Fraunhofer AISEC

# Gutachten zur Anwendbarkeit von ISIS12 in der öffentlichen Verwaltung

(Stand: November 2014)

Ansprechpartner

- Iryna Windhorst
  E-Mail: iryna.windhorst@aisec.fraunhofer.de
  Telefon: 089- 322 9986-157

# Management Summary

In der vom IT-Planungsrat verabschiedeten „Leitlinie für die Informationssicherheit in der öffentlichen Verwaltung“ werden die Mindestanforderungen für IT-Sicherheit für Bund und Länder festgelegt. Einer der wichtigsten Ziele dieser Leitlinie ist der Aufbau und die Etablierung des Informationssicherheitsmanagements in den öffentlichen Verwaltungen. Laut der Leitlinie ist ein ISMS auf Basis IT-Grundschutz des BSI oder ISO 27001 in den Behörden bis 2018 einzuführen.

Da sich viele IT-Verfahren der öffentlichen Verwaltung in miteinander vielfältig vernetzten Systemen auf allen drei Ebenen (Bund – Land – Kommune) vollziehen, ist die Absicherung der ganzen Prozesskette unerlässlich geworden. Bekannterweise ist „eine Kette nur so stark wie ihr schwächstes Glied“. Aus diesem Grund sollte die Leitlinie des IT-Planungsrats auch in den Kommunen umgesetzt werden. Der IT-Grundschutz mit seinen unzähligen Katalogen (über 4400 Seiten) und ISO/IEC 27001 Standard mit seinem sehr abstrakten Charakter stellen die Anwender jedoch vor eine große Herausforderung. Die Einführung eines ISMS ist gleichzeitig unerlässlich in Anbetracht der stetig wachsenden Bedrohungen und Gefährdungen geworden. So wurde ein neuer pragmatischer Ansatz zur Einführung von ISMS in 12 Schritten (ISIS12) vom Netzwerk des Bayerischen IT-Sicherheitscluster e.V. entwickelt. Dieses Vorgehen, nach dem Leitsatz „So einfach wie möglich, aber nicht einfacher“ konzipiert, bietet einen konkreten Handlungsrahmen zur Etablierung eines einfach einzuführenden ISMS in 12 sequentiell zu durchlaufenden Schritten. ISIS12 betrachtet nur wenige unternehmenskritische Anwendungen, wendet auf die damit verbundenen IT-Systeme einen gegenüber dem BSI IT-Grundschutz reduzierten Maßnahmenkatalog an und integriert die grundlegenden IT-Service-Management-Prozesse (Wartung, Änderung und Störungsbeseitigung). Des Weiteren ist dieses Vorgehen generisch aufgebaut und dementsprechend flexibel.

ISIS12 erfüllt im Groben die Mindestanforderungen des IT-Planungsrats an ein ISMS. Laut der durchgeführten Prüfung stellt ISIS12 eine geeignete Vorgehensweise für eine definierte „Standardbehörde“ mit ca. 500 Mitarbeitern, möglichst homogener IT-Basisinfrastruktur, keinen über öffentliche Netze ungeschützt angebundenen Außenstellen, überwiegend normalem Schutzbedarf, keinen Hochverfügbarkeitsanforderungen an IT-Systeme und keinen kritischen Anwendungen (im Sinne keine kritischen Infrastrukturen) dar. Da ISIS12 speziell mit der Möglichkeit der Skalierbarkeit entwickelt wurde, könnte das nach ISIS12 implementierte und etablierte ISMS nach dem Durchlauf weiterer erforderlichen Schritte und entsprechender Dokumentation ausgebaut werden und eine weiterführende Zertifizierung wie „ISO 27001 auf Basis von IT-Grundschutz“ bzw. „ISO/IEC 27001 nativ“ erreicht werden. Im Fall einer späteren Einführung der erwähnten Standards sind durch ISIS12 bereits essentielle Schritte eingeführt worden. Zum Beispiel wurden bereits Leitlinien für Informationssicherheit und IT-Dokumentation erstellt sowie kritische Systeme identifiziert und die entsprechenden Sicherheitsmaßnahmen eingeführt. Da in ISIS12 nur eine indirekte Risikoanalyse durchgeführt wird, muss diese im Rahmen von ISO/IEC 27001 vorangestellt bzw. bei der IT-Grundschutz-Vorgehensweise nachgelagert erfolgen und dokumentiert werden. Da für die ISIS12 Zertifizierung nur sieben Referenzdokumente vorgesehen sind, müssen für die weiterführenden Zertifizierungen noch einige mehr erstellt werden. Es werden jedoch die wichtigen Schritte im Rahmen des ISIS12 eingeführt und die spätere Einführung von ISO 27001 oder IT-Grundschutz wird dadurch erleichtert.

Behörden und Verwaltungen nach obiger Definition profitierten von einer Einführung eines ISMS nach ISIS12 insbesondere von der hohen Skalierbarkeit, dem generischen Aufbau, der Einführung von grundlegenden IT-Service-Management-Prozessen sowie den konkreten Handlungsempfehlungen und der stringenten Struktur mit Kontrollfragen. Die Implementierung eines ISMS nach ISIS12 deckt die grundlegenden Gefährdungen für die Informationssicherheit in der öffentlichen Verwaltung ab. Mit ISIS12 ließe sich ein Managementsystem für die Informationssicherheit einführen, das eine kontinuierliche Weiterentwicklung ermöglicht und einen nachweislich dokumentierten Sicherheitsprozess unterstützt.

# Inhalt

# Abbildungsverzeichnis

# Abkürzungsverzeichnis

| | |
|---|---|
| A | Annex im ISO/IEC 27001 |
| B | Baustein im ISIS12-Katalog bzw. IT-Grundschutzkatalog |
| BCM | Business Continuity Management (Betriebskontinuitätsmanagement) |
| BITKOM | Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. |
| BSI | Bundesamt für Sicherheit in der Informationstechnik |
| DIN | Deutsches Institut für Normung e.V. |
| DQS | Deutsche Gesellschaft zur Zertifizierung von Managementsystemen |
| IEC | International Electrotechnical Commission (Internationale Elektrotechnische Kommission) |
| ISB | Informationssicherheitsbeauftragte |
| ISIS12 | Informationssicherheitsmanagementsystem in 12 Schritten |
| ISM | Informationssicherheitsmanagement |
| ISMS | Informationssicherheitsmanagementsystem |
| ISO | International Organization for Standardization (Internationale Organisation für Normung) |
| IT | Informationstechnik |
| ITGS | IT-Grundschutz |
| ITIL | Information Technology Infrastructure Library |
| ITSM | IT-Service-Management |
| KMU | Kleine und mittlere Unternehmen |
| M | Maßnahme im ISIS12-Katalog bzw. IT-Grundschutzkatalog |
| MTA | Maximal tolerierbare Ausfallzeit |
| NATO | North Atlantic Treaty Organization (Nordatlantikpakt-Organisation) |
| QM | Qualitätsmanagement |
| PDA | Personal Digital Assistant (persönlicher digitaler Assistent) |
| PDCA | Plan-Do-Check-Act |

| | |
|---|---|
| PT | Personentage |
| R | ISIS12 Referenzdokument |
| S | Schicht im ISIS12-Katalog bzw. IT-Grundschutzkatalog |
| SLA | Service Level Agreement |

# 1 Einleitung

Die öffentliche Verwaltung befindet sich in einem umfassenden Veränderungsprozess, der das Arbeitsumfeld zunehmend digitalisiert. So gehört die elektronische Kommunikation auch in der Verwaltung seit Langem zum Standard. Viele Verwaltungsabläufe werden mittlerweile elektronisch unterstützt. Dieser Wandel macht auch vor Herausforderungen des Datenschutzes, der Wirtschaftsspionage, Ausfällen kritischer Infrastrukturen, Kompromittieren von IT-Systemen, der Notwendigkeit hoher IT-Verfügbarkeit und Integrität der Kommunikation nicht halt. Vor allem die Kommunen stehen vor großen Herausforderungen, wenn es um die Sicherung von zum Teil hochsensiblen Daten von Bürgern, Mitarbeitern und Unternehmen und deren Kommunikation geht. Auch die in der Regel kleinen IT-Abteilungen von Kommunen müssen daher in die Lage versetzt werden, die Informationssicherheit über das Mindestsicherheitsniveau hinaus effektiv und effizient zu garantieren.

In letzter Zeit wurde eine Reihe von Gesetzen, Vorschriften und Beschlüssen zur Erhöhung der Informationssicherheit verabschiedet u.a. Gesetz zur Stärkung der Sicherheit in der Informationstechnik des Bundes, Entwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz), Leitlinie für die Informationssicherheit in der öffentlichen Verwaltung, EU-Richtlinie zur Netz- und Informationssicherheit, Allianz für Cyber-Sicherheit, CERT-Verbund etc. Diese vielfältigen Gesetzesvorgaben und Initiativen machen deutlich, dass IT-Sicherheit seitens Politik und Staat immer wichtiger wahrgenommen wird. Dennoch hapert es an der Umsetzung dieser Vorgaben. So berichtete der IT-Sicherheitsexperte Tobias Morsches vor dem Landtag Nordrhein-Westfalen im Februar 2014, dass die allgemeine Sicherheitslage in der öffentlichen Verwaltung kritisch sei. Es gelang ihm und seinem Team in allen von ihnen untersuchten Kommunen vollständigen Zugriff auf alle relevanten Systeme, u.a. komplette Personenregister, detaillierte Informationen über ansässige Ausländer, gesonderte Listen mit Alias-Identitäten (z.B. gefährdete Personen), Daten der Finanzverwaltung, Alarmierungs- und Leitsysteme der Feuerwehr usw. zu erhalten [1]. Der Grund dafür ist das Fehlen essentieller Sicherheitsmaßnahmen.

Da Informationen das wertvollste Gut jeder Organisation sind, müssen diese entsprechend abgesichert werden - am besten ganzheitlich in einem sogenannten Informationssicherheitsmanagementsystem (ISMS). Die Notwendigkeit der Implementierung eines Informationssicherheitsmanagements ist erkannt und wird konsequenterweise auch in übergeordneten Sicherheitsstrategien des Bundes, u.a. in der Leitlinie des IT-Planungsrats gefordert. Dies soll auch in den Kommunen geschehen, weil „eine Kette nur so stark ist wie ihr schwächstes Glied“.

Die bestehenden Verfahren zur Einführung eines ISMS, wie BSI IT-Grundschutz oder ISO/IEC 27001, werden jedoch oft als zu komplex und zu teuer wahrgenommen. Auf Initiative des Bayerischen IT-Sicherheitscluster wurde daher im Jahr 2011 die Alternative ISIS12, ein Informationssicherheitsmanagementsystem in 12 Schritten, spezifiziert mit dem Ziel, den Einführungsprozess zu beschleunigen und anhand pragmatischer Richtlinien zu vereinfachen [2].

Das vorliegende Gutachten untersucht, ob ISIS12 zur Einführung des ISMS in den öffentlichen Verwaltungen geeignet ist und inwiefern diese alternative Vorgehensweise den Vorgaben des IT-Planungsrats [3] genügt. Darüber hinaus wird bewertet, ob ISIS12 als eine Vorstufe für eine eventuell später noch vorzunehmende Zertifizierung nach IT-Grundschutz bzw. ISO/IEC 27001 dienen kann.

# 2 Definition, Abgrenzung und Untersuchungsgegenstand

## 2.1 Definition und Abgrenzung grundlegender Begriffe

Da unterschiedliche Definitionen existieren, ist es wichtig, im ersten Schritt diese zu definieren, um somit eine grundlegende Basis für ein einheitliches Verständnis zu schaffen.

*Öffentliche Verwaltung* ist der Oberbegriff für Verwaltungen, die Aufgaben des Staates einschließlich Einrichtungen des öffentlichen Rechtes wahrnehmen. Träger der öffentlichen Verwaltung sind der Bund, die Länder und die Kommunen.

Unter *staatlicher bzw. öffentlicher IT* werden sowohl die öffentlichen als auch die nicht-öffentlichen Bestandteile von Informationstechnologien verstanden, die in der Verantwortung der öffentlichen Hand betrieben werden. Dies umfasst IT auf allen staatlichen und überstaatlichen Ebenen, d.h. auf internationaler, europäischer, Bundes-, Landes- und kommunaler Ebene sowie im Rahmen von Bündnissen, wie z.B. der NATO [4].

Unter *Informationssicherheitsmanagement (ISM)* wird die Planungs-, Lenkungs- und Kontrollaufgabe verstanden, die erforderlich ist, um einen durchdachten und wirksamen Prozess zur Herstellung von Informationssicherheit aufzubauen und kontinuierlich umzusetzen. Dabei handelt es sich um einen kontinuierlichen Prozess, dessen Strategien und Konzepte ständig auf ihre Leistungsfähigkeit und Wirksamkeit zu überprüfen und bei Bedarf fortzuschreiben sind [5].

In Anlehnung an den ISO/IEC Standard 27001 [6] sowie den BSI-Standard 100-1 [7] und erweitert um Aspekte nach Müller [8] lässt sich ein *Informationssicherheitsmanagementsystem (ISMS)* als Summe der Prozesse, Verantwortlichkeiten, Verfahren, Methodiken sowie der Ressourcen, Hilfsmittel und einer geeigneten Aufbauorganisation charakterisieren, um der Leitungsebene zu ermöglichen, alle auf Informationssicherheit ausgerichteten Aktivitäten und Aufgaben nachvollziehbar zu lenken und zu dokumentieren. Das beschriebene Konzept eines ISMS ist grundsätzlich unabhängig von konkreten Standards und der Implementierung dieser Standards.

