Grundschutzes, der auf der Normenfamilie ISO/IEC 2700x aufbaut.

Die Methodik des IT-Grundschutzes bietet verschiedene Vorgehensweisen, um Behörden sowie Organisationen unterschiedlicher Größe und Branchen einen geeigneten Einstieg in die Informationssicherheit zu ermöglichen.[6] Neben dem sogenannten IT-Grundschutz-Kompendium mit konkreten Anforderungen und Umsetzungshinweisen, das laufend aktualisiert wird, unterstützen die Einzel-Standards 200-1 bis 200-4 bei der konkreten Umsetzung. Der Standard 200-1 beschreibt dabei die allgemeinen Anforderungen, 200-2 die verschiedenen Vorgehensweisen. 200-3 legt dar, wie eine Risikoabschätzung erfolgen kann, und 200-4 unterstützt bei Aufbau und Gestaltung eines Systems zum Business Continuity Management (BCM Geschäftsfortführungs-Management).

[4] https://de.wikipedia.org/wiki/ISO/IEC-27000-Reihe
[5] IT-Grundschutz-Standards kostenlos verfügbar unter https://www.bsi.bund.de/dok/6603458.
[6] Vgl. den entsprechenden Leitfaden unter https://www.bsi.bund.de/dok/10051454.

Der IT-Grundschutz wurde vom BSI als Behörde (nicht nur) für Behörden entwickelt. Durch ein Ausleseverfahren konkret formulierter Sicherheitsmaßnahmen des IT-Grundschutz-Kompendiums kann ein einheitliches Mindestsicherheitsniveau etabliert werden, und gleichzeitig erleichtern diese die gesteuerte Einführung und Umsetzung. Darüber hinaus gehende Risiken sind zusätzlich zu betrachten.

Das IT-Grundschutz-Vorgehen wird meist als sehr aufwendig angesehen. Die Anzahl der Maßnahmen und der Umfang reduzieren sich jedoch, sobald bestimmte Aspekte, Systeme und Anwendungen nicht zum Einsatz kommen.

Im IT-Grundschutz-Kompendium werden nicht alle möglichen technischen Systeme sowie Spezialanwendungen katalogisiert. Fehlende Objekte sind durch eine Risikoanalyse (vergleichbar zum ISO-Standard) zu berücksichtigen und ggf. durch eigene Bausteine abzusichern. Darüber hinaus ermöglicht der modernisierte IT-Grundschutz durch das Angebot der drei Vorgehensweisen Basis-, Kern- und Standard-Absicherung eine schrittweise und auf die eigene Situation angepasste Implementierung eines ISMS: Über die Basis-Absicherung kann ein erster Einstieg in ein ISMS vollzogen werden, um schnellstmöglich die größten Risiken in der Breite zu senken. Im Vergleich dazu dient die Kern-Absicherung dem Schutz einzelner, elementarer Geschäftsprozesse und Ressourcen („Kronjuwelen“) in der Tiefe. Die Standard-Absicherung, die nach erfolgter Basis-Absicherung angestrebt werden sollte, entspricht der empfohlenen IT-Grundschutz-Vorgehensweise. Sie hat einen umfassenden Schutz für alle Prozesse und Bereiche der Institution als Ziel.

Darüber hinaus stellt das BSI sogenannte IT-Grundschutz-Profile[7] bereit, die von Anwender-Communitys für andere vergleichbare Organisationen entwickelt wurden, darunter auch das IT-Grundschutz-Profil Basis-Absicherung Kommunalverwaltung (s. u. 5.2.1). Diese Profile sollen ein Best-Practice-Beispiel bzw. eine Empfehlung abgeben, welche Anforderungen des IT-Grundschutzes in einer Kommune typischerweise relevant sind, was es ermöglichen soll, den zeitlichen und personellen Aufwand deutlich zu reduzieren.

Die Leitlinie zur Informationssicherheit des IT-Planungsrates von 2013 (aktuell Version 2.0 vom Dezember 2018[8]) bezieht sich ausdrücklich auf den IT-Grundschutz des BSI zur Festlegung eines einheitlichen Mindestsicherheitsniveaus. Ebenso orientieren sich die ebenenübergreifenden Verfahren z. B. der EU-Zahlstellen[9] am IT-Grundschutzvorgehen.

Alle IT-Grundschutz-Dokumente sind kostenfrei beim BSI erhältlich.[10]

5.2.1. IT-Grundschutz-Profil Basis-Absicherung Kommunalverwaltung

Das IT-Grundschutz-Profil Basis-Absicherung Kommunalverwaltung richtet sich an Kommunalverwaltungen, die einen systematischen Einstieg in die Informationssicherheit suchen. Anhand eines vordefinierten IT-Verbunds einer typischen Kommunalverwaltung mit ihren sicherheitsrelevanten Objekten referenziert das Profil die umzusetzenden BSI-Bausteine und leitet hieraus alle Anforderungen ab, die umzusetzen sind, um einen Mindestsicherheitsstandard zu erreichen. Das Profil erleichtert den Einstieg in die Informationssicherheit und hilft, die gröbsten Schwachstellen aufzudecken, die es zu beseitigen gilt, um möglichst schnell das Sicherheitsniveau in der Breite anzuheben. Um ein – dem Stand der Technik – angemessenes Sicherheitsniveau zu erreichen, müssen darauf aufbauend in einem weiteren Schritt zusätzliche Anforderungen erfüllt werden.

[7] https://www.bsi.bund.de/dok/it-grundschutz-profile
[8] https://www.it-planungsrat.de/beschluss/beschluss-2019-04
[9] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32006R0885&from=DE
[10] https://www.bsi.bund.de/dok/6603458

Das Profil wird regelmäßig durch kommunale Praktiker:innen der Arbeitsgruppe kommunale Basis-Absicherung der kommunalen Spitzenverbände (AG koBA) aktualisiert und kann kostenlos über die Webseite des BSI heruntergeladen werden.[11]

5.2.2. Weg in die Basis-Absicherung (WiBA)

Mit dem Projekt „Weg in die Basis-Absicherung (WiBA)“ trägt das BSI dem Umstand Rechnung, dass insbesondere für kleinere Behörden der Einstieg über die Basis-Absicherung immer noch sehr komplex ist. WiBA clustert 51 relevante BSI-Bausteine in 19 themenspezifische Checklisten, die durch die Reduzierung auf die wesentlichsten Anforderungen auch ohne tiefere Kenntnis der IT-Grundschutz-Methodik einen sehr schnellen Einstieg in den Aufbau eines ISMS ermöglichen und anschließend nahtlos in das IT-Grundschutz-Profil Basis-Absicherung Kommunalverwaltung überführt werden können; die Prüffragen in den Checklisten basieren auf diesem IT-Grundschutz-Profil Basis-Absicherung Kommunalverwaltung.[12]

5.3. SIKOSH (SICHERHEIT FÜR KOMMUNEN IN SCHLESWIG-HOLSTEIN)

SiKoSH (Sicherheit für Kommunen in Schleswig-Holstein) ist ein kostenfreies Angebot des ITV.SH AöR (IT-Verbund Schleswig-Holstein).[13]

In Zusammenarbeit mit Praktiker:innen aus den Kommunal- und Landesverwaltungen sowie dem Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein (ULD) und dem Landesrechnungshof Schleswig-Holstein ermöglicht SiKoSH den Kommunen einen einfachen und schnellen Einstieg in den Aufbau und den Betrieb eines entwicklungsfähigen ISMS. Grundlage von SiKoSH ist das IT-Grundschutz-Profil Basis-Absicherung Kommunalverwaltung“ (siehe oben).

SiKoSH teilt die Entwicklung des ISMS in sieben Phasen auf, beginnend mit der Aufbau- und Ablauforganisation. SiKoSH-Quickchecks prüfen in jeder Phase, wie gut die kommunalen Mindestanforderungen erfüllt sind und ermöglichen über eine Gewichtung der Einzelmaßnahmen einen schnellen Überblick über den aktuellen Sachstand. Sie zeigen, mit welchen Maßnahmen Quick-Wins erzielt werden können. Der jeweilige Umsetzungsstand kann direkt im Quickcheck dokumentiert werden.

Der SiKoSH-Standard „Einführung und Betrieb eines Informations-Sicherheits-Management-Systems (ISMS)“ führt den Anwender wie ein Kochbuch durch die sieben SiKoSH-Phasen und unterstützt kontextbezogen mit vielen Hilfsmitteln wie z. B. einer Muster-Informationssicherheitsleitlinie und zahlreichen Richtlinien, die als innerbehördliche Anleitungen zur Umsetzung der BSI-Bausteine herangezogen werden können.

SiKoSH richtet sich zwar primär an die Kommunalverwaltungen in Schleswig-Holstein, steht aber allen Interessierten kostenfrei zur Verfügung.

5.4. CISIS12

CISIS12[14] steht für „Compliance Informations-Sicherheits-Management-System in 12 Schritten“ und ist ein ISMS-Standard, der als Dienstleistungsprodukt durch den IT-Sicherheitscluster e. V. in Regensburg angeboten wird. Er besteht aus einem übersichtlichen Maßnahmenkatalog, der die relevanten technischen und organisatorischen Sicherheitsaspekte einer Organisation abdeckt.

[11] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Hilfsmittel/Profile/Basis_Absicherung_Kommunalverwaltung.html
[12] https://www.bsi.bund.de/dok/WIBA
[13] https://itvsh.de/sikosh/
[14] Website des IT-Sicherheitsclusters e. V. zum Angebot von CISIS12: https://cisis12.de/.

CISIS12 stellt die mittlerweile dritte Überarbeitung des bis dato ohne „C“ am Namensanfang bekannten Standards dar, der vorrangig im südöstlichen Deutschland bei kleinen und mittleren Unternehmen und auch in der öffentlichen Verwaltung verbreitet ist. Neben einigen grundlegenden Neuerungen gegenüber dem Vorgänger ISIS12 steht er dabei weiterhin für eine in zwölf Schritten erfolgende Einführung bzw. Pflege der Informationssicherheit. Mit dem „C“ sind gegenüber dem früheren Ansatz die Compliance sowie eine Prozessorientierung und die Betrachtung der Infrastruktur in den Blickpunkt gerückt. Die Anforderungen, Maßnahmenbeschreibungen und Handlungsanweisungen des CISIS12-Katalogs sind vor allem auf Verständlichkeit, Handhabbarkeit und Umsetzbarkeit ausgerichtet, allerdings nicht vollumfänglich kompatibel mit dem BSI IT-Grundschutz oder dem Vorgänger ISIS12. Dennoch kann CISIS12 als Grundlage zur späteren Vertiefung auf Basis des BSI IT-Grundschutzes oder zu einer Zertifizierung nach ISO/IEC 27001 genutzt werden. Zudem ist eine eigene Zertifizierung möglich. Teilweise wird CISIS12 für Kommunen und andere öffentliche Einrichtungen als geeignet empfohlen.[15]

5.5. VDS-RICHTLINIEN 10000

Die VdS[16] Schadenverhütung GmbH, ein Tochterunternehmen des Gesamtverbandes der Deutschen Versicherungswirtschaft e. V. (GDV), ist Herausgeber der kostenpflichtigen VdS-Richtlinien 10000 „Informationssicherheitsmanagementsystem für KMU (kleine und mittelständische Unternehmen)“.[17] Diese zielen vornehmlich auf die Wirtschaft ab, jedoch eignen sie sich inhaltlich und formal auch für öffentliche Einrichtungen.

Sie basieren auf ISO 27001 und dem BSI IT-Grundschutz, wobei die Anforderungen vielfach weniger konkret und damit in der Umsetzung flexibler sind. Der VdS wirbt damit, dass mit „ca. 20 % des Aufwandes im Vergleich zu ISO 27001 […] KMU aus den VdS-Richtlinien Maßnahmen und Prozesse ableiten [können], mit denen sie im IT-Bereich ein angemessenes Schutzniveau erreichen“. Zusätzlich sind die VdS-Richtlinien 10000 aufwärtskompatibel, so dass eine Überleitung in die ISO 27000er-Reihe bzw. zum BSI IT-Grundschutz möglich ist. Die VdS bietet eine Zertifizierung an.[18]

Die Richtlinien sind Grundlage der entsprechenden Zertifizierung durch VdS Schadenversicherer und umfassen auf knapp 40 Seiten unter anderem Maßnahmen zu den Bausteinen Organisation, ISLL und Sicherheitsrichtlinien, Personal, Wissen, kritische IT-Ressourcen, IT-Systeme, Netzwerke, Mobile Datenträger und weiteren Bausteinen. Formal sind die Maßnahmen so aufgebaut, dass durch eindeutige Vorgaben klar ist, welche davon zur Richtlinien-Konformität durchgeführt werden „MÜSSEN“, „SOLLTEN“ oder „KÖNNEN“. Dabei wird bei bestimmten Prozessen gelegentlich auf andere Standards zur Umsetzung der Maßnahmen verwiesen.