Unter einem *Standard* wird eine einheitliche und anerkannte Art und Weise etwas herzustellen oder durchzuführen verstanden. Grundlage für einen Standard ist häufig eine technische Spezifikation, deren Inhalt in Form eines Dokumentes festgehalten ist. Eine technische Spezifikation wird dann als Standard bezeichnet, wenn sie in Expertenkreisen hinreichend anerkannt ist und/oder in der Praxis hinreichend akzeptiert und genutzt wird. Im Zusammenhang mit öffentlicher IT sind vor allem Standards der Informations- und Kommunikationstechnologie (IT-Standards) relevant [4].

Die Standards ISO/IEC 27001 und ISO/IEC 27002 gehören zur ISO/IEC 27000-Reihe – einer Sammlung von Normen im Anwendungsbereich der IT-Sicherheit.

*ISO/IEC 27000 – Information security management systems – Overview and vocabulary*: Der Standard erklärt den Zweck eines ISMS, einem System zur Verwaltung von Risiken und Steuerungsvorgaben für die Informationssicherheit einer Organisation. Informationssicherheit zur bewussten Aufgabe des Managements zu machen, ist ein zentrales Prinzip des ISO/IEC 27000-Standards.

*ISO/IEC 27001 – Information security management systems – Requirements* [9] - legt allgemeine Anforderungen (Aufstellen, Umsetzen, Betrieb, Überwachung, Bewertung, Wartung und Verbesserung) an ein ISMS in Bezug auf die allgemeinen Geschäftsrisiken einer Organisation fest. Er legt außerdem die Anforderungen an die Einführung von auf die Bedürfnisse

einer Organisation oder Teilen davon zugeschnittenen Sicherheitskontrollen fest. Das ISMS ist dafür entwickelt worden, die Auswahl ausreichender und angemessener Sicherheitskontrollen zu gewährleisten, die den Informationsbestand sichern und interessierten Partnern Vertrauenswürdigkeit vermitteln. Die konkrete Umsetzung wird bewusst offen gelassen. Daneben verfügt die Norm über mehrere Anhänge. Im normativen Anhang A werden in 14 Themengebieten insgesamt 114 Maßnahmen (Controls) zur Verfügung gestellt, die analog zu ISO/IEC 27002 strukturiert sind [9].

*ISO/IEC 27002 – Code of practice for information security management* [10] - stellt Best-Practice Empfehlungen für die Einführung, Implementierung und Wartung eines ISMS zur Verfügung aus ISO/IEC 27001 Anhang A. Die Anforderungen an das ISMS sind im sogenannten Management-Rahmen (Kap. 4 bis 10) der ISO/IEC 27001 formuliert.

Einen weiteren Ansatz für ein Managementsystem für Informationssicherheit bietet das Bundesamt für Sicherheit in der Informationstechnik (BSI) mit dem "IT-Grundschutz". *BSI IT-Grundschutz* bezeichnet eine Methodik zum Aufbau eines Sicherheitsmanagementsystems sowie zur Absicherung von Informationsverbünden über Standard-Sicherheitsmaßnahmen. Außerdem wird mit IT-Grundschutz der Zustand bezeichnet, in dem die vom BSI empfohlenen Standard-Sicherheitsmaßnahmen umgesetzt sind, die als Gesamtheit von infrastrukturellen, organisatorischen, personellen und technischen Sicherheitsmaßnahmen, Institutionen mit normalem Schutzbedarf hinreichend absichern [5].

Dieser Ansatz ist laut BSI vollständig kompatibel zu ISO/IEC 27001 und berücksichtigt auch die Empfehlungen der ISO/IEC 27002. Die Methodik des IT-Grundschutzes ist in vier IT-Grundschutz-Standards festgelegt. Der BSI-Standard 100-1 beschreibt Managementsysteme für Informationssicherheit [7]. Wie auch bei der ISO/IEC 27001 ist das Informationssicherheitsmanagement ein Prozess und Teil des unternehmensweiten Risikomanagements. Die praktische Umsetzung des IT-Grundschutzes wird in BSI-Standard 100-2 dargestellt [11]. Dieser Teil des Standards bildet den Kern der Vorgehensweise nach IT-Grundschutz. Eine Risikoanalyse auf der Basis von IT-Grundschutz ist in BSI-Standard 100-3 beschrieben [12]. Der BSI-Standard 100-4 zum Notfallmanagement bietet darüber hinaus einen Ansatz für den systematischen Aufbau eines organisationsweiten Business Continuity Management (Betriebskontinuitätsmanagement (BCM)) [13].

*ISIS12* (Informationssicherheitsmanagementsystem in 12 Schritten) ist ein speziell für mittelständische Unternehmen entwickeltes Verfahren zur Etablierung eines einfach einzuführenden Informationssicherheitsmanagementsystems (ISMS) in 12 sequentiell zu durchlaufenden Schritten. Mit ISIS12 wird dem Anwender ein konkreter Handlungsrahmen im Gegensatz zum abstrakten Charakter der ISO/IEC 27001 vorgegeben. Im ISIS12 Vorgehen wird das ISMS mit dem IT-Service-Management verknüpft [14].

*IT-Service-Management* (ITSM) bezeichnet die Gesamtheit der Maßnahmen, die nötig sind, um die bestmögliche Unterstützung von Geschäftsprozessen durch die IT-Organisation zu erreichen. ITSM beschreibt den Wandel der Informationstechnik in Richtung Kunden- und Serviceorientierung. Von Bedeutung ist die Gewährleistung und Überwachung von IT-Services. Auf diese Weise kann kontinuierlich die Effizienz, die Qualität und die Wirtschaftlichkeit der jeweiligen IT-Organisation verbessert werden.

## 2.2 Inhalt und Ziel des Projektes

In der vom IT-Planungsrat verabschiedeten „Leitlinie für die Informationssicherheit in der öffentlichen Verwaltung“ [3] werden die Mindestanforderungen für IT-Sicherheit für Bund und Länder festgelegt. Einer der wichtigsten Ziele dieser Leitlinie ist der Aufbau und die Etablierung des Informationssicherheitsmanagements in den öffentlichen Verwaltungen, weil „Sicherheit kein unveränderbarer Zustand ist, sondern aktiv gemanagt werden muss, um ein einmal erreichtes Sicherheitsniveau aufrechtzuerhalten“ [3].

Laut der Leitlinie ist **ein ISMS auf Basis IT-Grundschutz des BSI oder ISO/IEC 27001** in den öffentlichen Verwaltungen bis 2018 einzuführen. Des Weiteren schreibt der IT-Planungsrat die Mindestanforderungen an das ISMS vor und zwar:

- Festlegung und Dokumentation von Verantwortlichkeiten hinsichtlich des Informationssicherheitsmanagements (z.B. Benennung des IT-Sicherheitsbeauftragten)
- Erstellung von jeweiligen verbindlichen Leitlinien für die Informationssicherheit
- Erstellung und Umsetzung von Sicherheitskonzepten für Behörden und Einrichtungen
- Festlegung und Dokumentation der Abläufe bei IT-Sicherheitsvorfällen
- Etablierung von Prozessen, mit denen Umsetzung, Wirksamkeit und Beachtung der Informationssicherheitsmaßnahmen regelmäßig kontrolliert und die Einleitung ggf. erforderlicher Maßnahmen (z. B. Fortschreibung der Sicherheitskonzepte) gewährleistet wird
- Information, Weiterbildung, Sensibilisierung aller Beschäftigten der öffentlichen Verwaltung zu Themen der Informationssicherheit. Hierzu gehört auch die Etablierung und Durchführung regelmäßiger Sensibilisierungsmaßnahmen für die oberste Leitungsebene
- Anforderungsgerechte und einheitliche Fortbildung der IT-Sicherheitsbeauftragten. Eine Zertifizierung der IT-Sicherheitsbeauftragten wird angestrebt
- Jahrestagungen der IT-Sicherheitsbeauftragten zum gegenseitigen Erfahrungsaustausch (Verantwortung für Organisation wechselt mit Vorsitz im IT-Planungsrat).

Da der IT-Grundschutz die Anwender mit seinen unzähligen Katalogen (über 4400 Seiten) vor eine große Herausforderung stellt und gleichzeitig unerlässlich in Anbetracht der stetig wachsenden Bedrohungen und Gefährdungen ist, wurde ein neuer pragmatischer Ansatz zur Einführung von ISMS in 12 Schritten (ISIS12) vom Netzwerk des Bayerischen IT-Sicherheitscluster e.V. entwickelt. Dieses Vorgehen wurde für die Zielgruppe der kleinen und mittelständischen Unternehmen (KMUs) nach dem Leitsatz „So einfach wie möglich, aber nicht einfacher“ konzipiert.

Im Rahmen des Projektes soll eine unabhängige Einschätzung erfolgen, inwieweit ISIS12 für öffentliche Verwaltungen geeignet ist, um die Vorgaben des IT-Planungsrats zu erfüllen. Darüber hinaus soll bewertet werden, ob ISIS12 als eine Vorstufe für eine eventuell später noch vorzunehmende Zertifizierung nach IT-Grundschutz bzw. ISO/IEC 27001 dienen kann.

Das Gutachten ist eine Momentaufnahme und gilt zum Zeitpunkt der Erstellung des Dokumentes als abschließend.

## 2.3 Vorgehen

Die für die Begutachtung benötigten Informationen wurden durch den Auftraggeber in Form von ISIS12-Dokumentation (Handbuch in Version 1.7 von August 2014 und Katalog in Version 1.3 von August 2014) bereitgestellt. Fragen, die sich darüber hinaus ergaben und mit Hilfe der Dokumentation nicht beantwortet werden konnten, wurden in Form von Workshops, E-Mail Kommunikation und in Telefonkonferenzen entweder vom Auftraggeber direkt oder vom Bayerischen IT-Sicherheitscluster e.V. als Entwickler des ISIS12 Vorgehens beantwortet.

Die Ergebnisse des Gutachtens basieren auf Informationen des Auftraggebers und des Bayerischen IT-Sicherheitscluster e.V. sowie auf Analyse und Abgleich der BSI-Vorgehensweise und der IT-Grundschutz-Kataloge mit dem Vorgehen [14] und Katalog [15] des ISIS12. Dabei werden die Rahmenbedingungen und Anforderungen öffentlicher Verwaltungen sowie ihre wichtigsten Unterschiede zu den KMUs berücksichtigt.

Im ersten Schritt wird die ISIS12 Vorgehensweise auf ihre Konsistenz und Vergleichbarkeit mit der Vorgehensweise des IT-Grundschutzes überprüft.

Im zweiten Schritt werden die Kataloge analysiert, um zu identifizieren, welche Grundschutz-Bausteine im ISIS12-Katalog gekürzt wurden, weil sie z.B. für KMUs keine Relevanz haben, aber für die öffentliche Verwaltung von Bedeutung sind. Es wird nicht jede einzelne Maßnahme geprüft, ob sie im Katalog vorhanden ist oder nicht, sondern es wird viel mehr auf der Ebene der Bausteine geschaut, welche von ihnen ggf. fehlen.

Im dritten Schritt wird untersucht, welche zusätzlichen Arbeitsschritte und Dokumente notwendig sind, um eine weiterführende Zertifizierung wie „ISO 27001 auf Basis von IT-Grundschutz“ bzw. „ISO/IEC 27001 nativ“ zu erreichen. Zum Schluss werden die drei Vorgehensmodelle – ISO/IEC 27001, IT-Grundschutz und ISIS12 – in einer Tabelle hinsichtlich relevanter Kriterien gegenübergestellt.

Das vorliegende Gutachten gliedert sich wie folgt: Kapitel 3 stellt das ISIS12 vor. Anschließend werden im Kapitel 4 die Mindestanforderungen und Rahmenbedingungen öffentlicher Verwaltungen betrachtet. Kapitel 5 stellt das Kernstück des Gutachtens dar, in dem die Analyseergebnisse vorgestellt werden. Kapitel 6 schließt das Gutachten mit einer Zusammenfassung ab.

# 3 Beschreibung des ISIS12

Die Einführung eines Informationssicherheitsmanagementsystems (ISMS) nach ISO/IEC 27001 oder dem BSI IT-Grundschutz stellt aus diversen Gründen oft große Hürden für öffentliche Verwaltungen und KMUs dar, vor allem, wenn diese nicht in der IT-Branche tätig sind [16]. Dazu gehören beispielsweise nicht ausreichend qualifiziertes Personal, genereller Personalmangel in der IT, nicht gut verständliche Vorgehensweise sowie Zeit- und Kostenaufwand. Das **Netzwerk des Bayerischen IT-Sicherheitscluster e.V.** ("Netzwerk für Informationssicherheit im Mittelstand (NIM)") entwickelte daher - aus IT-Grundschutz und ISO/IEC 27001 abgeleitet - ein Verfahren zur Einführung eines ISMS in 12 Schritten. Dabei stehen die folgenden drei schützenswerten Grundwerte im Fokus:

- Vertraulichkeit (Wirtschaftsspionage, Patente, Gesetze)
- Integrität (Korrektheit der Daten, Produktqualität)
- Verfügbarkeit (Verträge mit Kunden, Notfallvorsorge) [14]

Bei der Entwicklung des ISIS12 Verfahrens wurde wesentliches Augenmerk darauf gelegt, den Organisationen eine klare Handlungsanweisung in begrenztem Umfang und mit integriertem Einführungskonzept an die Hand zu geben. Dadurch soll ein ISMS nach ISIS12 Modell in einer Einrichtung mit vergleichsweise geringerem Aufwand eingeführt werden können.

Zu diesem Zweck wurden ein Handbuch zur effizienten Gestaltung von Informationssicherheit im Mittelstand [14] sowie ein Katalog mit den konkreten Sicherheitsmaßnahmen [15] entwickelt. Das Handbuch beschreibt den Einführungsprozess des ISMS in 12 sequentiell zu durchlaufenden Schritten. Der Katalog ist eine für die ISIS12 Zielgruppe (mittelständische Unternehmen) ausgewählte Untermenge der IT-Grundschutz-Kataloge mit dazugehörigen Maßnahmen. Bei der Auswahl der Sicherheitsmaßnahmen spielten Breitenwirkung, Umsetzbarkeit und eine systematische Abdeckung von Gefährdungen eine wichtige Rolle. ISIS12 betrachtet eine gezielte Auswahl unternehmenskritischer Anwendungen und wendet auf die damit verbundenen IT-Systeme einen gegenüber dem BSI IT-Grundschutz radikal reduzierten Maßnahmenkatalog an. Grundsätzlich hängt der Aufwand für die Einführung von ISIS12 sehr stark von der jeweiligen Organisation und von den verarbeiteten Informationen ab. Der konkrete Aufwand kann daher erst nach einer entsprechenden Analyse durch einen ISIS12-Berater ermittelt werden.

Der Einführungsprozess sowie die nachfolgenden Revisionsaufgaben im Rahmen der PDCA-Zyklen werden durch ein an der Universität Regensburg an die ISIS12 Vorgehensweise angepasstes Open-Source-Softwaretool unterstützt. Durch den Einsatz dieses speziellen ISIS12-Tools wird dem Anwender das Arbeiten mit dem Vorgehensmodell wesentlich erleichtert. Das Tool bildet den ISIS12 Workflow komplett ab, liefert Hinweise für die einzelnen Arbeitsschritte und dokumentiert diese zugleich. Des Weiteren wurde die GRC Suite von ibi systems um die ISIS12-Kataloge ergänzt und kann ebenfalls eingesetzt werden. Laut der Angaben ist ISIS12 am besten für Organisationen ab 150 rechnergestützte Arbeitsplätzen geeignet [16].

Da die IT-Service-Management-Prozesse (ITSM) sehr wichtig für die Organisationen sind, wurde in ISIS12 ein grundlegendes ITSM integriert, welches auf die wesentlichen Prozesse - Wartung, Änderung und Störungsbeseitigung - konsolidiert wurde. Diese Integration stellt ein Schlüsselelement von ISIS12 dar. Des Weiteren ist dieses Vorgehen generisch aufgebaut und dementsprechend flexibel. So kann ISIS12 mit anderen Managementsystemen integriert werden, wie z.B. Qualitätsmanagement (ISO 9000) oder Umweltmanagement (ISO 14000).

Die Einführung von ISIS12 in einer Organisation erfolgt in der Regel mit Unterstützung eines geschulten ISIS12-Beraters. Bei der Implementierung erhält der Kunde das ISIS12-Handbuch, den ISIS12-Katalog, der nur die relevanten

Sicherheitsmaßnahmen enthält, sowie das ISIS12-Software-Tool [17]. Im Anschluss an die erfolgreiche Einführung kann optional im Rahmen eines Audits eine Zertifizierung bei der DQS (Deutsche Gesellschaft zur Zertifizierung von Managementsystemen) durchlaufen werden. Hierzu wurde ein eigenes Zertifizierungsschema entwickelt [18]. Mittelfristiges Ziel ist die Positionierung von ISIS12 als eigenen Standard auf dem Markt [17]. ISIS12 wurde zudem mit der Möglichkeit zur Skalierbarkeit entwickelt. Nach einer erfolgreichen ISIS12 Implementierung und weiteren erforderlichen Schritten kann eine Zertifizierung nach „ISO/IEC 27001“ bzw. „ISO 27001 auf Basis von IT-Grundschutz“ vorbereitet und durchgeführt werden.

## 3.1 ISIS12 Vorgehensmodell

Der ISIS12-Workflow sieht 12 Schritte vor, die in drei Grobphasen – Initialisierungsphase, Festlegung der Aufbau- und Ablauforganisation, Entwicklung und Umsetzung ISIS12-Konzept – eingeteilt sind. ISIS12 beschreibt ein sequentielles Verfahren, welches den Top-Down Ansatz verfolgt. Die Unternehmensleitung trägt die Gesamtverantwortung für die Informationssicherheit, initiiert den dafür notwendigen Sicherheitsprozess und stellt die dafür erforderlichen Ressourcen zur Verfügung. Ohne diese Basis sind die weiteren Schritte nicht erfolgreich umzusetzen. In den ersten zwei Phasen werden die wichtigen Vorarbeiten, wie die Erstellung der Leitlinie zur Informationssicherheit und Festlegung der Aufbau- und Ablauforganisation, durchgeführt, bevor mit den operativen Arbeiten im Schritt 6 der Konzeption und Implementierung der integrierten Sicherheitskonzeption begonnen wird. [14]

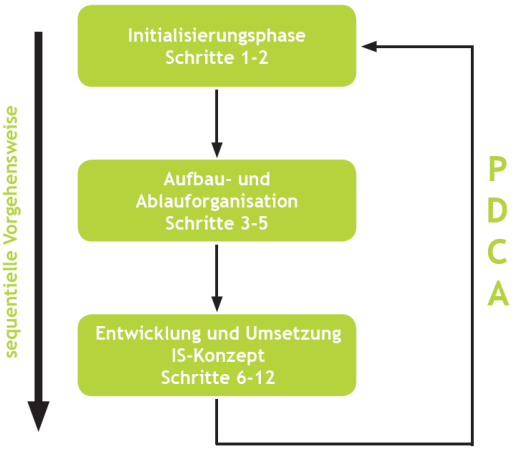


Abbildung 1: Grobphasen des ISIS12-Vorgehensmodells [14]

Ein Informationssicherheitsmanagementsystem ist ein wiederkehrender Prozess, der in Organisationen Einzug finden muss, um Informationssicherheit nachhaltig und dauerhaft zu gewährleisten. Die ISIS12-Schritte werden zeitabhängig iterativ durchlaufen, so dass sich ein PDCA-Zyklus einstellt (vgl. Abbildung 1). Die ausführlichen ersten zwei Phasen sind sehr wichtig für den Erfolg der ISMS-Einführung und sind bei anderen Vorgehensmodellen (IT-Grundschutz, ISO/IEC 27001) nicht so explizit wie es bei ISIS12 der Fall ist.

Die Abbildung 2 veranschaulicht das ISIS12 Vorgehensmodell zur Einführung eines ISMS in 12 Schritten.

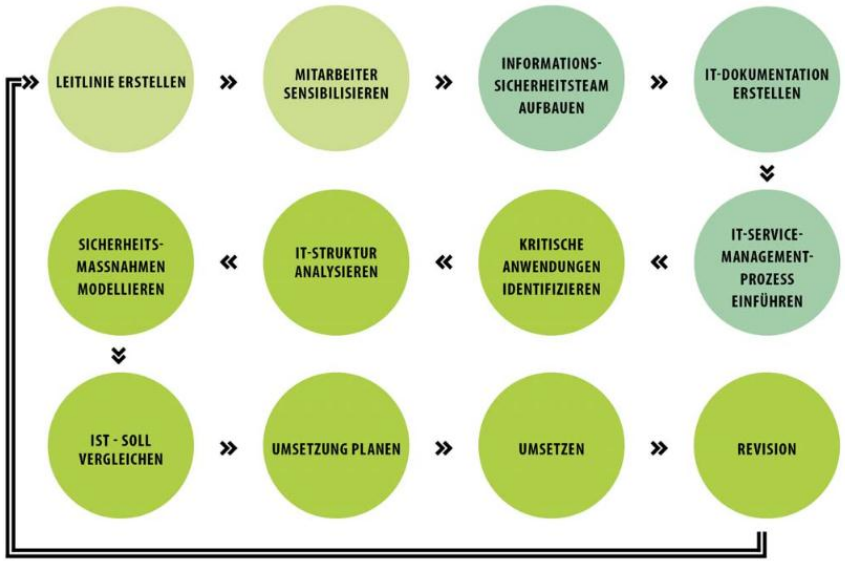


Abbildung 2: ISIS12 Vorgehensmodell [14]

Im Folgenden werden die zwölf Schritte kurz beschrieben. Die ausführlichen Informationen können dem ISIS12-Handbuch [14] entnommen werden.

### I. Initialisierungsphase

Schritt 1: *Leitlinie erstellen*: Als erstes wird eine Leitlinie für Informationssicherheit erstellt, in der die den Geschäftszielen korrespondierenden Informationssicherheitsziele und das angestrebte Sicherheitsniveau beschrieben sowie die daraus abgeleitete Strategie fixiert werden. Diese Leitlinie wird vom Management verabschiedet und den Mitarbeitern kommuniziert.

Schritt 2: *Mitarbeiter sensibilisieren*: Alle Organisationsebenen werden für die Bedeutung der Informationssicherheit sensibilisiert. Es wird frühzeitig um Kooperation und Mitarbeit der betroffenen Abteilungen geworben („Jeder ist für Informationssicherheit verantwortlich!“) und über die Arbeitsaufwände informiert.

### II. Festlegung der Aufbau- und Ablauforganisation

Schritt 3: *Informationssicherheitsteam aufbauen*: In diesem Schritt werden die Zusammensetzung, die Aufgaben und Pflichten des Sicherheitsteams festgelegt und die Teammitglieder werden mit der ISIS12-Methodik vertraut gemacht. Die zentrale Rolle nimmt dabei der Informationssicherheitsbeauftragte (ISB) ein. Weitere Teammitglieder können sein: Datenschutzbeauftragter, QM-Beauftragter, IT-Mitarbeiter, externer ISIS12-Berater etc.

Schritt 4: *IT-Dokumentation erstellen*: Da eine aktuelle und ganzheitliche IT-Dokumentation eine wesentliche Voraussetzung für das Gelingen von ISIS12 darstellt, wird eine Struktur für die IT-Dokumentation entwickelt und eingeführt. Neben formalen Festlegungen wie etwa Versionierung und verpflichtende Dokumenteninformationen werden verbindliche Dokumentenvorlagen und Rahmendokumente (Leitlinie, Organigramm, IT-Kompetenzmatrix, IT-Namenskonvention, Dokumentationsrichtlinie und Verfahrensanweisung) erarbeitet. Damit wird der Grundstein für eine nachhaltige IT-Dokumentation gelegt und Redundanzen vermieden. Auf der Basis der Rahmendokumente werden IT-Betriebshandbuch und IT-Notfallhandbuch erstellt. Das IT-Betriebshandbuch führt alle Schritte auf, die einen reibungslosen Betrieb der IT-

Systeme sicherstellen, und ist nach Systemakten und Prozesssteckbriefen gegliedert. Das IT-Notfallhandbuch enthält alle Maßnahmen und Zuständigkeiten, die bei einem Notfall zu ergreifen sind, um die Wiederaufnahmen des unterbrochenen Betriebs zu ermöglichen, wie z.B. Alarmierungspläne und Sofortmaßnahmen.

Schritt 5: *IT-Service-Management-Prozess (ITSM) einführen*: ISIS12 fordert die Definition der drei fundamentalen IT-Service-Management-Prozesse: Wartung, Änderung und Störungsbeseitigung. Zu jedem ITSM-Prozess wird ein Prozesssteckbrief erstellt und dem IT-Betriebshandbuch hinzugefügt sowie eine verantwortliche Stelle oder Person zugeordnet. Bei der Störungsbeseitigung sind die maximal tolerierbaren Ausfallzeiten (MTA) der wichtigsten IT-Systeme, die im ISIS12 Schritt 7 definiert werden, zu berücksichtigen.

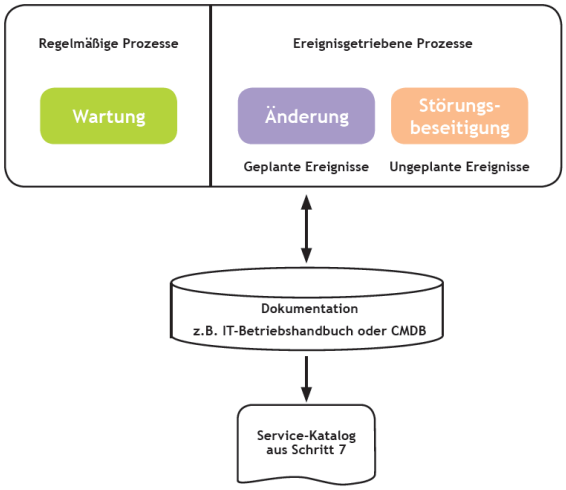


Abbildung 3: ISIS12 IT-Service-Management-Prozesse [14]

## III. Operative Arbeiten: Entwicklung und Umsetzung ISIS12-Konzept

Schritt 6: *Kritische Anwendungen identifizieren*: Das Kernstück bei der Entwicklung des integrierten ISMS stellt die Lokalisierung und Bewertung kritischer Anwendungen dar. Deren Schutzbedarf wird jeweils bezogen auf die Grundwerte Vertraulichkeit, Integrität und Verfügbarkeit untersucht und klassifiziert. Dies ist ein stark an den BSI IT-Grundschutz angelehntes Verfahren. Aus der Schutzbedarfsfeststellung werden die MTA (Maximal tolerierbare Ausfallzeit) und SLA (Service Level Agreement) abgeleitet, die im Service-Katalog dokumentiert werden. Zusätzlich wird die Verarbeitung personenbezogener Daten erfasst. Schritt 6 ist die Basis für das in den folgenden Schritten zu erstellende Sicherheitskonzept.

Schritt 7: *IT-Struktur analysieren*: In diesem Schritt erfolgt die Definition und Erfassung des Informationsverbundes. Den lokalisierten kritischen Anwendungen werden die erforderlichen IT-Systeme und Infrastruktur (Gebäude, Client- und Serversysteme, Netzwerk- und TK-Komponenten) zugeordnet. Bei ISIS12 werden IT-Systeme als Ganzes betrachtet. Schutzbedarf, MTA und SLA der Applikationen werden auf die IT-Systeme und infrastrukturelle Objekte vererbt.