Außerdem bietet die VdS sog. Quick-Audits an, bei denen für die Bereiche Informationssicherheit und Datenschutz – basierend auf Selbstauskünften – kostenpflichtig Testate erteilt werden.[19]

[15] https://bdsg-externer-datenschutzbeauftragter.de/isis12/
[16] Abkürzung für „Vertrauen durch Sicherheit“
[17] https://vds.de/kompetenzen/cyber-security/zertifizierungen/informationssicherheits-und-datenschutzmanagement/vds-10000-informationssicherheit-fuer-kmu
[18] https://shop.vds.de/publikation/vds-10002
[19] https://vds.de/vds-quick-check

5.6. GEGENÜBERSTELLUNG

Die oben beschriebenen Standards sind hier tabellarisch gegenübergestellt, um die Unterschiede und ggf. die Vorzüge zu verdeutlichen.

Kriterien	VdS 10000	CISIS12	SiKoSH	ISO/IEC 27000-Reihe	BSI IT-Grundschutz[20]
Herausgeber	VdS Schadenverhütung GmbH	IT-Sicherheitscluster e. V.[21]	ITV.SH AöR	International Standards Organisation[22]	Bundesamt für Sicherheit in der Informationstechnik[23]
Zielgruppe	kleine und mittlere Unternehmen	kleine und mittlere Unternehmen, öffentliche Verwaltung, Hochschulen	Kommunalverwaltungen	Organisationen jeder Größenordnungen	Organisationen jeder Größenordnungen und öffentliche Verwaltung
Dokumentation	ca. 40 Seiten	Handbuch 35 Seiten, Katalog 976 Seiten, Norm 61 Seiten	Standard 50 Seiten; insgesamt ca. 70 Dokumente	ca. 400 Seiten	ca. 5.000 Seiten
Detaillierung	minimal verweisend	mittel, praxisnah	praxisnah	minimalistisch abstrakt	maximal detailliert
Aufbau	Selektierte Bausteine und Maßnahmen	Selektierte Bausteine und Maßnahmen	Bausteine und Maßnahmen der kommunalen Basisabsicherung	Maßnahmen-empfehlungen	umfassende Bausteine, Gefährdungen und Maßnahmen
Umfang des Maßnahmenkatalogs	ca. 18 Kapitel plus Anhang, ca. 100 Maßnahmen	ca. 400 Maßnahmen	entsprechend Grundschutzprofil Basisabsicherung Kommunalverwaltung	ca. 150 Maßnahmen	ca. 1.100 Maßnahmen

[20] Die Spalte stellt nur den vollständigen IT-Grundschutz dar, nicht seine Unterformen.
[21] https://cisis12.de/impressum/
[22] https://www.iso.org/standard/27001
[23] https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/it-grundschutz_node.html

Kriterien	VdS 10000	CISIS12	SiKoSH	ISO/IEC 27000-Reihe	BSI IT-Grundschutz[20]
Risikoanalyse	Verweise auf andere Regelwerke	Vorgesehen, indirekt beschrieben	entfällt (ausgelegt für Basisabsicherung mit normalem Schutzbedarf)	grundsätzlich	enthalten (ergänzend für höheren Schutzbedarf)
Umsetzung	Verweise auf andere Regelwerke; konkret formulierte Maßnahmen umsetzen	konkret formulierte Maßnahmen, teilweise Hinweis auf BSI IT-Grundschutz	Vorformulierte, anpassbare, behördenorientierte Richtlinien	allgemeingültig formulierte Maßnahmen umsetzen	Auswahl konkret formulierte Maßnahmen umsetzen
Mögliche Zertifizierung	VdS-Zertifizierung	CISIS12-Norm[24]	Basisabsicherung nach BSI-Grundschutz	ISO-Zertifizierung	ISO-Zertifizierung nach IT-Grundschutz
Bezug der Standards für Kommunen	ca. 80 EUR	kostenlos	kostenlos	ca. 300 EUR (ISO 27001+27002)	kostenlos

Tabelle 1: Gegenüberstellung ausgewählter ISMS-Standards

[24] https://cisis12.de/zertifizierung/

6. DIE LEITLINIE DES IT-PLANUNGSRATES

Die Leitlinie[25] des IT-Planungsrats trägt den Titel „Leitlinie für die Informationssicherheit in der öffentlichen Verwaltung“ und befasst sich mit der Etablierung eines einheitlichen und einvernehmlichen Mindestsicherheitsniveaus zwischen Bund und Ländern unter Berücksichtigung des Grundsatzes der Wirtschaftlichkeit. Die Leitlinie wurde 2013 erstellt und Anfang 2019 in der Fassung vom 06.12.2018 fortgeschrieben.

Dieses Kapitel analysiert den formalen Aufbau. Zusätzlich enthält der zweite Abschnitt eine mehr inhaltliche Diskussion der Forderungen aus der Leitlinie.

6.1. FORMALE EIGENSCHAFTEN

Die Leitlinie ist für Behörden und Einrichtungen der Verwaltungen des Bundes und der Länder verbindlich, den Kommunen wird ihre Anwendung empfohlen. Bei ebenenübergreifenden Verfahren oder IT-Infrastrukturen können die Vorgaben der Informationssicherheitsleitlinie auch auf Kommunalverwaltungen ausgedehnt werden.

Die Leitlinie gilt nicht für einen Informationsverbund (abgeschlossene Behörde oder Organisation), sondern dient dem IT-Planungsrat, der für die Vereinbarung gemeinsamer Mindestsicherheitsanforderungen zwischen Bund und Ländern zuständig ist, als Mittel, um ein einheitliches Mindestsicherheitsniveau zu etablieren.

Formal sind die Elemente einer ISLL vorhanden. Allerdings kann diese Leitlinie nicht als Blaupause für eine ISLL einer Kommunalverwaltung herangezogen werden, da sie nicht aus Sicht einer Behörde formuliert ist und wesentliche Elemente wie z. B. die konkrete Verpflichtung der Behördenleitung und eine möglichst direkte Ansprache der Beschäftigten nicht enthält und – aus Gründen der Zielrichtung – nicht enthalten kann.

Von Belang sind jedoch die Inhalte dieser Leitlinie, da sie zumindest im Falle einer direkten Anbindung an das Verbindungsnetz oder im Falle ebenenübergreifender Verfahren auch für Kommunalverwaltungen verbindlichen Charakter hat.

6.2. INHALTLICHE ASPEKTE

Die Leitlinie des IT-Planungsrates adressiert inhaltlich die Punkte einer ISLL, allerdings nicht in der allgemein bekannten Struktur und Reihenfolge. Sie benennt in Kapitel 5 Umsetzungsstrategie fünf Handlungsfelder mit Vorgaben:

- Informationssicherheits-Management,
- Absicherung der IT-Netzinfrastrukturen der öffentlichen Verwaltung,
- einheitliche Sicherheitsstandards für ebenenübergreifende IT-Verfahren,
- gemeinsame Abwehr von IT-Angriffen sowie
- IT-Notfallmanagement.

Die Festlegung des Mindestsicherheitsstandards orientiert sich am IT-Grundschutz des BSI, auch wenn eingangs des Kapitels 5 noch ergänzend auf die ISO 2700x-Reihe verwiesen wird.

INFORMATIONSSICHERHEITSMANAGEMENT

Das Kapitel 5.1 Informationssicherheitsmanagement beschreibt die Anforderungen an ein ISMS in den öffentlichen Verwaltungen von Bund und Ländern. Es legt fest, dass die Leitungsebene die Verantwortung für die Informationssicherheit trägt und sicherstellen muss, dass Risiken angemessen gemanagt und gesetzliche

[25] Stand 06.12.2018, beschlossen vom IT-Planungsrat in seiner 28. Sitzung am 12.03.2019.

Vorgaben eingehalten werden. Ein ISMS soll als Rahmenwerk dienen, um kontinuierlich Sicherheitsmaßnahmen zu planen, umzusetzen, zu kontrollieren und zu verbessern. Zu den Mindestanforderungen gehören die Festlegung und Dokumentation von Verantwortlichkeiten, die Erstellung verbindlicher Leitlinien und Sicherheitskonzepte, die Etablierung eines kontinuierlichen Verbesserungsprozesses sowie klare Abläufe für den Umgang mit Sicherheitsvorfällen. Zudem wird die regelmäßige Aus- und Weiterbildung der ISBs gefordert, wobei eine Zertifizierung angestrebt wird. Schließlich sollen alle Beschäftigten regelmäßig in Informationssicherheitsthemen sensibilisiert werden, um einen sicheren Umgang mit Informationen und IT-Systemen zu gewährleisten.

ABSICHERUNG DER IT-NETZINFRASTRUKTUREN DER ÖFFENTLICHEN VERWALTUNG

Für die Absicherung der IT-Netzinfrastrukturen in der öffentlichen Verwaltung wird gefordert, dass die von Bund und Ländern beschlossenen Anschlussbedingungen an das Verbindungsnetz des Bundes erfüllt und regelmäßig überprüft werden. Dabei sind die aktuellen IT-Grundschutzstandards des BSI anzuwenden. Zu den Mindestanforderungen gehört die Errichtung eines ISMS, das eine ISLL, eine/n ISB und ein Sicherheitskonzept für direkt angeschlossene Netze umfasst. Es wird die Erfüllung der Anforderungen an einen hohen Schutzbedarf für kritische Netzwerkverbindungen angestrebt. Abweichungen von den Sicherheitsanforderungen müssen dem IT-Planungsrat gemeldet werden. Zur Qualitätssicherung ist ein Prozess der gegenseitigen Überprüfung vorgesehen.

Die Anforderungen der Anschlussbedingungen für eine direkte Anbindung an das Verbindungsnetz sind also hoch. Die meisten Kommunalverwaltungen bevorzugen daher eine indirekte Anbindung über einen kommunalen IT-Dienstleister oder Zweckverband.

EINHEITLICHE SICHERHEITSSTANDARDS FÜR EBENENÜBERGREIFENDE IT-VERFAHREN

Für ebenenübergreifende IT-Verfahren, die von Bund und Ländern gemeinsam genutzt werden, sind einheitliche Sicherheitsstandards erforderlich, um ein akzeptables Restrisiko für alle Beteiligten zu gewährleisten. Der Datenaustausch über Verwaltungsgrenzen hinweg erfolgt gemäß den Vorgaben des Gesetzes über die Verbindung der informationstechnischen Netze des Bundes und der Länder (IT-NetzG) über das Verbindungsnetz. Bei kritischen IT-Verfahren müssen im Rahmen der Notfallvorsorge gemeinsame Rückfallebenen festgelegt werden. Es wird gefordert, dass der IT-Grundschutz des BSI angewendet wird und ein einheitlicher Prozess zur Erfassung und Pflege der IT-Verfahren etabliert wird, der auch wesentliche Aspekte der Informationssicherheit berücksichtigt.

Die Vorgaben zu ebenenübergreifenden Verfahren sind folgerichtig, können aber bei konservativer Auslegung des IT-Grundschutzes zu erheblichen Mehraufwänden bei Kommunalverwaltungen führen, wenn der IT-Grundschutz nicht bereits flächendeckend realisiert wurde.

GEMEINSAME ABWEHR VON IT-ANGRIFFEN

Kapitel 5.4 der Leitlinie beschreibt die Anforderungen an die gemeinsame Abwehr von IT-Angriffen in der öffentlichen Verwaltung. Da IT-Angriffe oft ganze Behörden oder Netzverbünde betreffen, sind eine enge Zusammenarbeit und ein effizienter Informationsaustausch zwischen den beteiligten Stellen unerlässlich. Der VerwaltungsCERT[26]-Verbund (VCV) von Bund und Ländern wird weiterentwickelt, um eine schnelle Information, Warnung und Alarmierung zu gewährleisten. Die bestehenden CERTs müssen personell und finanziell ausreichend ausgestattet sein und eng zusammenarbeiten. Es wird besonderer Wert auf den Schutz von

[26] CERT = Computer Emergency Response Team

Informationen und Quellen gelegt, um ein hohes Maß an Vertrauen zu gewährleisten. Zudem sollen die Verfahren für den automatisierten Informationsaustausch zwischen den CERTs weiterentwickelt und in die internen Prozesse integriert werden.

Die Weiterentwicklung des VCV ist zu begrüßen. Während bei den ebenenübergreifenden Verfahren die Vorgaben auf Kommunalverwaltungen ausgedehnt werden, besteht für die Beteiligten des VCV jedoch keine Pflicht, ihre Leistungen auch der kommunalen Ebene anzubieten.

IT-NOTFALLMANAGEMENT

Im Kapitel IT-Notfallmanagement wird die Etablierung von Prozessen zur Notfallvorsorge und Notfallbewältigung gemäß dem IT-Grundschutzstandard des BSI gefordert. Ziel ist es, durch präventive Maßnahmen die Robustheit und Ausfallsicherheit der IT-Systeme zu erhöhen, sodass die Verwaltungstätigkeiten auch in Krisensituationen fortgeführt werden können. Das IT-Notfallmanagement ist Teil eines umfassenden Krisenmanagements und soll eng mit allgemeinen Krisenbewältigungsprozessen verknüpft werden. Zudem wird eine enge Zusammenarbeit und Abstimmung mit den Arbeitsgremien der Innenministerkonferenz gefordert, um die Wirksamkeit des IT-Notfallmanagements durch gemeinsame Übungen und abgestimmte Verfahren zu verbessern.

Der Anspruch, dass ein IT-Notfallmanagement Teil des ganzheitlichen Notfall- oder Krisenmanagements von Bund und Ländern ist, wird durch die Vorgaben nur zum Teil eingelöst. Auch hier wäre die Einbindung der kommunalen Ebene notwendig, die bei ebenenübergreifenden Verfahren Verwaltungstätigkeiten übertragen bekommt.

6.3. FAZIT

Die Leitlinie formuliert hohe Anforderungen an die IT- und Informationssicherheit, die insbesondere für kleinere Kommunalverwaltungen eine Herausforderung darstellen können. Die Anschlussbedingungen für das Verbindungsnetz und die Vorgaben für ebenenübergreifende Verfahren könnten zu erheblichen Mehraufwänden führen, wenn der BSI IT-Grundschutz nicht bereits umfassend umgesetzt ist. Während die Weiterentwicklung des VCV positiv zu bewerten ist, fehlt es an einer verbindlichen Einbeziehung der kommunalen Ebene, sowohl beim Zugriff auf CERT-Leistungen als auch beim IT-Notfallmanagement. Insgesamt bleibt die Leitlinie in Bezug auf die Einbindung der Kommunalverwaltungen hinter den Erwartungen zurück und könnte diese in ihrer Umsetzungskapazität überfordern, ohne ihnen gleichzeitig ausreichende Unterstützung zu bieten. Kommunalverwaltungen ist daher zu empfehlen, sich an den BSI IT-Grundschutzstandards zu orientieren, die einen De-facto-Standard für die öffentliche Verwaltung darstellen. Einstiegshilfen wie WiBA, SiKoSH und das IT-Grundschutz-Profil Basis-Absicherung Kommunalverwaltung bieten eine fundierte Grundlage und einen guten Ausgangspunkt dafür.

7. EINFÜHRUNG EINES ISMS

Dieses Kapitel ist eine Hilfestellung für die Einführung eines ISMS. Konkret werden die wesentlichen Handlungsschritte mit den vier Phasen des PDCA-Modells (siehe Abbildung 2) aus strategischer Sicht dargestellt.

Auf die einzelnen Bestandteile der Informationssicherheitsstrategie wird jeweils gesondert eingegangen. Das Zusammenspiel dieser Bestandteile ist existentiell für ein funktionierendes ISMS.

Abbildung 3: Die Säulen und Bestandsteile des Sicherheitsprozesses[27]

7.1. PLANUNG (PLAN)

Bei der Festlegung der Sicherheitsziele und der Sicherheitsstrategie ist zu berücksichtigen, dass der Aufwand des Sicherheitsprozesses von der Größe der Behörde, der Ausgangssituation und den Sicherheitsanforderungen abhängt.

In einer sehr großen Behörde mit mehreren Hierarchieebenen sollte die für den Sicherheitsprozess notwendige Steuerung und Auditierung formal festgelegt werden. Dazu zählen insbesondere:

- welche Prüfungs- und Überwachungsmaßnahmen zu berücksichtigen sind,
- wer an wen zu welchen Themen der Informationssicherheit berichtet,
- wer Entscheidungsvorlagen zu erstellen hat und
- wann die Behördenleitung über den Sicherheitsprozess berät.

Dagegen kann in kleinen Verwaltungen der Erfolg des Sicherheitsprozesses kritisch begleitet werden, indem regelmäßige Gespräche zwischen der Behördenleitung und der eigenen IT bzw. den IT-Verantwortlichen stattfinden. Inhalt der Gespräche sollten unter anderem festgestellte Probleme, entstandene Kosten und technische Weiterentwicklungen sein.

[27] Vgl. BSI: BSI-Standard 200-1, Managementsysteme für Informationssicherheit (ISMS), 2017, Seite 17: Abbildung 4 – Umsetzung der Sicherheitsstrategie mit Hilfe des Sicherheitskonzepts und einer Informationssicherheitsorganisation.

Der Basisaufwand für ein ISMS wird so gestaltet, dass dieser sinnvoll und tragbar erscheint. IT-Grundschutz kann hierbei als Option gesehen werden. ISO 27001 genügt bei der erstmaligen Einführung eines skalierbaren ISMS. Ein Einstieg könnte über CISIS12 gesucht werden.

Zur Steuerung und Umsetzung sollte eine auf Informationssicherheit fachlich spezialisierte Person (ISB) benannt werden. Sofern die Ernennung einer solchen Person nicht in Frage kommt, kann das ISMS auch ohne diese eingeführt werden. Hierbei ist zu beachten, dass die Leitung eines IS-Management-Teams durch entsprechenden Sachverstand gewährleistet werden muss und die Behördenleitung, als für die Sicherheit verantwortliche Stelle, stärker einbezogen wird. Die Funktion der/des ISB kann auch an ein Dienstleistungsunternehmen übertragen werden. In jedem Fall müssen die Rollen und Verantwortlichkeiten klar definiert sein.

Die Behördenleitung muss jedoch individuell festlegen, konkretisieren und verantworten, in welcher Ausprägung der Sicherheitsprozess als angemessen gelten kann, unter Berücksichtigung der Gesetze, Richtlinien und betrieblichen Vereinbarungen. Festzulegen sind,

- die Sicherheitsziele und Rahmenbedingungen der eigenen Behörde,
- der Ablauf zur Behandlung von Risiken,
- die Verantwortungen und Zuständigkeiten,
- die Durchführung von Schulungen und Sensibilisierungen,
- die Planung von Überprüfungen, Notfallübungen und Reserven,
- der Prozess möglicher Veränderungen.

7.1.1. Informationssicherheitsleitlinie

Die behördliche ISLL[28] stellt die formale Grundlage zur Einführung eines ISMS dar. Sie wird von der Behördenleitung vorgegeben und sollte neben den Sicherheitszielen, also den Erwartungen und Anforderungen an die Beteiligten, auch den Umgang mit möglichen Risiken und die Verantwortlichkeiten behandeln.

Die ISLL sollte unter Berücksichtigung die beiden anderen Bestandteile (Sicherheitsorganisation und Sicherheitskonzept) des Sicherheitsprozesses erstellt werden. Die ISLL ist Teil des Sicherheitsprozesses und unterliegt einem Lebenszyklus, wobei sie regelmäßig aktualisiert bzw. fortgeschrieben werden sollte.

Eine ISLL sollte möglichst prägnant und übersichtlich die von ISO und BSI vorgegebenen Inhalte adressieren, d. h. die einzelnen Punkte sollten in eben dieser Form behandelt werden.

Stellenwert der Informationssicherheit und zu schützende Objekte

Es sollte zunächst eine kurze Darstellung erfolgen, dass heutiges Verwaltungshandeln mehr und mehr auf IT-Diensten beruht und auf diesen aufbaut. Die von der Behörde zu erhebenden und zu verarbeitenden Informationen werden größtenteils in IT-Systemen verarbeitet und gespeichert. Diese Informationen sind die wesentlichen zu schützenden Objekte der modernen Verwaltung.

Bezug der Informationssicherheit zu den Geschäftszielen oder Aufgaben der Institution

In der ISLL wird dargestellt, wie sich die Informationssicherheit und die behördenspezifischen Organisationsziele wechselseitig beeinflussen.

[28] Informationssicherheitsleitlinien wurden in der Vergangenheit auch unter der Bezeichnung „IT-Sicherheitsleitlinie“ erlassen.

Sicherheitsziele

In diesem Abschnitt können Sicherheitsziele aufgelistet werden, die über das allgemeine Ziel, ein geeignetes Niveau der Informationssicherheit zu erreichen, hinaus konkreter gefasst werden sollen (z. B. Vertraulichkeit, Integrität, Verfügbarkeit). Da es sich um eine Leitlinie handelt, sollte eine zu große Detailtiefe vermieden werden. Es kann auch ausreichen, aufzuzeigen, wie und unter welchen Rahmenbedingungen die Organisation die eigenen Ziele herleiten will.

Kernelemente der Sicherheitsstrategie

Hier wird aufgezeigt, wie die Organisation die Ziele erreichen will. Auch dies sollte auf einem hohen Abstraktionsniveau erfolgen. Zum Beispiel könnte hier aufgeführt werden, dass die Organisation ein Sicherheitsmanagement mit einem ISMS einführt und Sicherheitsrichtlinien erlässt.

Verpflichtung zur Umsetzung der ISLL

Wichtig ist, dass die Behördenleitung klar formuliert, dass sie hinter den Sicherheitszielen steht und unter Beachtung der Kompetenzen die benötigten Ressourcen zur Verfügung stellt.

Informationssicherheits-Organisation

Die ISLL sollte den Rahmen aufzeigen, wie das Thema Informationssicherheit in der Organisation verankert wird. Die Gesamtverantwortung für die Informationssicherheit liegt bei der Behördenleitung. Es kann zielführend sein, die Zuständigkeit für die Informationssicherheit zu delegieren. Hierfür kommen das IS-Management-Team und/oder der/die ISB in Betracht. Die Ausgestaltung der Informationssicherheits-Organisation hängt von der Größe und Komplexität der Behörde ab. Unter diesem Punkt kann auch auf die Verantwortung der Führungskräfte und aller Beschäftigten für das Erreichen der Sicherheitsziele explizit verwiesen werden. Auch disziplinarische Folgen können aufgeführt werden.

Verpflichtung zur kontinuierlichen Verbesserung

Es braucht eine klar formulierte Aussage zur Fortentwicklung der Strategie zur Informationssicherheit.

Inkraftsetzung

Hier erfolgt eine Darstellung, wie die ISLL in Kraft gesetzt wird.

7.1.2. Organisation der Informationssicherheit

Die Umsetzung der Informationssicherheit kann nicht allein durch die für die IT zuständige Organisationseinheit erfolgen. Es handelt sich vielmehr um eine interdisziplinäre Aufgabe, bei der neben der IT auch weitere Bereiche, beispielsweise Gebäudemanagement (z. B. Zutrittsregelungen, Notstrom), Organisation (z. B. Zuständigkeiten, Rechte), aber auch die Technik (z. B. Telekommunikation, Arbeitsplatzrechner) einzubeziehen sind.

Der Aufbau einer geeigneten Organisationsstruktur und eines Regelwerkes für das Sicherheitsmanagement hat wesentlichen Einfluss auf die Erreichung der gesteckten Sicherheitsziele. Praktisch ist es nicht möglich, eine für jede Behörde unmittelbar anwendbare Organisationsstruktur anzugeben. Hinzu kommt, dass regelmäßig Anpassungen an spezifische Gegebenheiten erforderlich sein können.

Abhängig von der Größe der Behörde sollte ein/e unabhängige/r ISB und ggf. ein IS-Management-Team benannt werden. Dabei ist es nicht ausreichend, eine/n ISB nur zu benennen. Dieser Person sind zur Wahrnehmung der Tätigkeiten auch ausreichende zeitliche Ressourcen zur Verfügung zu stellen. Mitglieder des IS-Management-Teams können unter anderem Verantwortliche der IT, des Gebäudemanagements und der Organisation sein. Bei

Bedarf sollten der/die Datenschutzbeauftragte (DSB) und ein/e Vertreter/in des Personalrates hinzugezogen werden.