Schritt 8: *Sicherheitsmaßnahmen modellieren*: Die Ergebnisse der vorausgegangenen Strukturanalyse werden auf Plausibilität geprüft und eventuell angepasst. Jedem in der Strukturanalyse gefundenen Objekt (Anwendung, IT-Systeme, Räume, Gebäude etc.) wird ein entsprechender Baustein zugeordnet, der eine Liste empfohlener und umzusetzender

Sicherheitsmaßnahmen enthält. Hierbei wird der ISIS12-Katalog verwendet. Die Verknüpfung der IT-Zielobjekte mit den Maßnahmen des ISIS12-Maßnahmenkatalogs geschieht mit dem ISIS12-Tool automatisch.

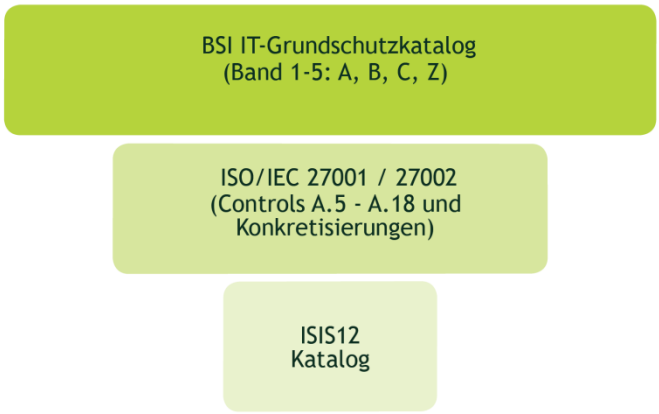


Abbildung 4: Genese des ISSI12-Katalogs [15]

Der Detailierungsgrad zwischen BSI IT-Grundschutz (extrem hoch) und der ISO/IEC 27001 (minimalistisch und abstrakt) wurde auf die Zielgruppe der mittelständischen Unternehmen angepasst (vgl. Abbildung 4). Bei Bedarf können in dieser Phase des Vorgehensmodells benutzerdefinierte Bausteine in den Katalog integriert werden, soweit dies erforderlich erscheint. Dieser modulare Aufbau des ISIS12 stellt einen Vorteil gegenüber dem etwas statischen IT-Grundschutz-Vorgehen dar.

Schritt 9: *Ist-Soll vergleichen*: Es wird der aktuelle Umsetzungsgrad der im Schritt 8 empfohlenen Sicherheitsmaßnahmen untersucht und mit „ja“, „teilweise“, „nein“ oder „nicht notwendig“ bewertet. Ziel ist es, die noch nicht vollständig umgesetzten Maßnahmen bezogen auf die IT-Zielobjekte zu identifizieren, da diese in den weiteren Schritten noch wirksam umzusetzen sind. Bereits vollständig umgesetzte Maßnahmen („ja“) und entbehrliche Maßnahmen („nicht notwendig“) werden an dieser Stelle bereits mit einem Revisionsdatum versehen, um diese dann im Rahmen des PDCA-Zyklus zu einem späteren Zeitpunkt erneut auf Wirksamkeit und Angemessenheit überprüfen zu können. Hier besteht auch die Möglichkeit zur ersten Messung des erreichten Grads an Informationssicherheit, wie z.B. „100% – X% der noch nicht umgesetzten Sicherheitsmaßnahmen aus dem ISIS12-Katalog“.

Schritt 10: *Umsetzung planen*: Die noch ganz oder teilweise nicht umgesetzten Sicherheitsmaßnahmen werden zunächst konsolidiert, dann bzgl. des Schutzbedarfs und der Breitenwirkung priorisiert und zusammen mit einer Kostenplanung (Bewertung der einmaligen und wiederkehrenden Kosten) der Geschäftsleitung als Entscheidungsvorschlag präsentiert. Hieraus resultiert ein konkreter Umsetzungsplan inkl. Umsetzungszeitraum und der Umsetzungsreihenfolge.

Schritt 11: *Umsetzen*: Die im vorhergehenden Schritt 10 genehmigten Sicherheitsmaßnahmen werden umgesetzt. Für jede Maßnahme werden die Rolle des Initiators/Umsetzers und der Zeitpunkt der finalen Realisierung festgelegt. Neben der Steuerung muss die Wirksamkeit der umgesetzten Maßnahmen kontrolliert werden.

Schritt 12: *Revision*: Im „abschließenden“ Schritt werden im Sinne des PDCA-Prinzips (Plan-Do-Check-Act) die Aktualität der ISIS12-Schritte eins bis elf und die wirksame Umsetzung der noch offenen Sicherheitsmaßnahmen im Sinne einer Revision kontinuierlich untersucht. Dadurch wird eine stetige Optimierung des ISMS erreicht.

## 3.2 ISIS12 Zertifizierung

Im Rahmen des ISIS12 Vorgehens besteht die Möglichkeit eine optionale ISIS12-Zertifizierung durchzuführen. Die Zertifizierung verfolgt extern den Zweck, Geschäftspartnern die Qualität des etablierten Managementsystems intersubjektiv zu belegen. Intern trägt eine Zertifizierung dazu bei, das ISMS ständig aktuell zu halten und kontinuierlich zu optimieren.

Nach Abschluss von Schritt 11 kann ein zertifizierter ISIS12-Auditor der DQS (Deutsche Gesellschaft zur Zertifizierung von Managementsystemen) nach dem ISIS12-Auditierungs- und Zertifizierungsschema [18] die Organisation prüfen. Grundlage für dieses ISIS12-Schema, die in Zusammenarbeit mit der DQS GmbH erstellt wurde, sind die Dokumente Auditierungs- [19] und Zertifizierungsschema [20] für eine Zertifizierung nach „ISO 27001 auf der Basis von IT-Grundschutz".

Im ISIS12-Zertifizierungsprozess gibt es drei Rollen:

1. *Antragsteller* als Initiator des Zertifizierungsprozesses stellt den Antrag auf Zertifizierung bei der Zertifizierungsstelle.
2. *Auditor* prüft die Referenzdokumente und das ISMS auf Wirksamkeit vor Ort und erstellt den Auditbericht für die Zertifizierungsstelle. Der Auditor muss alle 3 Jahre wechseln.
3. *Zertifizierungsstelle* wurde von der „ISIS12-Netzwerkgruppe" autorisiert, als unabhängige Instanz und auf Grundlage des jeweils aktuellen Zertifizierungs- und Auditierungsschemas für ISIS12 den Audit-Bericht zu prüfen. Bei positivem Prüfergebnis erteilt die DQS für den Informationsverbund des Antragsstellers ein ISIS12-Zertifikat. Des Weiteren prüft die Zertifizierungsstelle die Unabhängigkeit des Auditors und stellt sicher, dass Auditoren nach den Richtlinien der „ISIS12-Netzwerkgruppe" ausgebildet sind und somit entsprechende Audit- und ISIS12-Kenntnisse vorweisen (Lizenzierung der ISIS12-Auditoren). [18]

Die folgende Abbildung 5 zeigt die diesen drei Rollen zugeordneten Aufgaben und ihr Zusammenwirken bei der Zertifizierung.

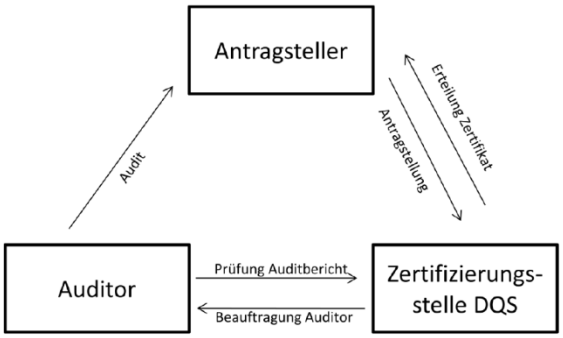


Abbildung 5: ISIS12-Zertifizierung Rollenverteilung [18]

Das ISIS12-Zertifikat wie auch ein ISO/IEC 27001 Zertifikat hat eine Gültigkeit von drei Jahren. Daraus ergeben sich die folgenden drei Audit-Typen:

- *Erst-Zertifizierungs-Audit*: Erstmalige Auditierung des Informationsverbundes und des ISMS nach ISIS12-Gesichtspunkten. Normalerweise dauert dieses Audit zwei Tage.

- *Überwachungs-Audit*: Jährliche eintägige Überwachungs-Audits des zertifizierten Informationsverbundes um sicherzustellen, dass der zertifizierte Informationsverbund auch weiterhin den ISIS12-Anforderungen entspricht. Die Überwachungs-Audits dürfen nicht früher als drei Monate vor Ablauf des ersten bzw. zweiten Jahres nach Zertifikatserteilung beginnen. Das Überwachungs-Audit, der Auditbericht und dessen Prüfung durch die Zertifizierungsstelle müssen ein bzw. zwei Jahre nach Ausstellung des Zertifikats abgeschlossen sein.
- *Rezertifizierungs-Audit*: Nach drei Jahren ist ein Rezertifizierungs-Audit erforderlich. Dieses unterscheidet sich bzgl. der Fristen und Voraussetzungen nicht vom Erst-Zertifizierungs-Audit. Der Auditbericht muss der Zertifizierungsstelle der DQS mindestens 2 Monate vor dem Gültigkeitsende des Zertifikates vorliegen.

Die Abbildung 6 stellt den Zertifizierungsablauf mit den drei ISIS12 Audit-Typen dar.


Abbildung 6: Zertifizierungsablauf [18]

Nach der Festlegung des Geltungsbereichs der Zertifizierung durch die Organisation (R.2 Beschreibung des Geltungsbereichs) erfolgt die ISIS12-Auditierung, die aus folgenden drei Teilen besteht:

1. *Dokumentenprüfung*: Der Auditor prüft, ob die Zertifizierungsfähigkeit des Informationsverbundes prinzipiell gegeben ist. Die Einsicht in die Dokumente erfolgt vor Ort. Hierzu werden dem Auditor die folgenden Referenzdokumente zur Verfügung gestellt:

   R.1 Unternehmensleitlinie für Informationssicherheit
   R.2 Beschreibung des Geltungsbereichs
   R.3 IT-Betriebshandbuch
   R.4 IT-Notfallhandbuch
   R.5 Bereinigter Netzplan
   R.6 Schutzbedarfsfeststellung und Sicherheitskonzept
   R.7 Umsetzungsplan

2. *Umsetzungsprüfung der ISIS12-Schritte*: Bei der Umsetzungsprüfung überzeugt sich der Auditor von der wirksamen Umsetzung der ISIS12-Schritte 1-11 anhand der Kontrollfragen.

3. *Umsetzungsprüfung von ISIS12-Sicherheitsmaßnahmen*: Der Auditor prüft die wirksame Umsetzung von Sicherheitsmaßnahmen aus fünf Bausteinen. Die Bausteine werden vom Auditor nach folgenden Regeln gewählt:

   - Aus Schicht 1 den Baustein 1.1 und zwei Bausteine nach Wahl des Auditors,
   - Aus Schicht 2 den Baustein 2.3 und einen Baustein nach Wahl des Auditors sowie
   - Aus Schicht 3-4 zwei Bausteine nach Wahl des Auditors.

Die Ergebnisse der Prüfung werden vom Auditor im Audit-Bericht dokumentiert. Bei dem Audit vor Ort werden sich in manchen Fällen Abweichungen ergeben. Diese müssen sachgerecht behoben werden. Dabei gibt es verschiedene Stufen der Behandlung von Abweichungen:

- *Schwerwiegende Abweichungen* (Hauptabweichung – 4) sind Mängel, ohne deren Behebung nicht sichergestellt werden kann, dass das ISMS effektiv und effizient funktioniert oder die Sicherheit des Informationsverbundes erheblich gefährdet ist. Ein solcher Mangel kann vorliegen, wenn ISIS12-Maßnahmen nicht oder in wesentlichen Teilen nicht umgesetzt sind. Bei Vorliegen schwerwiegender Abweichungen ist die Ausstellung eines ISIS12-Zertifikats nicht möglich.
- *Geringfügige Abweichungen* (Nebenabweichung – 3) sind zu kennzeichnen und mit einer Frist zur Behebung zu versehen. Sie kommen dann zustande, wenn einzelne Aspekte einer Maßnahme nicht umgesetzt wurden, aber das wesentliche Ziel der Maßnahme realisiert ist. Dies ist beispielsweise dann der Fall, wenn einzelne Teile eines Konzeptes konkretisiert oder aktualisiert werden müssen. Eine Ausstellung des Zertifikats kann unter Umständen trotzdem erfolgen. Mehrere geringfügige Abweichungen können allerdings zusammen eine schwerwiegende Abweichung darstellen.
- Der Auditor hat die Möglichkeit, *Empfehlungen* (Verbesserung – 2) an die Institution auszusprechen. Diese sind zwar nicht bindend, erhöhen aber die Effektivität und Effizienz des ISMS. Empfehlungen sind zum Beispiel Verbesserungsvorschläge, die im Rahmen der kontinuierlichen Verbesserung des Prozesses umgesetzt werden sollten, zumindest jedoch zu prüfen sind. Daher führt eine Nichtbeachtung zu einer geringfügigen Abweichung.

Der Auditor entscheidet bei Abweichungen, ob es sich um schwerwiegende oder geringfügige Abweichungen handelt. Er informiert die Institution möglichst frühzeitig schriftlich über festgestellte Abweichungen, damit diese zeitnah behoben werden können. Er muss der Organisation hierzu eine angemessene Frist einräumen. Die Liste mit den Abweichungen und die Frist zur Nachbesserung für die Korrekturmaßnahmen sowie die Empfehlungen werden im Auditbericht dokumentiert. Der Auditor prüft anhand der Dokumente vor Ort, ob alle festgestellten schwerwiegenden Abweichungen behoben wurden und dokumentiert die Prüfungsergebnisse im Auditbericht. Geringfügige Abweichungen werden ebenfalls mit einer Nachbesserungsfrist versehen, deren Behebung muss aber erst beim nächsten Überwachungsaudit begutachtet werden. Die Abbildung 7 stellt die Antrags- und Auditierungsphase dar.