Das IS-Management-Team sollte sich unter dem Vorsitz der/des ISB regelmäßig mit dem Ziel der kontinuierlichen Verbesserung der Informationssicherheit treffen. Weitere Aufgaben (beispielhaft), die durch die/den ISB bzw. das IS-Management-Team wahrgenommen werden sollten, sind:

- Einbindung und Steuerung des Sicherheitsprozesses,
- Entwickeln der Sicherheitsziele und Sicherheitsstrategie für die ISLL mit der Behördenleitung,
- Überprüfen der Umsetzung der ISLL,
- Festlegen von Schutzbedarfskategorien für Prozesse bzw. Informationen zur Verabschiedung durch die Behördenleitung,
- Entwickeln von Sicherheitskonzepten,
- Überprüfen der im Sicherheitskonzept geplanten Sicherheitsmaßnahmen auf Vollständigkeit, Funktionsfähigkeit und Wirksamkeit,
- Unterstützen der Wirtschaftlichkeitsbetrachtungen der Sicherheitsmaßnahmen,
- Entwickeln von Konzepten von Schulungen und Sensibilisierungen zur Informationssicherheit,
- Beraten und Unterrichten der Behördenleitung zu Themen der Informationssicherheit,
- Fortschreiben der Sicherheitsleitlinie und der Sicherheitskonzepte.

Um einen Interessenkonflikt und eine reine Selbstkontrolle zu vermeiden, sollte die Aufgabe der/des ISB mit Bedacht vergeben werden, da auch Interessenkonflikte Risiken für die Informationssicherheit darstellen. Die folgende Tabelle gibt Hinweise, inwieweit die Aufgabe der/des ISB mit anderen Rollen kombiniert werden kann.

Die nachfolgende Tabelle listet Rollen in alphabetischer Reihenfolge auf und **stellt keine Wertung oder Reihenfolge dar**.

Rolle/Aufgabenbereich	Beschreibung	Ernennung als ISB
Anwendungsverantwortliche	Zuständig für den reibungslosen Betrieb und ggf. Administration von Fachanwendungen	Nicht zu empfehlen, da Interessenkonflikt möglich
BCM-Beauftragte	Koordinierung von Maßnahmen zur Aufrechterhaltung und Wiederherstellung zeitkritischer Geschäftsprozesse im Krisenfall	Einige Überschneidungen, nur zu empfehlen, wenn ausreichende zeitliche Ressourcen vorhanden sind
Datenschutzbeauftragte	Verantwortlich für den gesetzeskonformen Umgang mit personenbezogenen Daten[29]	Einige Überschneidungen, Vereinbarkeit wird wegen möglicher Interessenkonflikte von vielen verneint
Digitalisierungsbeauftragte	Koordiniert und steuert Digitalisierungsprojekte	Nicht zu empfehlen, da Interessenkonflikt möglich
Geheimschutzbeauftragte	Durchführung und Beachtung der VS-Anweisung, Beratung der Behörde in allen Fragen des Geheimschutzes	Wenige Überschneidungen auf kommunaler Ebene. Ggf. möglich, wenn ausreichende Ressourcen vorhanden sind
IT-Betrieb/Administration	Betreibt, überwacht und wartet IT-Systeme	Nicht zu empfehlen, da Interessenkonflikt möglich
IT-Leitung	Ist verantwortlich für die Organisation der IT und deren Betrieb	Nicht zu empfehlen, da Interessenkonflikt möglich[30]
Personalrat	Vertritt die Interessen der Mitarbeitenden gegenüber der Behördenleitung	Nicht möglich
Revision/Rechnungsprüfungsamt	Kontrolliert, ob geplanten Maßnahmen wirtschaftlich und sparsam umgesetzt wurden, um den ordnungsgemäßen und sicheren Einsatz zu gewährleisten[31]	Nicht zu empfehlen, da Interessenkonflikt möglich
Rechtsabteilung	Berät, ob Sicherheitsmaßnahmen rechtlich umgesetzt werden dürfen, da die Komplexität von Gesetzen um das Thema Informationssicherheit gelegentlich schwer zu bewerten ist	Möglich, wenn ausreichend technisches Verständnis und Unabhängigkeit in der Organisation gewährleistet werden können

Tabelle 2: Vereinbarkeit verschiedener Rollen mit der der/des ISB

[29] https://www.bsi.bund.de/dok/10027846, S. 42 ff.
[30] Vgl. LAG Düsseldorf, Urteil vom 23.07.2012, Az. 9 Sa 593/12
[31] https://www.bundesrechnungshof.de/SharedDocs/Downloads/DE/ver%C3%B6ffentlichungen_brh_lrh/it-mindestanforderungen.pdf?__blob=publicationFile&v=4; http://www.diir.de/fachwissen/revisionshandbuch-marisk/

Erfahrungen aus den Sicherheitsvorgaben zu den EU-Zahlstellen und dem Nationalen Waffenregister (NWR) haben gezeigt, dass einzelne Sicherheitsvorgaben Einfluss auf Behörden-übergreifende Prozesse haben können. Es ist sinnvoll, die daran Beteiligten an den Planungen zu beteiligen.

Informationssicherheit kann nicht allein durch die IT sichergestellt werden. Technische Maßnahmen allein zeigen kaum Wirkung, wenn diese nicht genutzt oder womöglich umgangen werden können. Es müssen beispielsweise Angriffe auf das Behördennetzwerk, Datendiebstähle und auch menschliches Fehlverhalten bedacht und verhindert werden. Technik sollte dabei immer der Organisation folgen.

7.1.3. Sicherheitskonzeption und Sicherheitskonzept

Wesentlicher Bestandteil der Planung ist die Erstellung eines Sicherheitskonzeptes, das den IST-Stand der maßgeblichen Geschäftsprozesse einer Behörde und die diese unterstützende Infrastruktur, IT-Systeme und Anwendungen abbildet. Hierbei sind die jeweiligen Schutzbedarfe und die bereits vorhandenen Sicherheitsmaßnahmen zu dokumentieren. Die Erstellung einer Sicherheitskonzeption ist detailliert in BSI-Standard 200-2 IT-Grundschutz-Methodik beschrieben.

Die Sicherheitsorganisation und das Sicherheitskonzept müssen nach Planung und Umsetzung einer Prüfung unterzogen werden. Dabei werden die Eignung und Effizienz der umgesetzten Maßnahmen und eine eventuelle Veränderung der Rahmenbedingungen (z. B. Organisationsziele oder Gesetze) betrachtet.

Fehlende Maßnahmen und deren Umsetzung sind in einem weiteren Schritt (DO) zu planen. Dazu zählen insbesondere auch die Sicherheitsmaßnahmen, die aus einer Risikoanalyse heraus entwickelt wurden.

7.2. UMSETZUNG (DO)

7.2.1. Informationssicherheitsleitlinie (MUSTERTEXTE)

Nachfolgend wird auf den Aufbau und den Inhalt einer ISLL speziell eingegangen, wobei der Text als Vorlage für die Erstellung einer behördenspezifischen ISLL genutzt werden kann.

In eckigen Klammern dargestellter Text ist durch eigene Angaben der Behörde zu ersetzen.

Die nachfolgend angegebenen Textvorschläge können nach eigenem Ermessen und in Abhängigkeit der Größe der Behörde ausgewählt werden. Die Einleitung zu einem Textbaustein und der nichtzutreffende Textbaustein sind zu entfernen.

Die Definition der Schutzbedarfskategorien können in einer Anlage (siehe Tabelle 3 und Tabelle 4) dargestellt werden.

> ***Stellenwert der Informationssicherheit und der zu schützenden Objekten***
>
> *Die [Name der Behörde] besitzt eine enorme Aufgabenvielfalt – von der Daseinsfürsorge bis zu Dienstleistungen für Bürgerinnen und Bürger – die zusätzlich permanenten Änderungen unterliegt. Eine wirtschaftliche, zeitnahe Aufgabenerfüllung stützt sich dabei zunehmend auf die Möglichkeiten der Informationstechnologien.*
>
> *Aufgaben, Prozesse und die Aufbauorganisation unterliegen einem stetigen Wandel und einer Anpassung der technischen Möglichkeiten.*
>
> *In Abwägung der zu schützenden Werte, der gesetzlichen Anforderungen, Informationen und der damit verbundenen Risiken wird ein angemessenes Informationssicherheitsniveau geschaffen.*

Modernes Verwaltungshandeln erfordert den Einsatz aktueller Informationstechnologien, um die Aufgabenerfüllung der Kommunalverwaltung im Sinne der Bürgerinnen und Bürger, ortsansässiger Unternehmen oder weiterer Partner effizient und effektiv zu gestalten. Dies trifft auch auf die [Name der Behörde] zu. Beim Einsatz von Informationstechnologie muss die [Name der Behörde] darauf achten, dass der Sensibilität der ihr übertragenen und von ihr verarbeiteten Informationen mit der nötigen Sorgfalt Rechnung getragen wird. Die Informationssicherheit wird in zunehmendem Maße zu einer unverzichtbaren Grundlage für ein Verwaltungshandeln, dem die Bürgerinnen und Bürger, die Unternehmen und alle unsere Partner ihr Vertrauen schenken können. Daher muss sich die [Name der Behörde] dem Thema Sicherheit in der Informationstechnik in geeigneter Form stellen und die verarbeiteten Informationen geeignet schützen.

Bezug der Informationssicherheit zu den Geschäftszielen oder Aufgaben der Institution

Es ist notwendig, das Zusammenspiel der Informationen, IT-Fachverfahren, Aufgaben und Produkte sowie der Infrastruktur der Informationstechnik und Kommunikationskanälen ganzheitlich zu betrachten. Informationssicherheit umfasst die Summe aller organisatorischen, personellen und technischen Maßnahmen, um diese Ziele zu erreichen.

Sowohl bei der Erbringung der Pflichtaufgaben als auch der Aufgaben, die die [Name der Behörde] auf freiwilliger Basis übernimmt, werden Informationen erhoben und verarbeitet, deren Vertraulichkeit, Integrität und Verfügbarkeit ein hohes Gut darstellen. Hierbei handelt es sich z. B. um Daten, die entsprechend gesetzlicher Anforderungen geschützt werden müssen, oder auch um wettbewerbsrelevante Informationen ortsansässiger Unternehmen, die Unberechtigten nicht bekannt werden dürfen.

Sicherheitsziele

Für den IT-Einsatz sind die Grundwerte der Informationssicherheit – Vertraulichkeit, Integrität und Verfügbarkeit – im jeweils erforderlichen Maße zu erreichen.

Jede Leistung, Aufgabe oder Information wird nach einem Schutzbedarf eingestuft. Die Einstufung gibt die Anforderungen bezüglich der Grundwerte wieder. Die Feststellung des Schutzbedarfes erfolgt gemäß der [Anlage Schutzbedarfskategorien].

Damit ist es ein grundlegendes Ziel der Aufgabenerfüllung, die Schutzbedürfnisse der verarbeiteten Informationen zu wahren. Über geeignete Sicherheitsmaßnahmen muss dafür gesorgt werden, dass die Vertraulichkeit, die Integrität und die Verfügbarkeit der Informationen ihrem Schutzbedarf entsprechend gewährleistet werden können. Hierbei sind rechtliche Bestimmungen zu berücksichtigen. Um dies in einer auch wirtschaftlich angemessenen Form zu tun, ist es unabdingbar, den Schutzbedarf der Informationen zu kennen und dann die zu diesem Schutzbedarf passenden Maßnahmen zu ergreifen.

Neben den Informationen müssen auch [weitere Schutzobjekte benennen, falls diese explizit erwähnt werden sollen].

Kernelemente der Sicherheitsstrategie

Die ISLL ist ein Rahmenwerk.

Die [Name der Behörde] erlässt nach Bedarf weitere Richtlinien zur Aufrechterhaltung der Informationssicherheit. Die Kommunalverwaltung führt eine Bedarfsermittlung durch und legt die Mindestsicherheitsstandards für ihre eigenen Verfahren fest. Bei ebenenübergreifenden Verfahren sind die entsprechenden Festlegungen des Bundes oder des Landes umzusetzen.