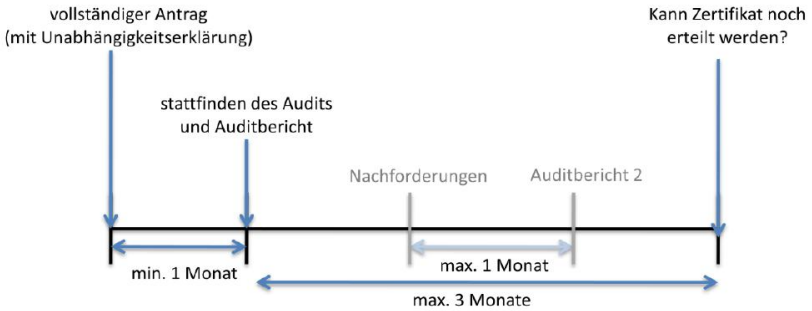


Abbildung 7: Antrags- und Auditierungsphase [18]

Der Auditbericht, der alle Prüfaktivitäten und -ergebnisse dokumentiert, wird vom Auditor erstellt, unterschrieben und der Zertifizierungsstelle weitergeleitet. Er ist vertraulich zu behandeln und nicht an Dritte weiterzugeben. Der Auditbericht wird von der Zertifizierungsstelle begutachtet und ist die Basis für die Erteilung des ISIS12-Zertifikats (bei Erst- oder Rezertifizierung) bzw. der Aufrechterhaltung des Zertifikats beim Überwachungsaudit. Der Auditor gibt im Fall einer positiven

Bewertung eine Empfehlung an die DQS. Die DQS erteilt anschließend ein ISIS12-Zertifikat für den geprüften Geltungsbereich. Unter bestimmten Voraussetzungen kann die Zertifizierungsstelle ISIS12-Zertifikate aussetzen bzw. zurückziehen. Bei nicht fristgerechter Einreichung des Auditberichts oder negativem Abschluss des Überwachungsaudits kann die Zertifizierungsstelle das bestehende Zertifikat zurückziehen. Es erfolgt somit keine Bestätigung des Zertifikats.

# 4 Mindestanforderungen und Rahmenbedingungen der öffentlichen Verwaltungen

Die IT der öffentlichen Verwaltung unterliegt besonderen Einflüssen, wie etwa das regulatorische Umfeld (Gesetze und Verordnungen), ausgeprägte Hierarchie, Haushalt (Kameralistik), die Dynamik des Leistungsportfolios (z.B. E-Government), die Steuerung (Controlling) sowie traditionell sehr präzise Vorgaben zu einzelnen Geschäftsabläufen. Die öffentliche Verwaltung hängt in ständig steigendem Maße bei ihrer Aufgabenwahrnehmung und dem Erreichen der Behördenziele von einem sicheren IT-Einsatz ab. Mit dem am 1. August 2013 in Kraft getretenen E-Government-Gesetz des Bundes [21] wurden die entscheidenden rechtlichen Voraussetzungen für ein breites Angebot elektronischer Dienstleistungen der Verwaltung geschaffen. Wesentliches Ziel des Gesetzes ist es, auf allen staatlichen Ebenen nutzerfreundliche, effiziente und medienbruchfreie elektronische Verwaltungsverfahren bereitzustellen. Die Gewährleistung von Verfügbarkeit, Vertraulichkeit, Integrität, Authentizität und Nachweisbarkeit im jeweils erforderlichen Maße ist unabdingbare Voraussetzung und Bestandteil jedes IT-Verfahrens.

Ein Großteil der Verwaltungskontakte der Bürgerinnen und Bürger (z.B. KFZ, Einwohnermeldewesen, Personenstandwesen etc.) entfällt auf die Kommunalverwaltung. Die Bundesländer selbst bieten wenige Leistungen direkt für die Bürger wie z.B. Elterngeld oder Betreuungsgeld an. Deswegen sind der Einsatz von Informationstechnik und das Angebot der E-Government-Anwendungen auf kommunaler Ebene besonders bedeutsam. In vielen Kommunen, bei denen die Prozesse über E-Government-Anwendungen ihren Bürgern angeboten werden, gilt: „Die Anwendung ist das Geschäft“.

Viele IT-Verfahren und Geschäftsprozesse der öffentlichen Verwaltung vollziehen sich zunehmend in miteinander vielfältig vernetzten Systemen auf allen drei Ebenen (Bund – Land - Kommune), wie es im Beispiel des Zentralen Melderegisters der Fall ist. Daraus ergeben sich völlig neue Risiken sowohl in qualitativer als auch in quantitativer Hinsicht. Dies führt dazu, dass die ganze Prozesskette abgesichert werden muss, weil „eine Kette nur so stark ist wie ihr schwächstes Glied“. Daraus leitet sich die Anforderung ab, dass Kommunen die Leitlinie des IT-Planungsrats [3] umsetzen müssen. Fehlende oder unzureichende Sicherheitsmaßnahmen können zu großen materiellen und immateriellen Schäden mit teilweise beträchtlichen politischen Auswirkungen führen. Somit muss IT-Sicherheit zwingend als integraler Bestandteil der originären Fachaufgabe betrachtet werden. Damit verbleibt, ausgehend von der fachlichen Verantwortung, die letztendliche Verantwortung für IT-Sicherheit bei der jeweiligen Behördenleitung. Nach der Selbstverwaltungsgarantie - in Artikel 28 Absatz 2 Satz 1 des Grundgesetzes der Bundesrepublik Deutschland bzw. auf Landesebene z.B. Artikel 10 und 11 in der Verfassung des Freistaates Bayern - üben die Kommunen in Deutschland das Selbstverwaltungsrecht verfassungsmäßig aus. Dadurch sind sie selbst im Rahmen des eigenen Wirkungskreises für Verwaltungsverfahren und ihre Sicherheit verantwortlich sowie erfüllen ihre Aufgaben unabhängig und eigenverantwortlich ohne Weisungen von übergeordneten Stellen [22].

Darüber hinaus sind IT-Prozesse der öffentlichen Verwaltung in der Regel wenig dokumentiert, es gibt viele Ausnahmen und oftmals nur wenige wiederholbare Prozesse. Die Nachvollziehbarkeit und der geregelte IT-Betrieb stellen jedoch eine Grundvoraussetzung für eine erfolgreiche Einführung eines ISMS und für die Informationssicherheit selbst dar.

Da Behörden eine sehr hohe Heterogenität aufweisen, ist es in der Regel sehr schwer, alle Vorgaben und Anforderungen zusammenzuführen. Deswegen ist die Verwendung eines abstrahierten Metamodells in diesem Zusammenhang hilfreich. Bei der Begutachtung der Eignung des ISIS12-Vorgehens bei der Einführung des ISMS in der öffentlichen Verwaltung wird von einer „*Standardbehörde*“ ausgegangen. Ihre Definition erfolgt in Anlehnung an die BSI Definition [23]. Eine „Standardbehörde“ hat:

- bis zu ca. 500 Mitarbeiter,
- eine möglichst homogene IT-Basisinfrastruktur,
- keine über öffentliche Netze ungeschützt angebundene Außenstellen,
- einen überwiegend normalen Schutzbedarf,
- keine Hochverfügbarkeitsanforderungen an IT-Systeme und
- keine kritischen Anwendungen (im Sinne keine kritischen Infrastrukturen).

Die Definition betrifft vor allem kleine bis mittelgroße Behörden bzw. Kommunen mit niedrigem bis mittlerem Schutzbedarf. Für Landesverwaltungen, große Behörden und große Städte wie z.B. München, Nürnberg, Augsburg etc. sowie für Bereiche mit besonderen Sicherheitsanforderungen wie z.B. Polizei, Feuerwehr, Steuerverwaltung ist ein Vorgehen nach ISO/IEC 27001 oder nach BSI IT-Grundschutz unabdingbar. Für Sicherheitsdomänen, bei denen der IT-Grundschutz nicht ausreicht, ist zusätzlich zum IT-Grundschutz das ebenfalls vom BSI herausgegebene "IT-Sicherheitshandbuch" partiell und ergänzend auf die durch den IT-Grundschutz nicht oder nicht ausreichend geschützten Objekte anzuwenden. In allen Fällen ist das Verhältnismäßigkeitsgebot - aufzuwendende Mittel im Verhältnis zum Grad der Sicherheitsverbesserung - zu beachten. Verbleiben trotz der realisierbaren Sicherheitsmaßnahmen untragbare Risiken, dann ist der IT-Einsatz so zu modifizieren, dass den Sicherheitsanforderungen entsprochen werden kann.

# 5 Bewertung

In diesem Kapitel wird die Anwendbarkeit des ISIS12 in der öffentlichen Verwaltung bewertet. Es wird dargestellt, inwieweit die Anforderungen des IT-Planungsrats an ein ISMS erfüllt werden sowie die Hauptunterschiede zwischen ISIS12 und ISO/IEC 27001 Zertifizierungen auf Basis des IT-Grundschutzes und nativ beschrieben.

## 5.1 Erfüllung der Mindestanforderungen des IT-Planungsrats an ISMS durch ISIS12

In der folgenden Tabelle wird die Erfüllung der in der „Leitlinie für die Informationssicherheit in der öffentlichen Verwaltung“ des IT-Planungsrats [3] festgelegten Mindestanforderungen an das ISMS beschrieben.

| Nr. | Mindestanforderungen an ISMS aus der Leitlinie des IT-Planungsrats [3] | Erfüllt durch ISIS12 im Schritt n (S*) | Begründung |
|---|---|---|---|
| 1 | Festlegung und Dokumentation von Verantwortlichkeiten hinsichtlich des Informationssicherheitsmanagements (z.B. Benennung des ISB). | S1 und S3 | Im Schritt 1 wird schriftlich festgehalten, dass die Unternehmensleitung die Gesamtverantwortung für Informationssicherheit hat. Im Schritt 3 wird ein IS-Team aufgebaut und ein Informationssicherheits-beauftragter (ISB) ernannt. |
| 2. | Erstellung von jeweiligen verbindlichen Leitlinien für die Informationssicherheit. | S1 | Im Schritt 1 wird die Leitlinie für die Informationssicherheit erstellt. |
| 3. | Erstellung und Umsetzung von Sicherheitskonzepten für Behörden und Einrichtungen. | S1-12 bzw. S6-12 | Die ganze ISIS12 Vorgehens-weise ist darauf ausgerichtet, die Sicherheitskonzepte zu erstellen und umzusetzen. Die Schritte 1 bis 5 stellen lediglich die Vorbereitung und Basis für die operativen Arbeiten in den Schritten 6 bis 12 dar. |
| 4. | Festlegung und Dokumentation der Abläufe bei IT-Sicherheitsvorfällen. | S5 | Bei IT-Sicherheitsvorfällen geht es vor allem um die Störungs-beseitigung (ITSM-Prozess im Schritt 5 eingeführt) |

| | | | |
|---|---|---|---|
| 5. | Etablierung von Prozessen, mit denen Umsetzung, Wirksamkeit und Beachtung der Informationssicherheitsmaßnahmen regelmäßig kontrolliert und die Einleitung ggf. erforderlicher Maßnahmen (z.B. Fortschreibung Sicherheitskonzepte) gewährleistet wird. | Plan-Do-Check-Act (PDCA) mit S9, S12 | Im ISIS12 Vorgehensmodell spielt das PDCA Zyklus mit seinen regelmäßigen Kontrollen eine wichtige Rolle. PDCA kommt vor allem im Schritt 9 „Ist-Soll Vergleich der umgesetzten Informationssicherheitsmaßnahmen“, im Schritt 12 „Revision“ sowie am Ende fast jedes ISIS12-Schrittes im Punkt Revision zustande. |
| 6. | Information, Weiterbildung, Sensibilisierung aller Beschäftigten der öffentlichen Verwaltung zu Themen der Informationssicherheit. Hierzu gehört auch die Etablierung und Durchführung regelmäßiger Sensibilisierungsmaßnahmen für die oberste Leitungsebene. | S1 und S2 | Im Schritt 1 wird die Leitlinie den Mitarbeitern bekannt gegeben und sie werden zu ihrer Einhaltung motiviert. Schritt 2 „Mitarbeiter sensibilisieren“ zielt auf die Sensibilisierung aller Organisationsebenen inkl. der Leitungsebene für die Bedeutung der Informations-sicherheit. |
| 7. | Anforderungsgerechte und einheitliche Fortbildung der ISB. Eine Zertifizierung der ISB wird angestrebt. | | Die Bundesakademie für öffentliche Verwaltung (BAköV) bietet ein Fortbildungs-programm für IT-Sicherheitsbeauftragte an, u.a. Jahrestagung für ISB [24], Fortbildung für ISB in der öffentlichen Verwaltung und Zertifizierung von ISB in der öffentlichen Verwaltung – Basis bzw. Aufbau [25]. |
| 8. | Jahrestagungen der ISB zum gegenseitigen Erfahrungsaustausch (Verantwortung für Organisation wechselt mit Vorsitz im IT-Planungsrat). | | Dies ist keine direkte Anforderung an ein ISMS. |

Aus der Tabelle wird deutlich, dass die Mindestanforderungen an ein ISMS, die in der Leitlinie des IT-Planungsrats definiert sind, durch das ISIS12 Verfahren erfüllt werden. Die letzten zwei Anforderungen sind keine direkten Anforderungen an ein ISMS, sondern sind als Maßnahmen zu Erhalt, Aktualisierung und Erhöhung der beruflichen Kompetenzen von Informationssicherheitsbeauftragten zu verstehen.

## 5.2 ISIS12 Vorgehensmodell

Das ISIS12 Vorgehensmodell wurde den Bedürfnissen und Ressourcen der Zielgruppe KMU angepasst. Die grundlegenden Unterschiede im Vorgehen zwischen dem ISIS12 und BSI IT-Grundschutz bzw. ISO/IEC 27001 werden hier beschrieben und motiviert. Die wesentlichen Unterschiede des ISIS12 Vorgehensmodells sind die Durchführung einer immanenten Risikoanalyse und die Einführung der IT-Service-Management-Prozesse im Rahmen einer ISMS Etablierung.

### 5.2.1 Risikoanalyse

Eine Risikoanalyse im Kontext der Informationssicherheit hat die Aufgabe, relevante Gefährdungen für den Informationsverbund zu identifizieren und die daraus möglicherweise resultierenden Risiken abzuschätzen. Das Ziel ist es, die Risiken durch angemessene Gegenmaßnahmen auf ein akzeptables Maß zu reduzieren, die Restrisiken transparent zu machen und dadurch das Gesamtrisiko systematisch zu steuern. Der effektive Umgang mit IT-Risiken erfordert in jedem Fall eine strukturierte Vorgehensweise, in welcher der IT-Risikoanalyse als wichtigem Werkzeug zur Identifikation der relevanten Risiken eine zentrale Rolle zukommt.

Eine Risikoanalyse wird sowohl im Rahmen des IT-Grundschutzes als auch im Rahmen ISO/IEC 27001 durchgeführt. Bei der Entwicklung von ISIS12 wurde, ausgehend von den Designkriterien, auf eine vorangestellte Risikoanalyse verzichtet, wie dies etwa bei der ISO/IEC 27001 der Fall ist. Auch nachgestellt wird, wie bei der BSI IT-Grundschutzmethodik, keine Risikoanalyse explizit angewandt (BSI IT-Grundschutz Standard 100-3 [12]). Stattdessen beinhaltet das an die BSI-Grundschutzmethodik angelehnte ISIS12 Verfahren eine sogenannte immanente Risikoanalyse. Die empfohlenen Sicherheitsmaßnahmen des ISIS12-Katalogs, die in der Umsetzungsphase wirksam umgesetzt werden müssen, decken Grundgefährdungen ab.

Die Standard-Sicherheitsmaßnahmen des IT-Grundschutzes sind in der Regel für typische Geschäftsprozesse, Anwendungen und IT-Systeme mit normalem Schutzbedarf angemessen und ausreichend. In bestimmten Fällen müssen die IT-Grundschutz-Maßnahmen jedoch mit Hilfe einer Risikoanalyse um spezielle Sicherheitsmaßnahmen ergänzt werden. Dies ist besonders bei Organisationen der Fall, die über einen höheren Schutzbedarf verfügen, wie z.B. Unternehmen mit Forschungsabteilungen, Just-in-Time-Lieferanten, Behörden mit besonderen Sicherheitsanforderungen wie Polizei, Feuerwehr, Verfassungsschutz und Ähnliches. Für solche Organisationen ist eine Risikoanalyse auch im Rahmen des ISIS12 Vorgehens empfehlenswert. [14]

Im ISIS12 Schritt 6 „Kritische Anwendungen identifizieren“ wird darauf hingewiesen, dass bei Anwendungen bzw. bei den damit verarbeiteten Informationen, die einen sehr hohen Schutzbedarf aufweisen, eventuell eine nachgelagerte Risikoanalyse angebracht ist. Im ISIS12 Vorgehensmodell, respektive dem ISIS12-Katalog, wird ein angemessenes Sicherheitsniveau angestrebt. Falls bei den verarbeiteten Informationen die Verletzung der Grundwerte Vertraulichkeit, Integrität oder Verfügbarkeit ein hohes Risiko für die Organisation darstellt, sollte die Durchführung einer Risikoanalyse in Erwägung gezogen werden. Aus Kompatibilität zum ISIS12 Vorgehensmodell bietet sich hier eine Vorgehensweise nach dem 2011 angepassten BSI-Standard 100-3 „Risikoanalyse auf der Basis von IT-Grundschutz“ [12] an. Durch die Verwendung der vom BSI publizierten 46 Grundgefährdungen [26] reduziert sich der dafür notwendige Aufwand erheblich. Es wird somit noch einmal analysiert, inwieweit die in der Sicherheitskonzeption enthalten Sicherheitsmaßnahmen aus dem ISIS12-Katalog für die Organisation angemessen sind. Es können sich daraus noch weitere zusätzliche Sicherheitsmaßnahmen ergeben, die in

die Sicherheitskonzeption integriert werden müssen. Diese grundlegende Entscheidung sollte mit der Leitungsebene diskutiert und letztendlich auch von dieser entschieden werden.

So kann im Rahmen des ISIS12 genau wie in der IT-Grundschutz-Vorgehensweise ein zweistufiger Ansatz verfolgt werden. In der ersten Stufe wird der Schutzbedarf der Objekte des Informationsverbundes (Schritt 6) ermittelt, die IT-Struktur analysiert (Schritt 7) und Standard-Sicherheitsmaßnahmen modelliert (Schritt 8). Dabei wird pauschal von einem üblichen Einsatzszenario und von einem normalen Schutzbedarf ausgegangen. Anhand der Bausteine des ISIS12-Katalogs analog zu IT-Grundschutz-Katalogen kann auf diese Weise das Sicherheitsniveau des Informationsverbundes schnell und effizient erhöht werden. Diese erste Stufe dient dazu, Sicherheitsmaßnahmen aufzuzeigen, die den elementaren Risiken entgegenwirken, die in der Praxis nahezu immer auftreten. Somit verfügt die ISIS12 Vorgehensweise über die erste Stufe der Risikoanalyse, in der eine grundlegende Risikobehandlung durchgeführt wird. Dem momentanen ISIS12 Vorgehen fehlt in diesem Zusammenhang im Vergleich zur IT-Grundschutz-Vorgehensweise die zweite Stufe der Risikoanalyse - eine sogenannte ergänzende Sicherheitsanalyse – in der weitere relevante Risiken für den Informationsverbund berücksichtigt werden. Diese müsste dann für alle Zielobjekte des Informationsverbundes durchgeführt werden, wenn sie

- einen hohen oder sehr hohen Schutzbedarf in mindestens einem der drei Grundwerte Vertraulichkeit, Integrität oder Verfügbarkeit haben oder
- mit den existierenden Bausteinen des ISIS12-Katalogs nicht hinreichend abgebildet (modelliert) werden können oder
- in besonderen Einsatzszenarien (z.B. in Umgebungen oder mit Anwendungen) betrieben werden. [11]

Im Rahmen der IT-Grundschutz-Vorgehensweise entscheidet die Leitungsebene auf der Basis des Management-Reports der ergänzenden Sicherheitsanalyse, für welche Zielobjekte eine Risikoanalyse durchgeführt wird. Der mit der Durchführung von Risikoanalysen verbundene Aufwand konzentriert sich somit auf die Bereiche, bei denen die Institution eine solche Risikoanalyse für zweckdienlich und gewinnbringend einschätzt. Für die Umsetzung der Entscheidungen, die in der ergänzenden Sicherheitsanalyse getroffen wurden, empfiehlt das BSI die Anwendung einer Risikoanalyse auf der Basis von IT-Grundschutz, wie sie im BSI-Standard 100-3 „Risikoanalyse auf der Basis von IT-Grundschutz“ beschrieben ist. ISIS12 verweist in diesem Fall ebenfalls auf den BSI-Standard 100-3 [12].

### 5.2.2 IT-Service-Management-Prozesse

Das IT-Service-Management (ITSM) umfasst die Implementierung und das Managen von Services, welche die Bedürfnisse einer Organisation und eine bestmögliche Unterstützung von Geschäftsprozessen durch die IT-Organisation abdecken. ITIL ist ein Best Practice Referenzmodell für IT-Serviceprozesse und sieht als solches, Sicherheitsaspekte als unverzichtbaren Bestandteil eines ordnungsgemäßen IT-Betriebs an.

Die öffentliche Verwaltung genauso wie Unternehmen ist heute in hohem Maß von der Verfügbarkeit von Informationssystemen abhängig. Oft wird die Informationssicherheit dadurch gefährdet, dass Verantwortlichkeiten und Abläufe bei der Wartung und Änderung der IT-Infrastruktur nicht ausreichend festgelegt sind. Das vorrangig zu erreichende Ziel, an welchem die in diesem Schritt umzusetzenden Maßnahmen gemessen werden sollen, ist die Sicherstellung einer stets aktuellen Dokumentation der IT-Landschaft einer Organisation. Zum Management der Informationssicherheit gehört daher auch ein grundlegendes IT-Service-Management. Dies wurde bei der Entwicklung des ISIS12-Verfahrens erkannt. Im

Vergleich zu den anderen Vorgehensweisen wie ISO/IEC 27001 und IT-Grundschutz werden im Rahmen von ISIS12 die grundlegenden IT-Service-Management-Prozesse – **Wartung, Änderung und Störungsbeseitigung** – eingeführt.

Die wichtigste Aufgabe in der Etablierung des *Änderungsmanagements* besteht darin, ein Optimum zwischen Flexibilität und Stabilität der Verfahren herzustellen. Hierbei ist sicher zu stellen, dass alle Änderungen unter Kontrolle des Managementprozesses gestellt werden. Ein besonderes Änderungsmanagementszenario stellt das Patch-Management dar. Sicherheitsrelevante Patches haben nicht nur eine hohe Brisanz und müssen in der Regel unter Termindruck ausgerollt werden, sondern sie greifen auch teilweise tief in bestehende Funktionalitäten und Prozesse ein. Hier gilt es, über gemeinsame Vorgaben Wege zu definieren, die den Zielkonflikt zwischen Reaktionsschnelligkeit und Qualitätssicherung ausgewogen beantworten.

*Wartung* ist einer der wichtigsten Prozesse im Verfügbarkeitsmanagement (Availability Management). Verfügbarkeit ist eines der zentralen Sicherheitsziele. Der Prozess liefert nicht nur Standards für die Verfügbarkeit und Wartbarkeit der IT-Komponenten, er bewertet auch die Chancen und Risiken der Auslagerung von Prozessen und Infrastruktur. Im Rahmen des ISIS12 werden die Service Level Agreements (SLAs) und die maximal tolerierbaren Ausfallzeiten (MTAs) definiert, die eine Verknüpfung zwischen den IT-Service-Management und Informationssicherheitsmanagement darstellen. Bei der Störungsbeseitigung werden die MTAs der wichtigsten IT-Systeme berücksichtigt.

*Störungsbeseitigung* stellt den dritten wichtigen ITSM-Prozess dar, der im Rahmen des ISIS12 Vorgehensweise eingeführt wird. Sicherheitsvorfälle sind Störungen in IT-Services und umgekehrt können Störungen in IT-Services auch Folge unerkannter Sicherheitsvorfälle sein. Durch die Verzahnung der Anforderungen des Sicherheits- und Service-Managements in einem gemeinsamen Störungsmanagementprozess, fördert die ISIS12 Vorgehensweise die Etablierung einer serviceorientierten IT-Organisation.

Im Schritt 5 des ISIS12 Vorgehensmodells werden die drei Basis ITSM-Prozesse beschrieben und verbindlich als Ziel des Schritts 5 gefordert. Dabei werden die Abläufe und vor allem die Zuständigkeiten für ITSM definiert. Der Änderungsprozess stellt einen wesentlichen Bestandteil des ISMS dar und wurde deshalb nicht als Baustein im Schritt 8 bzw. 9 betrachtet, sondern bereits im Rahmen der Ablauforganisation festgelegt. Im ISIS12-Handbuch wird ein Muster-Änderungsprozess mit den wesentlichen Handlungsrollen beschrieben. [14] In jährlich zu beantworteten Kontrollfragen wird ebenfalls überprüft, ob die IT-Service-Management-Prozesse wirksam umgesetzt und durchgeführt werden. Bei der IT-Grundschutz-Vorgehensweise, in der es einen eigenen Baustein für das Änderungsmanagement gibt, besteht die Gefahr, dass der Änderungsprozess erst zu einem späteren Zeitpunkt, z.B. erst nach Beginn der IT-Strukturanalyse, betrachtet und umgesetzt wird. Dies hat zur Folge, dass vormals durchgeführte Erhebungen nicht mehr aktuell sind. Bei ISIS12 wird diese Lücke durch eine frühere Einführung der ITSM-Prozesse vermieden und somit vollständig und effizient erfasst.

Inkonsistente und manuelle IT-Service-Management-Prozesse, die heute in der öffentlichen Verwaltung oft der Fall sind, erschweren es der Entwicklung und dem IT-Betrieb, zusammen zu arbeiten und Anfragen effizient und zeitnah zu erfüllen. Deswegen ist die Einführung der ITSM-Prozesse im Rahmen des ISIS12 Vorgehens insbesondere für kleine Kommunen und Behörden von Vorteil. Durch eine Umsetzung der IT-Service-Management-Prozesse, z.B. nach ITIL, ergeben sich erhebliche Chancen für ein noch wirksameres und effizienteres IT-Sicherheitsmanagement.

## 5.3 ISIS12-Katalog

Im ISIS12-Katalog [15] werden konkret umzusetzende Standard-Sicherheitsmaßnahmen für die Entwicklung des Sicherheitskonzepts beschrieben. Im Schritt 8 „*Sicherheitsmaßnahmen modellieren*“ wird der ISIS12-Katalog mit seinen Bausteinen, die eine Liste empfohlener und umzusetzender Sicherheitsmaßnahmen enthalten, verwendet. Wie im Kapitel 3.1 dargelegt, besteht der ISIS12-Katalog aus den gekürzten IT-Grundschutz-Katalogen und Maßnahmen, die aus ISO/IEC 27001/27002 abgeleitet wurden (s. auch Abbildung 4Abbildung 4: Genese des ISSI12-Katalogs . Die Reduktion der im BSI IT-Grundschutzkatalog enthaltenen Bausteine erfolgte in Verbindung mit den vom BSI publizierten „Goldenen Regeln“ [27]. Nach dem Grundsatz „So einfach wie möglich – aber nicht einfacher“ wurden die Bausteine zusammengefasst und vereinfacht. Im Gegensatz zur ISO/IEC 27001 stehen mit dem ISIS12-Katalog konkrete Handlungsempfehlungen zur Verfügung, deren Umfang entsprechend der Zielgruppe der kleinen und mittelständischen Unternehmen reduziert wurde.