Als zentrale Sicherheitsinstanz ernennt die Behördenleitung eine/n Informationssicherheitsbeauftragte/n (ISB) und eine Stellvertretung. Diese Personen sind für alle Belange und Fragen der Informationssicherheit zuständig.

Die/der ISB ist unabhängig und weisungsfrei. Er/Sie ist der Behördenleitung in dieser Rolle direkt unterstellt. Berichtswege sind festzulegen.

Ein Austausch mit der Leitung der Informationstechnik findet regelmäßig statt.

Der/dem ISB sind geeignete Qualifizierungsmaßnahmen zu ermöglichen, um ihre/seine Verantwortung fachlich und zeitlich zu erfüllen.

Ein Informationssicherheits-Managementsystem (ISMS) ist zu etablieren. In regelmäßigen Abständen ist zu prüfen, ob die ausgewählten Sicherheitsmaßnahmen noch ausreichend sind. Die/der ISB leitet das IS-Management-Team und entwickelt die notwendigen Maßnahmen fort.

Bei Gefahr im Verzug ist die/der ISB oder die Stellvertretung berechtigt, erforderliche Sicherheitsmaßnahmen auch kurzfristig umzusetzen oder anzuordnen. Das kann bis zur vorübergehenden Sperrung von Anwendungen oder Netzübergängen führen.

Personen und Unternehmen, die nicht zur [Name der Behörde] gehören, für diese aber Leistungen erbringen (Auftragnehmende), haben die Vorgaben der [Name der Behörde] (Auftraggebende) zur Einhaltung der Informationssicherheitsziele gemäß dieser ISLL einzuhalten. Die Auftraggebende informiert die/den Auftragnehmende/-n über diese Regeln und verpflichtet sie/ihn in geeigneter Weise zur Einhaltung.

Sicherheitsanforderungen von übergeordnetem Interesse, für deren Umsetzung eine vertragliche oder gesetzliche Verpflichtung besteht, sind zu erfüllen. Entsprechende Vorschriften und Maßnahmen stellen den Mindeststandard bei der Formulierung behördeninterner Vorschriften und Maßnahmen dar. Gemeinsame Basiskomponenten innerhalb der Behörde zur Vereinfachung und Stärkung der ebenenübergreifenden Verfahren sind zu nutzen.

Die Beschäftigten werden regelmäßig zu Fragen der Informationssicherheit sensibilisiert und qualifiziert.

Die vorliegende ISLL gibt den Rahmen für das Management der Informationssicherheit bei der [Name der Behörde] vor. Die wesentlichen Eckpunkte und Kernelemente der Strategie zur Informationssicherheit sind:

Textvorschlag 1 für eine mittlere bis große Kommunalverwaltung:

Die [Name der Behörde] etabliert ein ISMS mit einem geeigneten Werkzeug zur Steuerung.

Die [Name der Behörde] verankert das Thema Informationssicherheit in der Organisation über

- *eine geeignete Informationssicherheits-Organisation, die aktiv das Thema Informationssicherheit betreibt,*

- *klar formulierte Sicherheitsvorgaben, die für alle Beschäftigten verbindlich sind,*
- *die Integration von Sicherheitsaspekten in alle aus Sicht der Informationssicherheit relevanten Prozesse,*
- *kontinuierliche und flächendeckende Sensibilisierungsmaßnahmen für alle Beschäftigten.*

Die [Name der Behörde] sorgt sukzessive für eine Absicherung der IT-Infrastruktur durch Umsetzung geeigneter Sicherheitsmaßnahmen auf der Infrastrukturebene.

Die [Name der Behörde] orientiert sich bei allen Aktivitäten zur Informationssicherheit an den aktuellen Standards und Best Practices.

Textvorschlag 2 für eine kleine Kommunalverwaltung:

Die für die [Name der Behörde] notwendigen Themen eines Informationssicherheits-Managements werden in angemessener Form adressiert. Hierzu wird ein/e ISB ernannt, die/der die notwendigen Maßnahmen mit der Behördenleitung abstimmt und für deren Umsetzung verantwortlich zeichnet.

Verpflichtung zur Umsetzung der ISLL

Die Behördenleitung trägt die Gesamtverantwortung für die Informationssicherheit. Es obliegt ihr, für die Umsetzung der Maßnahmen zur Gewährleistung der Informationssicherheit zu sorgen und die dafür benötigten Ressourcen bereitzustellen.

Die [Name der Behörde] orientiert sich für die Umsetzung von Informationssicherheit am IT-Grundschutz und der Norm ISO/IEC 27001 der „International Organization for Standardization" (ISO), der mindestens dem Standard-Schutzbedarf des BSI IT-Grundschutzes entspricht.

Der Aufwand für die Bereitstellung von Personal und Finanzmitteln zur Gewährleistung der Informationssicherheit soll für die eingesetzten und geplanten IT-Systeme ein angemessenes Informationssicherheitsniveau schaffen. Zur Umsetzung der Maßnahmen sind erforderliche Ressourcen und Investitionsmittel einzuplanen.

Die Sicherheitsmaßnahmen müssen in einem wirtschaftlich vertretbaren Verhältnis zum Schaden stehen, der durch Sicherheitsvorfälle verursacht werden kann. Dieser definiert sich durch den Wert der zu schützenden Informationen und der IT-Systeme selbst. Zu bewerten sind die Auswirkungen auf die körperliche und seelische Unversehrtheit von Menschen, das Recht auf informationelle Selbstbestimmung, finanzielle Schäden, Beeinträchtigung der Aufgabenerfüllung, Beeinträchtigungen des Ansehens der Behörde und die Folgen von Gesetzesverstößen.

Es sind Regelungen für ein angemessenes Risikomanagement und ein internes Kontrollsystem (IKS) zu berücksichtigen. Die Behördenleitung ist zu informieren, falls notwendige Sicherheitsmaßnahmen aus bestimmten Gründen nicht umgesetzt werden können.

Informationssicherheits-Organisation

Für bereits betriebene und für geplante Informationstechnik sind Sicherheitskonzepte zu erstellen. Der Schutzbedarf ist zunächst aus fachlicher Sicht für die Leistungen und Aufgaben zu erstellen. Anschließend wird der Schutzbedarf auf die Zielobjekte der Informationstechnik und Infrastruktur übertragen (vererbt).

Die Maßnahmen sind auch dann umzusetzen, wenn sich Beeinträchtigungen für die Nutzung ergeben. Bleiben Risiken untragbar, ist an dieser Stelle auf den Einsatz von Informationstechnik zu verzichten.

Die Verantwortlichen haben bei Verstößen und Beeinträchtigungen die zur Aufrechterhaltung des Betriebes und der Informationssicherheit geeigneten und angemessenen Maßnahmen zu ergreifen.

Unabhängig davon, ob und in welcher Weise Teilaufgaben delegiert werden, verbleibt die Gesamtverantwortung für die Gewährleistung der Informationssicherheit immer bei der Behördenleitung.

Textvorschlag 1 für eine mittlere oder große Kommunalverwaltung:

Die Behördenleitung kann die Verantwortung für die laufenden Angelegenheiten zum Informationssicherheits-Management an eine oder mehrere Verantwortliche in der [Name der Behörde] delegieren. Sie ernennt eine Person als zuständig für die Informationssicherheit der gesamten Kommunalverwaltung. Das ISMS wird durch ein IS-Management-Team aufgebaut und betrieben, das die für das Informationssicherheits-Management notwendigen Aufgaben und Maßnahmen definiert und koordiniert. Hierzu gehören auch Vorschläge für die weitere Ausgestaltung der Informationssicherheits-Organisation. Die Informationssicherheit gehört zu den Dienstpflichten aller Beschäftigten. Nur wenn alle Beschäftigten ihre Verantwortung in der täglichen Arbeit wahrnehmen, kann ein geeignetes Niveau der Informationssicherheit erreicht werden.

Textvorschlag 2 für eine kleine Kommunalverwaltung:

Die Behördenleitung ernennt eine/n ISB, die/der alle notwendigen Maßnahmen mit der Behördenleitung abstimmt und für deren Umsetzung verantwortlich zeichnet. Die Informationssicherheit gehört zu den Dienstpflichten aller Beschäftigten. Nur wenn alle Beschäftigten ihre Verantwortung in der täglichen Arbeit wahrnehmen, kann ein geeignetes Niveau der Informationssicherheit erreicht werden.

Verpflichtung zur kontinuierlichen Verbesserung

Die Behördenleitung verpflichtet sich, sich an der Optimierung der Informationssicherheit zu beteiligen. Sie ist regelmäßig bzw. im Einzelfall akut über den aktuellen Sicherheitszustand durch die/den ISB zu informieren und ist für die Absicherung der Kontinuität des Sicherheitsprozesses verantwortlich.

Die Sicherheitsmaßnahmen sind regelmäßig daraufhin zu untersuchen, ob sie den betroffenen Beschäftigten bekannt, umsetzbar und in den Betriebsablauf integrierbar sind.

Zur Erhaltung und Verbesserung der Informationssicherheit bedient sich die/der ISB einer Arbeitsgruppe "Informationssicherheit", die aus Vertretern der Ämter oder Fachbereiche besteht.

Die/der ISB ist bei allen organisatorisch-technischen Neuerungen oder Änderungen, die Auswirkungen auf die Informationssicherheit haben können, frühzeitig einzubinden. Sie/Er hat ein Vetorecht.

Durch eine kontinuierliche Betrachtung der Regelungen und deren Einhaltung wird das angestrebte Sicherheitsniveau sichergestellt. Abweichungen werden mit dem Ziel analysiert, die Informationssicherheit zu verbessern und ständig auf dem aktuellen Stand zu halten.

Verantwortlich für die Weiterentwicklung der ISLL und der IT-Sicherheitskonzepte ist die/der ISB, wobei sie/er von den Fachverantwortlichen bestmöglich unterstützt wird. Die Beschäftigten sind angehalten, mögliche Verbesserungen oder Schwachstellen an die entsprechenden Stellen weiterzugeben.

Informationssicherheit ist kein unveränderlicher Zustand, sondern hängt von vielen internen und externen Begebenheiten und Einflüssen ab, wie z. B. neuen Bedrohungen, neuen Gesetzen oder auch der Entwicklung neuer technischer Lösungen. Diesen Entwicklungen müssen sich die Ansätze zum Management der Informationssicherheit anpassen. Aus diesem Grund muss dafür Sorge getragen werden, dass sich die Sicherheitsstrategie der [Name der Behörde] kontinuierlich fortentwickelt.

Inkraftsetzung

Diese ISLL gilt für die gesamte Behörde.

Die ISLL tritt mit Unterschrift der Behördenleitung/Wirkung vom […] in Kraft und wird allen Beschäftigten nach Unterschrift umgehend zur Kenntnis gebracht.

Anlage Schutzbedarfsdefinition

Definition der Schutzbedarfskategorien

Ziel: Auswahl eines dreistufigen Bewertungsmodells für die Schutzbedarfskategorien in Anlehnung an den IT-Grundschutz nach BSI-Standard 200-2 für die Grundwerte der Informationssicherheit: Vertraulichkeit, Integrität und Verfügbarkeit.

Schutzbedarf	*Schadensauswirkung*
Normal	*Die Schadensauswirkungen sind begrenzt und überschaubar.*
Hoch	*Die Schadensauswirkungen können beträchtlich sein.*
Sehr hoch	*Die Schadensauswirkungen können ein existentiell bedrohliches, katastrophales Ausmaß erreichen.*

Tabelle 3: Schutzbedarfsdefinition

Hinweise zur Festlegung

Folgende Schadensszenarien sind zu berücksichtigen. Im Einzelfall wird geprüft, ob ggf. weitere Schadensszenarien möglich sind:

a. *Beeinträchtigung von Leib- und Leben (persönliche Unversehrtheit)*
b. *Verursachung finanzieller Schäden (Grundsatz der Wirtschaftlichkeit und Sparsamkeit)*
c. *Beeinträchtigung des Ansehens der Behörde*
d. *Verletzung des Rechts auf informationelle Selbstbestimmung (Datenschutzgesetze)*
e. *Verletzung von Gesetzten, Vorschriften oder Verträgen*
f. *Beeinträchtigung der Aufgabenerfüllung (intern, extern)*

Es können ein oder mehrere Schadensszenarien einzeln oder zur gleichen Zeit auftreten.