Die Gliederung der BSI IT-Grundschutzkataloge in 5 Schichten (S) wurde dazu auf die folgenden vier Schichten reduziert (s. Abbildung 8). Die Schicht 1 wurde von „Übergreifende Aspekte“ bei BSI in „Universelle Aspekte“ beim ISIS12 umbenannt. Die Schichten 3 „IT-Systeme“ und 4 „Netze“ des IT-Grundschutzes wurden zur einen ISIS12 Schicht 3 „IT-Systeme und Netze“ zusammengelegt.

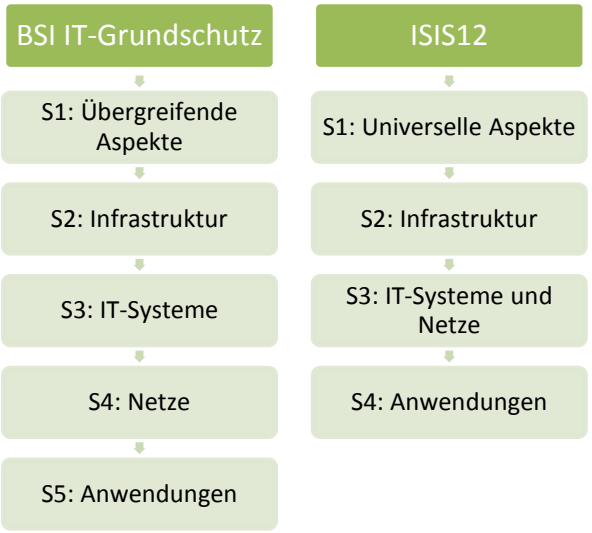


Abbildung 8: Gegenüberstellung des BSI IT-Grundschutzes und ISIS12

In den ISIS12 Schichten (S1 – S4) finden sich Bausteine mit entsprechenden Sicherheitsmaßnahmen. Die einzelnen Maßnahmen (M) sind wie auch im IT-Grundschutz in sechs Kategorien unterteilt:

- M1: Infrastruktur
- M2: Organisation
- M3: Personal
- M4: Hardware und Software
- M5: Kommunikation
- M6: Notfallvorsorge

Die Maßnahmen selbst sind in verschiedene Lebenszyklusphasen unterteilt:

- Planung und Konzeption
- Beschaffung
- Umsetzung
- Betrieb
- Aussonderung
- Notfallvorsorge

Aus Transparenzgründen hat ISIS12 die Kategorisierung aus den BSI IT-Grundschutzkatalogen übernommen.

Der ISIS12-Katalog wird jährlich im Turnus der Erscheinung der BSI Ergänzungslieferung des IT-Grundschutzkataloges aktualisiert und angepasst. So wird sichergestellt, dass alle neuen IT-Grundschutz-Bausteine ebenfalls im ISIS12 enthalten sind. Als weiteres Kriterium wird die vom BSI jährlich veröffentlichte „Zuordnungstabelle ISO/IEC 27001 und 27002 und IT-Grundschutz“ [28] herangezogen.

Nach dem Abgleich der vorhandenen Bausteine zwischen IT-Grundschutz (ITGS) und ISIS12 lässt sich folgendes Ergebnis festhalten:

- In S1 Universale Aspekte (ITGS: Übergreifende Aspekte) wurden Bausteine: B1.7 Kryptokonzept, B1.10 Standardsoftware, B1.13 Sensibilisierung und Schulung zur Informationssicherheit, B1.15 Löschen und Vernichten von Daten und B1.16 Anforderungsmanagement gekürzt. Der Baustein B1.12 Archivierung ist in S4 Anwendungen in B4.9 Archivierung zu finden. Die Bausteine B1.8 Behandlung von Sicherheitsvorfällen und B1.14 Patch- und Änderungsmanagement wurden als Grundlage für die im Schritt 5 beschriebenen drei grundlegenden ITSM-Prozesse - Wartung, Änderung und Störungsbeseitigung – herangezogen.
- In ISIS12 S2 Infrastruktur besteht B2.1 Gebäude aus den drei gekürzten ITGS-Bausteinen B2.1 Allgemeines Gebäude, B2.2 Elektrotechnische Verkabelung und B2.12 IT-Verkabelung. Die Bausteine B2.5 Datenträgerarchiv und B2.7 Schutzschränke wurden gestrichen. B2.9 Rechenzentrum soll bei erhöhtem Schutzbedarf zusätzlich zum B2.3 Serverraum verwendet werden.
- In S3 IT-Systeme und Netze wurde auf betriebssystemspezifische Besonderheiten verzichtet und somit kommen beim ISIS12 Vorgehensmodell nur allgemeine Server– und Client-Baustein für alle Client-Betriebssysteme zum Einsatz. Alle ITGS-Bausteine aus den Netzkomponenten und Schicht 4 Netze sind im ISIS12 zu finden. Lediglich einige von ihnen wurden aktualisiert, wie z.B. von PDA zum Smartphone.
- In Schicht 4 Anwendungen wurde auf spezifische ITGS-Bausteine, wie B5.2 Datenträgeraustausch, B5.3 Groupware, B5.5 Lotus Notes/ Domino, B5.9 Novell eDirectory, B5.13 SAP System, B5.16 Active Directory, B5.17 Samba, B5.18 DNS Server, B5.20 OpenLDAP verzichtet. Dazu wurde der Baustein Cloud Nutzung (B4.7) erstellt. ITGS B5.8 Telearbeit ist im ISISI12-Baustein B 2.5 Häuslicher/Mobiler Arbeitsplatz enthalten. Der ITGS Baustein B5.22 Protokollierung, der erst seit der letzte Ergänzungslieferung (13. EL Stand 2013) Bestandteil beim IT-Grundschutz ist, wurde nicht übernommen, weil in den Einzelbausteinen Protokollierung bereits vorhanden ist (z.B. B1.7: M2.64 Kontrolle der Protokolldateien, B3.1: M5.9 Protokollierung am Server, B3.4: M4.47 Protokollierung der Sicherheitsgateway-Aktivitäten etc.). ITGS Baustein B5.21 Webanwendungen wurde etwas angepasst und in ISIS12 B4.8 Nutzung von Webanwendungen umbenannt.

Aus dieser Auflistung ist ersichtlich, dass die meisten IT-Grundschutz Bausteine in den ISIS12-Katalog übernommen wurden. Lediglich einige der Maßnahmen wurden gekürzt. Da die ISIS12 Vorgehensweise flexibel und skalierbar designt wurde, können neue Bausteine, falls nötig, jederzeit ergänzt und/oder erstellt werden.

Um die Arbeit mit dem ISIS12-Katalog zu erleichtern, kann ein ISIS12-Tool verwendet werden. Die notwendige Modellierung, d.h. die Zuordnung von Bausteinen, mit den darin enthaltenen Maßnahmen, geschieht beim Eintrag der Anwendungen und den damit verbunden IT-Zielobjekten (IT-Systeme, Netze, Räume und Gebäude) automatisch. Es werden die betreffenden Bausteine aus den Schichten 2-4 den entsprechenden Objekten im definierten Informationsverbund zugeordnet. Die Bausteine aus der Schicht 1 (Universale Aspekte) werden, wie im Kapitel 8 des ISIS12 Vorgehensmodells beschrieben, notwendigerweise komplett dem Informationsverbund zugeordnet. Die entsprechenden Maßnahmen werden somit im ISIS12-Tool zur weiteren Verarbeitung bereitgestellt.

## 5.4 ISIS12 als Vorstufe zu BSI IT-Grundschutz bzw. ISO27001

ISIS12 nutzt das vom Bundesamt für Sicherheit in der Informationstechnik entwickelte und anerkannte IT-Grundschutzverfahren, ist jedoch so verändert worden, dass es in der Zielgruppe kleine und mittlere Unternehmen (KMU) mit relativ geringem Aufwand (zeitlich und monetär) eingeführt werden kann. ISIS12 ist durch die konkreten 12 Schritte gegenüber dem BSI IT-Grundschutzverfahren stärker geführt. Bei ISIS12 werden dem Anwender konkrete Sicherheitsmaßnahmen zur Abdeckung der Grundgefährdungen an die Hand gegeben.

Da ISIS12 speziell mit der Möglichkeit der Skalierbarkeit entwickelt wurde, könnte das nach ISIS12 implementierte und etablierte ISMS nach dem Durchlauf weiterer erforderlichen Schritte und entsprechender Dokumentation ausgebaut werden und eine weiterführende Zertifizierung wie „ISO 27001 auf Basis von IT-Grundschutz“ bzw. „ISO/IEC 27001 nativ“ erreicht werden. Im Fall einer späteren Einführung der erwähnten Standards sind durch ISIS12 bereits essentielle Schritte eingeführt worden. Zum Beispiel wurden bereits Leitlinien für Informationssicherheit und IT-Dokumentation erstellt sowie kritische Systeme identifiziert und die entsprechenden Maßnahmen eingeführt. Den erforderlichen Aufwand für eine weiterführende Zertifizierung kann ein ISIS12-Berater nach entsprechender Beratung ermitteln, weil es je nach angestrebten Zertifizierung und Art der Organisation unterschiedlich ist und im Detail differenziert bewertet werden müsste. [14]

### 5.4.1 Von ISIS12 zur „ISO 27001 auf Basis von IT-Grundschutz“ Zertifizierung

Da sich die Architektur des ISIS12 Vorgehensmodells in den Schritten 1 und 6-12 sehr stark an der BSI IT-Grundschutzmethodik orientiert hat, ist nach erfolgter ISIS12-Zertifizierung der Weg zur Zertifizierung nach „ISO 27001 auf Basis von IT-Grundschutz“ zwar noch lang, aber in Sachen Methodik vertraut und somit abschätzbar. Folgende Arbeitsschritte müssten im Wesentlichen noch durchgeführt werden:

- Es sind noch weitere Maßnahmen aus den BSI IT-Grundschutzkatalogen umzusetzen, die im ISIS12-Katalog nicht enthalten sind.
- Es sind noch zusätzliche Bausteine der BSI IT-Grundschutzkataloge bei der Modellierung zu berücksichtigen. Speziell Bausteine in der Schicht 1 (Übergreifende Aspekte) und der Schicht 3 (IT-Systeme) fallen hier an. Die Liste der fehlenden Bausteine kann dem Kapitel 5.3 entnommen werden.

- Es ist noch eine ergänzende Sicherheitsanalyse mit einer eventuell daraus abgeleiteten Risikoanalyse nach dem BSI-Standard 100-3 „Risikoanalyse auf der Basis von IT-Grundschutz“ [12] durchzuführen.
- Aus dem BSI Zertifizierungsschema [20] ergeben sich noch weitere Dokumente (Referenzdokumente) die noch erstellt werden müssen.

Folgende Dokumente sind dem Auditor und der Zertifizierungsstelle vom Antragsteller für die „ISO 27001 auf Basis von IT-Grundschutz“ Zertifizierung als Arbeitsgrundlage zur Verfügung zu stellen [29]:

1. Richtlinien für Informationssicherheit (A.0)
2. Strukturanalyse (A.1)
3. Schutzbedarfsfeststellung (A.2)
4. Modellierung des Informationsverbunds (A.3)
5. Ergebnis des Basis-Sicherheitschecks (A.4)
6. Ergänzende Sicherheitsanalyse (A.5)
7. Risikoanalyse (A.6)
8. Risikobehandlungsplan (A.7)

Diese Referenzdokumente bilden die Grundlage für die Auditierung nach IT-Grundschutz. Vor allem die Dokumente A5, A6, A7 müssten im Vergleich zu ISIS12 neu erstellt werden. Die Richtlinien für Informationssicherheit, u.a. Unternehmensleitlinie für Informationssicherheit (R.1), Bereinigter Netzplan (R.5) für die Strukturanalyse, Schutzbedarfsfeststellung (R.6) sowie andere Dokumente werden im Rahmen des ISIS12 erstellt und können so für die „ISO 27001 auf Basis von IT-Grundschutz“ Zertifizierung genutzt werden.

### 5.4.2 Von ISIS12 zur ISO/IEC 27001 Zertifizierung

Für die weiterführende Zertifizierung ISO/IEC 27001 müssten im Wesentlichen noch folgende Arbeitsschritte durchgeführt werden:

- Es ist eine Risikoanalyse (Risikoeinschätzung, Analyse, Bewertung und Messung der Risiken) durchzuführen, deren Ergebnisse die Grundlage der Sicherheitskonzeption sind.
- Umsetzung der daraus abgeleiteten Sicherheitsmaßnehmen in Verbindung mit den anzuwendenden Maßnahmenzielen aus ISO 27001 Annex A (A.5 - A.18). Viele dieser Sicherheitsmaßnahmen werden bereits im Rahmen der ISIS12 ISMS Einführung umgesetzt.
- Eine „Erklärung zur Anwendbarkeit“ (statement of applicability) ist zu erstellen.
- Ein Prozess zur kontinuierlichen Messung der Effizienz des ISMS ist zu etablieren.
- Die permanente Weiterentwicklung und Anpassung des ISMS gilt es dokumentiert zu betreiben.