Verantwortlich für die Festlegung ist der Prozessverantwortliche. Zur Unterstützung bei dieser Abgrenzung ist eine enge Kommunikation mit der Behördenleitung erforderlich. Die Notwendigkeit der Einbindung der IT-Leitung, der/des ISB oder des/der Datenschutzbeauftragten (DSB) ist zu empfehlen.

Schutzbedarfsfeststellung und Schlussfolgerungen nach BSI-Standard 200-2 „IT-Grundschutz-Vorgehensweise“

(Für jedes der Schutzziele **„Vertraulichkeit“**, **„Integrität“** und **„Verfügbarkeit“** gesondert anzuwenden.)

Schutzbedarfs-kategorien Schadens-szenarien	**„normal“** *Die Schadensauswirkungen sind begrenzt und überschaubar.*	**„hoch“** *Die Schadensauswirkungen können beträchtlich sein.*	**„sehr hoch“** *Die Schadensauswirkungen können ein existentiell bedrohliches, katastrophales Ausmaß erreichen.*
1. Verstoß gegen Gesetze/Vorschriften/ Verträge	• Verstöße gegen Vorschriften und Gesetze mit geringfügigen Konsequenzen • Geringfügige Vertragsverletzungen mit maximal geringen Konventionalstrafen	• Verstöße gegen Vorschriften und Gesetze mit erheblichen Konsequenzen • Vertragsverletzungen mit hohen Konventionalstrafen	• Fundamentaler Verstoß gegen Vorschriften und Gesetze • Vertragsverletzungen, deren Haftungsschäden ruinös sind
2. Beeinträchtigung des informationellen Selbstbestimmungsrechts	• Es handelt sich um personenbezogene Daten, durch deren Verarbeitung der Betroffene in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen beeinträchtigt werden kann.	• Es handelt sich um personenbezogene Daten, bei deren Verarbeitung der Betroffene in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen erheblich beeinträchtigt werden kann.	• Es handelt sich um personenbezogene Daten, bei deren Verarbeitung eine Gefahr für Leib und Leben oder die persönliche Freiheit des Betroffenen gegeben ist.
3. Beeinträchtigung der persönlichen Unversehrtheit	• Eine Beeinträchtigung erscheint nicht möglich.	• Eine Beeinträchtigung der persönlichen Unversehrtheit kann nicht absolut ausgeschlossen werden.	• Gravierende Beeinträchtigungen der persönlichen Unversehrtheit sind möglich. • Gefahr für Leib und Leben
4. Beeinträchtigung der Aufgabenerfüllung	• Die Beeinträchtigung würde von den Betroffenen als tolerabel eingeschätzt werden. • Die maximal tolerierbare Ausfallzeit ist größer als 24 Stunden.	• Die Beeinträchtigung würde von einzelnen Betroffenen als nicht tolerabel eingeschätzt. • Die maximal tolerierbare Ausfallzeit liegt zwischen einer und 24 Stunden.	• Die Beeinträchtigung würde von allen Betroffenen als nicht tolerabel eingeschätzt werden. • Die maximal tolerierbare Ausfallzeit ist kleiner als eine Stunde.
5. Negative Innen- oder Außenwirkung	• Eine geringe bzw. nur interne Ansehens- oder Vertrauens-beeinträchtigung ist zu erwarten.	• Eine breite Ansehens- oder Vertrauensbeeinträchtigung ist zu erwarten.	• Eine landesweite Ansehens- oder Vertrauensbeeinträchtigung, eventuell sogar existenzgefährdender Art, ist denkbar.
6. Finanzielle Auswirkungen	• Der finanzielle Schaden bleibt für die Institution tolerabel.	• Der Schaden bewirkt beachtliche finanzielle Verluste, ist jedoch nicht existenzbedrohend.	• Der finanzielle Schaden ist für die Institution existenzbedrohend.
Schlussfolgerungen	*Standard-Sicherheitsmaßnahmen nach IT-Grundschutz sind **im Allgemeinen ausreichend und angemessen**.*	*Standard-Sicherheitsmaßnahmen nach IT-Grundschutz bilden einen **Basisschutz**, sind aber **unter Umständen alleine nicht ausreichend**. Weitergehende Maßnahmen können durch eine **Risikoanalyse** ermittelt werden.*	*Standard-Sicherheitsmaßnahmen nach IT-Grundschutz bilden einen **Basisschutz**, sind aber **alleine im Allgemeinen nicht ausreichend**. Die erforderlichen zusätzlichen Sicherheitsmaßnahmen müssen **individuell durch eine Risikoanalyse** ermittelt werden.*

Tabelle 4: Schutzbedarfsfeststellung und Schlussfolgerungen

7.2.2. Übergreifende Aspekte der Informationssicherheit

Die IT-Grundschutz-Bausteine des BSI-Grundschutzes sind zehn verschiedenen Themenbereichen zugeordnet, den sogenannten Schichten. Dazu zählen etwa „Organisation und Personal (ORP)“, „IT-Systeme (SYS)“, „Anwendungen (APP)“ oder „Detektion und Reaktion“ (DER). Neben technischen Aspekten werden auch Sicherheitsaspekte zu Infrastruktur, Organisation und Personal berücksichtigt. Der Aufbau ist stets gleich: Nach einer Einführung in die jeweilige Thematik werden exemplarische Gefährdungen benannt und danach die Sicherheitsanforderungen erläutert.

Mit diesen Bausteinen lässt sich ein Regelwerk für die Informationssicherheit hinreichend aufbauen bzw. lassen sich bestehende Regelungen dahingehend anpassen.

Art und Umfang der Regelungen richten sich nach den behördenspezifischen Rahmenbedingungen, den Sicherheitszielen sowie den zu berücksichtigenden Bausteinen der jeweiligen Schichten des IT-Grundschutzes.

Als Beispiel sei der Baustein „OPS.2.3 Nutzung von Outsourcing“ genannt, in dem elf Gefährdungen und 25 korrespondierende Anforderungen gelistet sind (Stand: Februar 2023). Dieser ist entbehrlich, wenn keiner der vorhandenen oder geplanten Geschäftsprozesse in der Behörde an externe Dienstleister vergeben wurde.

Darüber hinaus sind mehrere Bausteine während der Planungsphase nur einmal anzuwenden. Das bedeutet, dass die dafür notwendigen Regelungen an zentraler Stelle nur einmal erarbeitet werden müssen. Dazu zählen u.a. die Prozessbausteine zum Sicherheitsmanagement, der Organisation, des Personals, der Sensibilisierung und Schulung, zum Datensicherungskonzept, für das Löschen und Vernichten von Daten sowie die zum Schutz vor Schadprogrammen. Natürlich ist die Umsetzung der Regelungen regelmäßig zu prüfen und ggf. anzupassen. Diese Aufgabe lässt sich jedoch in bereits bestehende Managementprozesse integrieren.

7.2.3. Priorisierung und Abgrenzung kritischer Prozesse und Informationen

Ein funktionierendes Sicherheitsmanagement ist dadurch gekennzeichnet, dass im Hinblick auf das Schadenspotenzial kritische Geschäftsprozesse und Informationen bereits in der Planungsphase erfasst und im Sicherheitsprozess vorrangig berücksichtigt werden, da für diese in der Regel höhere Anforderungen an die Grundwerte der Informationssicherheit (Vertraulichkeit, Integrität und Verfügbarkeit) bestehen.

Hierfür sind die Prozesse bzw. Informationen und deren Schutzbedarf zu erfassen. Der Schutzbedarf kann durch die drei Kategorien „normal“, „hoch“ und „sehr hoch“ abstrakt und allgemeinverständlich dargestellt werden. Die Festlegung der Kategorien basiert auf der Betrachtung möglicher Schadensauswirkungen für die Kommunalverwaltung. Je höher mögliche Schäden ausfallen können, desto kritischer ist der genutzte Prozess bzw. der Umgang mit den Informationen.

Der/Die ISB bzw. das IS-Management-Team sollte die Schutzbedarfskategorien erarbeiten und der Behördenleitung zur Entscheidung vorlegen. Dieser Ablauf ist auch bei der Priorisierung der Prozesse und Verfahren zweckmäßig.

7.2.4. Sicherheitskonzepte

Das Sicherheitskonzept ist ein Hilfsmittel zur Umsetzung der Sicherheitsstrategie. Bei der Erarbeitung von Sicherheitskonzepten kann das PDCA-Modell genutzt werden, da diese auch einem Lebenszyklus unterliegen.

Im Sicherheitskonzept werden die Abhängigkeiten zwischen den Geschäftsprozessen (Aufgabenerfüllung) und den Gefährdungen (Höhere Gewalt, technische Mängel, menschliche Fehlhandlungen, etc.) analysiert, und es werden geeignete Anforderungen zur Vermeidung, Reduzierung, Überwälzung oder Übernahme der erkannten Risiken ermittelt sowie geeignete Maßnahmen zur erforderlichen Risikobehandlung festgelegt. Die damit

verbundenen Aufgaben sollten durch einen dafür qualifizierten Beschäftigten wahrgenommen werden, wobei die Qualitätssicherung und Kontrollmöglichkeiten unabhängig bleiben sollten, z. B. durch die/den ISB.

Bei der Dokumentation von Sicherheitskonzepten besteht in der Regel Formfreiheit. Einen ersten öffentlichen Entwurf zur IT-Grundschutz-konformen Dokumentation hat das BSI zur Verfügung gestellt.[32]

Zur Erstellung, Verwaltung, Fortschreibung und Dokumentation von Sicherheitskonzepten nennt das BSI zudem entsprechende Tools[33] auf seinen Internetseiten.

[32] Erster öffentlicher Entwurf IT-Grundschutz-konforme Dokumentation (FAQ und Hilfsmittel zur Dokumentation im IT-Grundschutz Stand Kompendium 2023): https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Drafts/Community_Draft/IT_Grundschutz_konforme_Doku_FAQ.html

[33] https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/Alternative-IT-Grundschutztools/IT-Grundschutztools_node.html

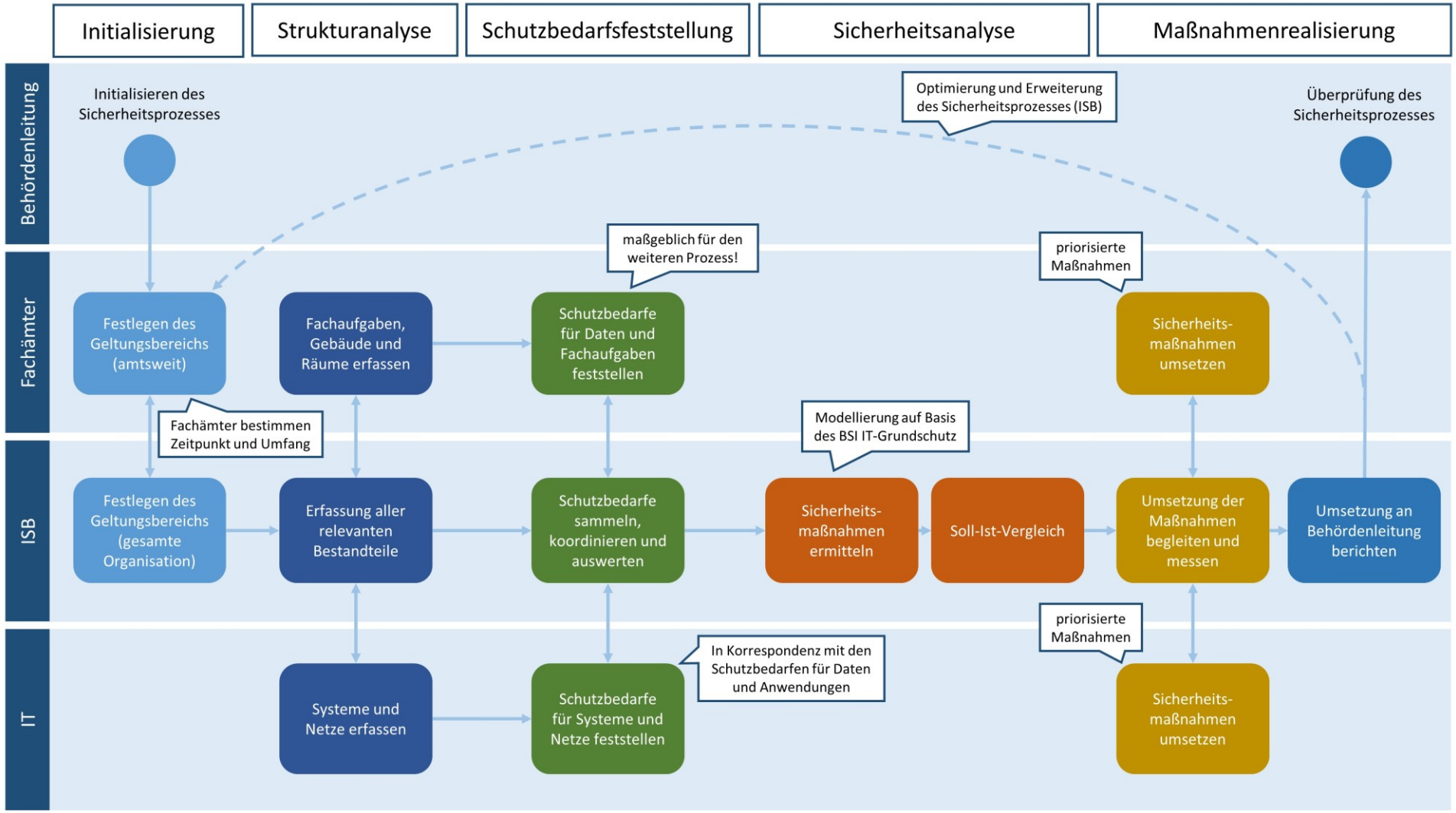

Abbildung 4: Ein Beispiel für die Phasen und Zuständigkeiten bei der Erstellung und Umsetzung eines IT-Sicherheitskonzepts

7.2.5. Beispiel zum IT-Grundschutzvorgehen

Durch eine optimale Zusammenstellung der technischen und organisatorischen Maßnahmen kann ein angemessenes Sicherheitsniveau erreicht und ausgebaut werden. Um Erfolg dabei zu haben, bedarf es der engen Zusammenarbeit aller Beteiligten.

Dies soll anhand des *Beispiels* des Landkreises Anhalt-Bitterfeld verdeutlicht werden.

Im Landkreis Anhalt-Bitterfeld wurde eine ISB benannt. Sie ist dem Fachbereich Strategische Entwicklung und Controlling zugeordnet. Dieser Fachbereich untersteht keinem Dezernat und ist direkt dem Bereich Landrat zugeordnet. Eine Arbeitsgruppe Informationssicherheit (ISMS-Team) unterstützt die ISB.

Für die ISLL wurden eine Mustervorlage des BSI sowie diese „Handreichung zur Ausgestaltung der Informationssicherheitsleitlinie in Kommunalverwaltungen“ mit Stand März 2017 zugrunde gelegt. Die Vorlage wurde von der ISB an die Bedürfnisse des Landkreises Anhalt-Bitterfeld angepasst und weiter in der Arbeitsgruppe Informationssicherheit sowie in Zusammenarbeit mit der Stabsstelle Organisation diskutiert und abschließend bearbeitet. Sie wurde als Leitlinie in Kraft gesetzt und veröffentlicht.

In den Grundsätzen wurden die Umsetzung des IT-Grundschutz-Profils Basis-Absicherung Kommunalverwaltung als erstes Ziel und somit die Vorgehensweise nach IT-Grundschutz des BSI festgelegt. Sicherheitsmaßnahmen waren im Hinblick auf die Wirksamkeit, Zuverlässigkeit und die wirtschaftliche Angemessenheit zu bewerten.

Als Sicherheitsziele sollen alle Beschäftigten der Landkreisverwaltung die Informationssicherheit durch ihr verantwortliches Handeln gewährleisten und den Bürgerinnen und Bürgern vermitteln, dass ihre Daten vor Dritten geschützt sind (Vertraulichkeit), dass die Daten korrekt sind (Integrität) und, dass sie Dienste in Anspruch nehmen können, wenn sie sie benötigen (Verfügbarkeit). Für alle Geschäftsprozesse sind diese Sicherheitsziele im jeweils erforderlichen Maße zu erreichen.

Die Schutzbedarfskategorien orientieren sich am Vorschlag im BSI-Standard 200-2 „IT-Grundschutz-Methodik“ und werden auf die Bedürfnisse der Landkreisverwaltung angepasst.

Weiterhin werden nachfolgende Sicherheitsziele in der ISLL definiert.

1) Schutz der Vertraulichkeit

Es muss sichergestellt sein, dass Informationen nur für befugte Personen zur Verfügung stehen.

2) Schutz der Integrität

Die Unversehrtheit und Korrektheit von Informationen müssen sichergestellt sein. Sie dürfen nicht ohne entsprechende Autorisierung verändert werden und jegliche Änderung an Informationen muss nachvollziehbar sein.

3) Schutz der Verfügbarkeit

Es muss sichergestellt sein, dass alle technischen und räumlichen Einrichtungen zur Informationsverarbeitung, -sicherung und -lagerung den Beschäftigten der Landkreisverwaltung Anhalt-Bitterfeld für die Aufgabenerfüllung zur Verfügung stehen und gegen organisationsbedingte, technische und umweltbedingte Ausfälle geschützt sind.

4) Schutz der Authentizität

Es muss sichergestellt sein, dass Informationen jederzeit ihrem Ursprung zugeordnet werden können.

5) Gewährleistung der Rechtmäßigkeit

Es muss sichergestellt sein, dass beim Umgang mit Informationen die geltenden Gesetze und Vorschriften sowie vertragliche und sonstige Verpflichtungen eingehalten werden. Vor allem bei der Verarbeitung personenbezogener Daten müssen die einschlägigen datenschutzrechtlichen Vorgaben, insbesondere die Verarbeitungsgrundsätze (wie beispielsweise Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Zweckbindung, Datenminimierung, Speicherbegrenzung und andere), berücksichtigt werden.

6) Aufrechterhaltung kritischer Geschäftsprozesse

Es muss sichergestellt sein, dass die zeitkritischen Geschäftsprozesse und IT-Fachverfahren der Landkreisverwaltung Anhalt-Bitterfeld auch in Krisen und Notfällen aufrechterhalten werden können und eingetretene Schäden minimiert werden.

7) Gewährleistung der Wirtschaftlichkeit

Es muss sichergestellt sein, dass die Kosten der Sicherheitsmaßnahmen in einem wirtschaftlich vertretbaren Verhältnis zum Wert der schützenswerten Informationen stehen.

Der Landrat trägt die Gesamtverantwortung für die Informationssicherheit in der Landkreisverwaltung.

Zur fachlichen Unterstützung und Koordinierung der Belange der Informationssicherheit wurden durch den Landrat eine ISB sowie eine Stellvertretung benannt.

Die ISB hat die Leitung der Arbeitsgruppe Informationssicherheit inne, welche sie bei ihrer Aufgabenwahrnehmung unterstützt. Die Arbeitsgruppe hat zudem die Aufgabe, das Zusammenwirken aller Organisationseinheiten mit Informationssicherheitsbezug in der Landkreisverwaltung zu koordinieren und erforderliche Maßnahmen abzustimmen und zur Entscheidung für den Landrat vorzubereiten.

Die Arbeitsgruppe setzt sich, der Informationssicherheitsleitlinie folgend, aus Vertreterinnen und Vertretern des Fachbereichs Informationstechnologie und Digitalisierung, dem behördlichen Datenschutzbeauftragten, einem Vertreter des Personalrats sowie bedarfsweise aus technischen Multiplikatoren und weiteren Teilnehmenden aus den Fachbereichen zusammen. In der Praxis hat sich das Team im Kern um weitere Teilnehmende aus den Bereichen Bau, Personal, zentrale Dienste und weitere vergrößert.

Besondere Verantwortung obliegt den verantwortlichen Beschäftigten für IT-Anwendungen, IT-Verfahren, IT-Systeme oder für spezifische Informationen. Sie sind für deren Informationssicherheit zuständig. Die zentrale Instanz für die operative und strategische IT-Sicherheit ist die Leitung des Fachbereichs Informationstechnik und Digitalisierung. Sie ist für den sicheren Betrieb der IT und die Umsetzung geeigneter Sicherheitsmechanismen verantwortlich.

Es wird sichergestellt, dass ausreichend finanzielle und personelle Ressourcen für die Umsetzung von Informationssicherheit bei IT-Anwendungen, IT-Verfahren, IT-Systemen vorhanden sind.

Jede Fachbereichsleitung bzw. Leitung einer Stabsstelle sorgt in ihrem Verantwortungsbereich für die Schaffung und Verbesserung eines angemessenen Sicherheitsniveaus, indem sie die Umsetzung von Sicherheitsmaßnahmen unterstützt.

Alle Beschäftigten der Landkreisverwaltung Anhalt-Bitterfeld tragen die Verantwortung, bestimmungsgemäß und sachgerecht mit den von ihnen genutzten Informationen und Systemen umzugehen und die hierfür geltenden Informationssicherheitsvorgaben einzuhalten.

Bei Unregelmäßigkeiten müssen die Beschäftigten unverzüglich den Fachbereich Informationstechnik und Digitalisierung, den/die ISB und ihre Vorgesetzten informieren.

Bedarfsweise und regelmäßige Schulungen und Sensibilisierungsmaßnahmen zur korrekten Nutzung der IT-Dienste und den hiermit verbundenen Sicherheitsmaßnahmen sollen allen Beschäftigten erteilt werden.

Die ISLL ist ein Rahmenwerk, das durch Dienstanweisungen und -vereinbarungen, Konzepte und Strategien wirksam ausgestaltet wird. Detaillierte Ziele, Anforderungen und Maßnahmen zur Ausgestaltung der ISLL werden in Sicherheitsrichtlinien, organisatorischen und technischen Konzepten sowie sonstigen Vorgabe- und Nachweisdokumenten beschrieben. Konkrete Vorgaben und Abläufe zu einzelnen Sicherheitsthemen werden in entsprechenden Anweisungen definiert. Diese Dokumente werden entsprechend ihrer inhaltlichen Zielsetzung und Detailtiefe in einer hierarchischen Struktur gegliedert und den betroffenen Beschäftigten der Landkreisverwaltung Anhalt-Bitterfeld und gegebenenfalls berechtigten Dritten (z. B. Dienstleistern) zur Verfügung gestellt.

7.3. PRÜFEN UND ÜBERWACHEN (CHECK)

Ein wichtiger Bestandteil eines funktionierenden ISMS ist die Erfolgskontrolle. Dabei erscheinen der Umsetzungsstand festgelegter Sicherheitsmaßnahmen, aber auch die Erfassung und Auswertung von Sicherheitsvorfällen als geeignete Hilfsmittel. Diese Aufgaben sollte der/dem ISB übertragen werden, alternativ einer für die Informationssicherheit verantwortlichen Person, die ein hohes Maß an Vertrauen bei den Beschäftigten genießt und gleichzeitig Unabhängigkeit in Bezug auf die Umsetzung der Informationssicherheit hat. Dadurch kann eine neutrale Auswertung des Erfolges erreicht werden.

Gegenüber der Behördenleitung sollten die Ergebnisse der Erfolgskontrollen regelmäßig in geeigneter Form mitgeteilt werden, um das Sicherheitsniveau durch geeignete Maßnahmen zu steuern und dadurch kontinuierlich zu verbessern. Der zuständigen Person sollte explizit gegenüber der Behördenleitung ein direktes Vortragsrecht eingeräumt werden.

Indikatoren für den Stand der Informationssicherheit sollten festgelegt und vom IS-Management-Team analysiert werden. Dazu zählen unter anderem die Ergebnisse von Sensibilisierungsmaßnahmen und internen Audits. Weiterhin sollten alle Sicherheitsvorfälle, Ausnahmeregelungen im Umgang mit Informationen und Fehlreaktionen von Beschäftigten ausgewertet werden, um Schwachstellen zu identifizieren und abzustellen.

7.3.1. Behandlung von Sicherheitsvorfällen

Sicherheitsvorfälle sind unter anderem das Auftreten von Computerviren, die Offenlegung von Informationen und der Ausfall existentieller IT-Dienste. Die mit einem Sicherheitsvorfall verbundenen Schäden können weitreichende Auswirkungen haben. Sie führen unter anderem zu einer Einschränkung der Aufgabenerfüllung, können hohe Kosten verursachen und sind in der Regel geschäftsschädigend.

Sicherheitsvorfälle lassen sich nicht immer sofort erkennen. Durch Fehlplanungen, mangelnde Steuerung und falsche Entscheidungen ergeben sich Risiken, die ein Sicherheitsproblem darstellen können. Schnell wird aus einem Sicherheitsvorfall ein größeres Sicherheitsproblem. Somit ist es wichtig, Sicherheitsvorfälle frühzeitig zu erkennen und umgehend zu behandeln.

Die Behördenleitung sollte eine Anlaufstelle zur Meldung von eingetretenen, aber auch vermuteten Sicherheitsvorfällen festlegen. Falls ein Service Desk (auch Help Desk genannt) existiert, kann dieser benannt werden. In kleineren Behörden können die Meldungen z. B. auch direkt an die/den ISB oder die IT-Leitung erfolgen. Die Beschäftigten sind darüber zu informieren und sollten motiviert werden, dass die Meldung von Sicherheitsproblemen und Sicherheitsvorfällen zur Lösungsstrategie zählt und sich daraus keinesfalls Schuldzuweisungen ergeben. So können Bedrohungen schneller erkannt und berücksichtigt werden.

Bei der Festlegung der Meldewege ist eine Eskalationsstrategie vorzusehen, wodurch beim Auftreten von schwerwiegenden Sicherheitsvorfällen bzw. für den Fall, dass für die Behörde kritische Sicherheitsprobleme eingetreten sind, die Behördenleitung und andere Stellen durch die zentrale Meldestelle einzubeziehen sind.

7.3.2. Berichtswesen zur Informationssicherheit

Die Leitungsebene sollte in regelmäßigen Abständen über die Probleme, die Erfolge und die Verbesserungsmöglichkeiten der Informationssicherheit schriftlich durch die/den ISB bzw. das IS-Management-Team informiert werden. Der Bericht sollte mindestens einmal jährlich erstellt und der Behördenleitung vorgelegt werden.

Neben dem Sicherheitsstatus zu kritischen Prozessen und Informationen sind weitere Punkte aufzunehmen. Dazu zählen unter anderem Ergebnisse interner und ggf. externer Audits, Folgemaßnahmen aufgrund vorheriger Sicherheitsbewertungen, Ergebnisse der Beratungen des IS-Management-Team, ein Überblick aller Sicherheitsvorfälle des Berichtszeitraumes, wesentliche organisatorische oder personelle Änderungen im Bereich der Informationssicherheit und ggf. zur allgemeinen Sicherheitslage.

Der Bericht dient insbesondere als Entscheidungsgrundlage für die Behördenleitung.

7.4. VERBESSERN (ACT)

Im Planungsprozess zum ISMS ist die Informationssicherheitsrevision zu berücksichtigen. Nur durch regelmäßige Überprüfung und Bewertung des etablierten Sicherheitsprozesses und der Sicherheitsmaßnahmen können Aussagen zur Konformität, Effizienz und Effektivität getroffen werden.

Die Revisionen und deren Ergebnisse sind durch die/den ISB bzw. durch das IS-Management-Team auszuwerten. Daraus ergeben sich Vorschläge zur Verbesserung der Informationssicherheit. Die im Kapitel 7.2.2 dargestellten übergreifenden Aspekte der Informationssicherheit bieten einen Ansatz für die Themenbereiche, wozu die Punkte Sicherheitsmanagement, Organisation und Personal zählen. Weitere Themenschwerpunkte für Vorschläge zur Verbesserung können unter anderem auch die Prozesse, Verfahren und die Technik berücksichtigen. Die Vorschläge sollten in das Berichtswesen integriert werden.

Zielsetzung ist die stetige Verbesserung des ISMS. Dies kann durch Korrekturen zur Vermeidung bestehender Ursachen, aber auch durch Verhindern weiterer Einflüsse geschehen. Die Behördenleitung übernimmt dabei die Steuerung des Prozesses und hat im Rahmen ihrer Managementverantwortung die Ergebnisse zu prüfen und die Vorschläge zu bestätigen.

8. FAZIT

100 % Sicherheit gibt es nicht! Bestimmten Risiken kann man nicht wirtschaftlich sinnvoll entgegentreten.

Die Leitungsebene hat die verbleibenden Risiken transparent zu erheben und zu dokumentieren, mit geeigneten Mitteln entgegenzusteuern (etwa durch Umstrukturierungen) oder diese unter bestimmten Umständen zu akzeptieren. Je nach Größe, Organisationsstruktur, Sicherheitsbedürfnis bzw. Reifegrad und finanziellen Möglichkeiten werden die Anforderungen an das ISMS dabei unterschiedlich ausfallen.

Größtmögliche Sicherheit ist nicht im Rahmen eines einmal zu durchlaufenden Projektes zu erreichen. Die stetige Verbesserung der Sicherheit stellt einen Regelkreis dar. Gemäß dem Pareto-Prinzip können 80 % der Ergebnisse in 20 % der Gesamtzeit eines Projektes erreicht werden, wobei für die Erreichung der verbleibenden 20 % der Ergebnisse 80 % der Zeit benötigt werden und dadurch die meiste Arbeit verursachen. Steigende Anforderungen an die Informationssicherheit sind mit einem höheren Bedarf an Ressourcen verbunden – dies ist bei der Planung des ISMS zu berücksichtigen.

Unabhängig von der Organisation der IT (Betrieb in Eigenregie oder durch IT-Dienstleister) kann keine pauschale Empfehlung zum ISMS und dem erreichbaren Sicherheitsniveau gegeben werden. Auch bei der Zusammenarbeit mit IT-Dienstleistern ist die Behörde nicht vom Informationssicherheits-Management entbunden. Die Verantwortung und die Kontrollpflichten verbleiben beim Auftraggeber. Die übergreifenden Aspekte der Informationssicherheit (z. B. Sicherheitsmanagement, Organisation, Personal usw.) und die Risiken für die Geschäftsprozesse sind auch durch einen IT-Dienstleister nicht oder nur teilweise zu beeinflussen. Nichtsdestotrotz reduziert die Übertragung von Aufgaben des IT-Betriebs an einen IT-Dienstleister die Komplexität des Informationsverbundes deutlich und erleichtert die Beherrschung der Informationssicherheit. Den Aufbau eines ISMS können IT-Dienstleister unterstützen, da die notwendigen Kompetenzen hier standardmäßig vorhanden sind und durch vertragliche Regelungen eingefordert werden sollten.

Vor dem Hintergrund der weiter zunehmenden Komplexität der kommunalen IT-Infrastrukturen, der prognostizierbaren weiteren Öffnung der Verwaltung nach außen (Open Data, Registermodernisierung, Digitalisierung etc.), der wachsenden Intransparenz vielgestaltiger Bedrohungen und schließlich der zunehmenden Aufmerksamkeit der Bürgerinnen und Bürger (und der Medien) sollten Verwaltungen, die ihre IT allein betreiben, intensiv prüfen, ob eine Zusammenarbeit mit einem professionellen kommunalen IT-Dienstleister zu einer Verbesserung der Informationssicherheit beiträgt.

Generell bedarf es des Bekenntnisses der Behördenleitung zur Informationssicherheit und eines klaren Regelwerkes unter Berücksichtigung der Verantwortlichkeiten. Alle Beschäftigten der Behörde sind in den Sicherheitsprozess einzubeziehen. Bestimmten Gefährdungen, wie z. B. dem Social Engineering[34], kann nur zusammen mit organisatorischen Maßnahmen wirksam entgegengewirkt werden.

Die Leitlinie für die Informationssicherheit des IT-Planungsrates fordert eine ebenenübergreifende Informationssicherheit für Bund, Länder und Kommunalverwaltungen. Dabei ist die interkommunale Zusammenarbeit zur Umsetzung einheitlicher Sicherheitsmaßnahmen nicht nur unter Berücksichtigung von Wirtschaftlichkeitsaspekten nötig. Die kommunalen Spitzenverbände sind die Interessenvertretungen in den Steuerungsgremien von Bund und Ländern. Mit dem IT-SiBe-Forum[35] bieten sie zudem eine Austauschplattform für ISBs und Praktiker:innen in den Kommunalverwaltungen.

[34] Unter diesem Begriff werden allgemein Angriffstechniken zusammengefasst, die sich auf die gezielte Manipulation von Menschen beziehen, um Zugang zu Computersystemen zu erlangen. Ein Beispiel bildet die Vortäuschung bestimmter Identitäten, um angriffsrelevante Informationen von Beschäftigten zu erhalten.

[35] Link zum IT-SiBe-Forum (Plattformbetreiber: Deutscher Landkreistag): https://it-sibe-forum.de

9. GLOSSAR UND ABKÜRZUNGEN

AG koBA	Arbeitsgruppe kommunale Basis-Absicherung
Bedrohung	Umstand, der zur Schädigung der Grundwerte (Vertraulichkeit, Integrität und Verfügbarkeit) führen kann.
Best Practice	Gängige Praxis
BSI	Bundesamt für Sicherheit in der Informationstechnik
BSI-Standard	Reihe der Veröffentlichungen zur Einführung eines ISMS, zum IT-Grundschutzvorgehen, zur Risikoanalyse auf Basis von IT-Grundschutz und zum Notfallmanagement
CERT	Computer Emergency Response Team (Computer-Notfall-Team)
E-Government-Services	Dienstleistungen der öffentlichen Verwaltung durch Einsatz moderner Informations- und Kommunikationstechniken
EU-Zahlstellen	Öffentliche Stelle zur Bewilligung, Kontrolle und Zahlungen von EU-Fördergeldern
Gefährdung	Stellt eine Bedrohung dar, falls Schwachstellen existierten und ausgenutzt werden.
Geschäftsprozess	Abfolge von Arbeitsschritten eines Verwaltungsvorganges
IKS	Internes Kontrollsystem, auch Revision
ISB	Informationssicherheitsbeauftragte/r
ISLL	Informationssicherheitsleitlinie
ISMS	Informationssicherheits-Managementsystem
ISO	International Standards Organisation
IS-Organisation	Bezeichnung der aktiv am ISMS beteiligten Personen und des Informationssicherheitsbeauftragten
IT	Informationstechnik
IT-Grundschutz	Empfehlungen des BSI für ein Standard-Sicherheitsniveau mit ganzheitlichem Ansatz bezüglich organisatorischen, personellen, infrastrukturellen und technischen Sicherheitsmaßnahmen
IT-Sicherheitsbeauftragte/r	Bezeichnung für Verantwortliche der IT-Sicherheit oder Informationssicherheit. Kann synonym für Informationssicherheitsbeauftragte verwendet werden, aber auch eine Zusatzfunktion mit speziellem Fokus auf IT-Sicherheit sein.
NWR	Nationales Waffenregister, zentrale Komponente zur Verwaltung von Schusswaffen, an die alle Waffenbehörden angeschlossen sind
Open Data	Bereitstellung allgemein zugänglicher Daten und Informationen zur Weiternutzung
Outsourcing	Auslagerung von Geschäftsprozessen an externe Dienstleister
Pareto-Prinzip	Nach Vilfredo Pareto (1848–1923) benanntes Prinzip, dass 80 % der Ergebnisse in 20 % der Gesamtzeit erreicht werden können.
PDCA-Zyklus	Auch als Deming-Rad bezeichnet, ist ein nach William Edwards Deming (1900–1993) benannter iterativer vierphasiger Problemlösungsprozess mit Ursprüngen in der Qualitätssicherung
Risikoanalyse	Mittel zur Feststellung und Bewertung von Gefährdungen und Bedrohungen im Risikomanagement

Risikomanagement	Prozess zur Behandlung von Risiken, wobei Maßnahmen festgelegt werden, um verbleibende Risiken zu vermeiden, zu reduzieren, auf Dritte abzuwälzen oder ggf. die damit verbundenen Konsequenzen zu tragen
Roadmap	Synonym für eine zeitliche Darstellung eines geplanten Ablaufes
Schadprogramme	Computerprogramme mit unerwünschten und meist schädigenden Funktionen
Sicherheitskonzept	Dokument zur Umsetzung der Sicherheitsstrategie und zur Erreichung der Sicherheitsziele
Sicherheitsstrategie	Abstrakte Festlegung, mit welchen Mitteln die Organisation die Sicherheitsziele erreichen will
Sicherheitsziele	Festlegungen zum angestrebten Sicherheitsniveau
Social Engineering	Ausnutzen persönlicher Umstände oder des persönlichen Umfeldes einer Person zur Erlangung vertraulicher Informationen
Verbindungsnetz	Informationstechnisches Netz, welches die Netze des Bundes und der Länder verbindet (§ 2 IT-NetzG)

10. VERZEICHNIS DER ABBILDUNGEN UND TABELLEN