Für die ISO/IEC 27001 Zertifizierung werden die folgenden Dokumente benötigt [9]:

1. Anwendungsbereich des ISMS (ISMS scope) – wird bereits im ISIS12 R.2 Beschreibung des Geltungsbereichs dokumentiert
2. Informationssicherheitsrichtlinie (Information security policy) – entspricht R.1 Unternehmensleitlinie für Informationssicherheit

3. Beschreibung des Prozesses zur Risikoeinschätzung (Information security risk assessment process)
4. Beschreibung des Risikobehandlungsprozesses (Information security risk treatment process)
5. Informationssicherheitsziele (Information security objectives) – werden in der R.1 Unternehmensleitlinie für Informationssicherheit beschrieben
6. Kompetenznachweise (Evidence of the competence of the people working in information security)
7. Sonstige ISMS bezogene Dokumente, die für notwendig erachtet werden (Other ISMS-related documents deemed necessary by the organization)
8. Operative Planungs- und Steuerungsdokumentation, z.B. Verfahren und Maßnahmen, die das ISMS unterstützen (Operational planning and control documents)
9. Ergebnisse der Risikoeinschätzung (The results of the risk assessments)
10. Risikobehandlungspläne (The decisions regarding risk treatment)
11. Ergebnisse der Leistungsbewertung des ISMS (Evidence of the monitoring and measurement of information security)
12. Auditergebnisse/ Ergebnisse eines internen Audits (The ISMS internal audit program and the results of audits conducted)
13. Management-Review-Berichte (Evidence of top management reviews of the ISMS)
14. Feststellungen von Nichtkonformitäten zu ISMS-Vorgaben (Evidence of nonconformities identified and corrective actions arising)
15. Dokumente im Rahmen der Maßnahmenumsetzung. Weitere Dokumente werden im Anhang A erwähnt, aber nicht genau spezifiziert. So sind einige der Kontrollen aus Anhang A zu dokumentieren, wie z.B. Bestandsaufnahme der Vermögenswerte/ Assets (A.7.1.1), Regeln für akzeptable Verwendung von Vermögenswerten/ Assets (A.7.1.3), Aufgaben und Zuständigkeiten der Mitarbeiter, Lieferanten und Drittparteien (A.8.1.1), Bedingungen der Beschäftigung (A.8.1.3), Betriebsverfahren, Engineering Prinzipien für ein sicheres System, Incident-Response-Verfahren, sowie die damit verbundenen Compliance-Verfahren und Informationssicherheit-Kontinuitätsverfahren (A.10.1.1), Zugriffs- und Zugangskontrollen (A.11.1.1), Identifikation der geltenden Rechtsvorschriften, relevanten Gesetze, Vorschriften und vertraglichen Verpflichtungen, Vertraulichkeits- und Geheimhaltungsvereinbarungen (A.15.1.1) [9]

Der Ablauf einer Konformitätsprüfung bezüglich der Norm ISO/IEC 27001 ist nicht willkürlich bestimmbar, da unter anderem die Norm ISO/IEC 27006 die Rahmenbedingungen dafür liefert. Nach dem Abstimmen des ISMS-Geltungsbereichs und Schließen des Vertrags führen Auditoren das Dokumentenreview durch und danach findet ein Vor-Ort-Audit statt. Die ISO 27001-Norm spezifiziert die Form der Dokumentation jedoch nicht genau [30].

## 5.5 ISO/IEC 27001 nativ, BSI IT-Grundschutz und ISIS12 gegenübergestellt

In der nachfolgenden Tabelle werden die drei Ansätze zur Einführung eines ISMS nach dem internationalen Standard ISO/IEC 27000-Familie, dem nationalen Standard nach BSI IT-Grundschutz und dem vom Netzwerk des Bayerischen IT-Sicherheitscluster e.V. für die Zielgruppe KMU entwickelten ISIS12 Verfahren hinsichtlich wesentlicher Kriterien gegenübergestellt.

Tabelle 1: Gegenüberstellung ISO/IEC 27001, BSI IT-Grundschutz und ISIS12 (in Anlehnung an [30])

| | ISO/IEC 27001:2013 | BSI IT-Grundschutz (auf Basis ISO/IEC 27001) | ISIS12 |
|---|---|---|---|
| Verfügbarkeit und Kosten | Normen 27001/27002 auch in Deutsch verfügbar (über Beuth-Verlag, DIN ISO/IEC 27001:2014-02 – ca. 100 Euro und ISO/IEC 27002:2013-10 – ca. 180 Euro) | Normen, Kataloge und vollständiges Zertifizierungsschema in deutscher Sprache und kostenfrei im Internet verfügbar | Standard (ISIS12-Handbuch) und ISIS12-Katalog sind Public Domain Dokumente, die gegen eine Schutzgebühr (ca. 150.- € netto) erhältlich sind. Das Zertifizierungsschema ist frei verfügbar. Alle Dokumente in deutscher Sprache. |
| Umfang der Norm | 27001: etwa 32 Seiten, ca. 10 Seiten netto;<br><br>27002: 114 generische Maßnahmen/ Kontrollen in 14 Kontrollgruppen auf ca. 90 Seiten | Standards 100-1 bis 100-3: mit ca. 160 Seiten;<br><br>IT-Grundschutzkataloge: ca. 4.400 Seiten mit ca. 79 Bausteinen, 483 Gefährdungen und ca. 1.200 Maßnahmen | ISIS12-Handbuch mit 96 Seiten und ISIS12-Katalog mit 75 Seiten |
| Auditoren | Auditoren müssen von einer akkreditierten Zertifizierungsstelle berufen sein. | Ca. 250 lizenzierte Auditoren, Liste veröffentlicht durch BSI | Ca. 11 lizenzierte Auditoren |
| Anzahl der derzeit zertifizierten Institutionen | Ca. 20.000 Zertifikate weltweit gemäß ISO Bericht 2012, ca. 488 registrierte Zertifizierungen in Deutschland [31] | Rund 50 Zertifikate veröffentlicht beim BSI | 10 laufende ISIS12-Projekte, bis Ende 2014 – 2-3 Zertifizierungen |
| Bedeutung International | International uneingeschränkt anerkannt | Hoher Bekanntheitsgrad im deutschsprachigen Raum, insbesondere Public Sector | Im KMU-Umfeld steigt der Bekanntheitsgrad, sonst eher unbekannt |
| Zertifizierungsstellen | Zehn akkreditierte Zertifizierungsstellen, diese sind frei wählbar | BSI als einzige Zertifizierungsstelle | DQS GmbH |

| | | | |
|---|---|---|---|
| Grad der technischen Detaillierung | Schreibt keine technischen Umsetzungsdetails vor; Maßnahmenziele und Maßnahmen gelten nicht mehr (seit Version 2013) verpflichtend; risikoorientierter Ansatz | Technisch sehr detailliert, konkret und umfangreich | Konkrete Handlungsempfehlungen, stark geführt, basiert auf der IT-Grundschutz-Vorgehensweise und -Katalogen |
| Zertifizierungsaufwand | Zertifizierungsaufwand wird nach ISO 27006 kalkuliert und ist vorrangig abhängig von der Mitarbeiteranzahl des Geltungsbereich (Scopes), beginnt bei 5 PT für Erst-Audit (+-30% für konkrete Faktoren wie Komplexität, Standorte, etc.) | Zertifizierungsaufwand mindestens 15 PT unabhängig vom Geltungsbereich (Größe des IT-Verbundes) ohne Mängelbehandlung und Rückfragen durch Zertifizierungsstelle, praktische Erfahrungen und Einschätzungen durch BSI selbst: Zertifizierungsaufwand von 14 bis 30 PT | Erst-Zertifizierungs-Audit dauert i.d.R. 2 PT und Überwachungs-Audit - 1 PT |
| Verbindung mit Risikomanagement | Freie Wahl einer angemessenen Risikomethodik (vgl. z.B. ISO 27005), Hauptfokus auf die Risiken | Sollte mit der Risikoanalyse 100-3 des BSI einhergehen, aber andere Risikoanalysen sind ebenfalls zulässig. | Nur immanente Risikoanalyse, bei einem höheren Schutzbedarf wird eine Risikoanalyse nach BSI-Standard 100-3 oder Ähnlichem empfohlen. |
| Werkzeuge zur Unterstützung | Tools mit sehr differenzierter Qualität und deutlich unterschiedlichen Kosten auf dem Markt verfügbar, die Auswahl gestaltet sich demzufolge schwieriger. Anwendung und Zertifizierung auch ohne Tools möglich. | Mehrere (auch kostenfreie) Tools am Markt verfügbar. Das BSI hat ein eigenes Tool (GSTOOL). Tooleinsatz wird dringend empfohlen. | ISIS12-Softwaretool und kommerzielles Tool (ibi Systems) stehen zur Verfügung. Tooleinsatz wird empfohlen, aber Anwendung und Zertifizierung auch ohne ISIS12-Tool möglich, wenn auch sehr aufwendig. |

| | | | |
|---|---|---|---|
| Voraussetzungen für Zertifizierung | Das ISMS sollte mindestens bereits 6 Monate betrieben werden, um die gelebten Prozesse und Lebenszyklen bis hin zum Verbesserungsprozess nachweisen zu können. Der Anwendungsbereich (Scope) darf sich in dieser Zeit nicht wesentlich ändern. | Das ISMS sollte mindestens bereits 6 Monate betrieben werden, um die gelebten Prozesse und Lebenszyklen bis hin zum Verbesserungsprozess nachweisen zu können. In dieser Zeit sollte der IT-Verbund relativ stabil sein, da sich ansonsten die Dokumentationen von IT-Strukturanalyse, Schutzbedarfsanalyse, Basissicherheits-Check etc. ändern und nachdokumentiert bzw. vollständig auch nachgearbeitet werden müssen. | Die 12 Schritte des ISMS müssen einmal komplett durchlaufen und wirksam umgesetzt worden sein. Der Anwendungsbereich (Scope) sollte relativ stabil gehalten werden. Die Realisierung des PDCA-Ansatzes muss erkennbar sein. |
| Kombination mit anderen Zertifikaten | Zertifizierung ist kombinierbar, z.B. mit ISO 9001 (im Kombi-Audit ca. 30% weniger Aufwand) | Die Kombination mit einer anderen Zertifizierung ist beim BSI nicht möglich. | Kombinierbar mit ISO 9000 (Qualitäts-management), ISO 14000 (Umwelt-management) und ISO 20000 (IT-Service-Management) |

# 6 Fazit/ Schlussfolgerungen

In diesem Gutachten wurde untersucht, ob das ISIS12 Vorgehensmodell zur Einführung des Informationssicherheitsmanagementsystems für die öffentliche Verwaltung geeignet ist. Darüber hinaus wurde bewertet, ob ISIS12 als eine Vorstufe für eine eventuell später noch vorzunehmende Zertifizierung nach IT-Grundschutz bzw. ISO/IEC 27001 dienen kann.

Die Bewertung erfolgte in drei Schritten: Im ersten Schritt wurde untersucht, ob die Vorgaben des IT-Planungsrats an ein ISMS, die in „Leitlinie für die Informationssicherheit in der öffentlichen Verwaltung“ festgeschrieben sind, durch die ISIS12 erfüllt werden. Hier lässt sich als ein Teilergebnis festhalten: Die Mindestanforderungen werden durch das ISIS12 Vorgehensmodell erfüllt.

Im zweiten Schritt wurden die Unterschiede zwischen den Vorgehensweisen des ISO 27001 bzw. IT-Grundschutz und ISIS12 analysiert. Im Gegensatz zu den etablierten Standards werden bei ISIS12 am Anfang des Projektes bereits Leitlinien für Informationssicherheit sowie Regeln für die IT-Dokumentation eingeführt. ISIS12 verfügt über eine festvorgeschriebene und sequentielle Vorgehensweise mit einem Top-Down Ansatz. Die ersten zwei Phasen – Initialisierung sowie Festlegung der Aufbau- und Ablauforganisation – sind sehr wichtig für eine erfolgreiche Einführung des ISMS. Erst nachdem diese Basis umgesetzt ist, können die operativen Arbeiten im Schritt 6 mit Konzeption und Implementierung der integrierten Sicherheitskonzeption beginnen. Die verbindliche Durchführung dieser ersten fünf Schritte stellt einen Unterschied zu den anderen Vorgehensweisen, wie ISO 27001 und IT-Grundschutz, dar. Die Verkopplung des Informationssicherheits-managements mit dem IT-Service-Management erlaubt die Nutzung von Synergien und ist eine empfehlenswerte Vorgehensweise, weil Sicherheitsprozesse ein unverzichtbarer Bestandteil eines ordnungsgemäßen IT-Betriebs sind.

Darüber hinaus wurde der ISIS12-Katalog analysiert, um zu identifizieren, welche IT-Grundschutz-Bausteine im ISIS12 Katalog gekürzt wurden, weil sie z.B. für KMUs keine Relevanz haben, aber für die öffentliche Verwaltung ggf. von Bedeutung sind. Es wurde nicht jede einzelne Sicherheitsmaßnahme geprüft, ob sie im Katalog vorhanden ist oder nicht, sondern es wurde viel mehr auf der Ebene der Bausteine identifiziert, welche von ihnen ggf. fehlen, oder geprüft, ob die Informationen anderswo eingeflossen sind. Beispielsweise wurden die Grundschutz-Bausteine „Behandlung von Sicherheitsvorfällen“ und „Patch- und Änderungsmanagement“ als Grundlage für die im ISIS12 Schritt 5 beschriebenen drei grundlegenden ITSM-Prozesse - Wartung, Änderung und Störungsbeseitigung – herangezogen.

Als Ergebnis für diese erste Bewertung lässt sich festhalten: die ISIS12 Vorgehensweise orientiert sich sehr stark an der BSI-Grundschutzmethodik und enthält die relevanten Sicherheitsmaßnahmen für den geringeren bis normalen Schutzbedarf.

Im letzten Schritt wurde geprüft, welche zusätzlichen Schritte und Unterlagen notwendig sind, um von einer ISIS12 Zertifizierung zu einer ISO 27001 Zertifizierung nativ bzw. ISO 27001 auf Basis von IT-Grundschutz zu gelangen. Da in ISIS12 nur eine indirekte Risikoanalyse durchgeführt wird, muss diese im Rahmen von ISO 27001 vorangestellt bzw. bei der IT-Grundschutz-Vorgehensweise nachgelagert erfolgen und dokumentiert werden. Da für die ISIS12 Zertifizierung nur sieben Referenzdokumente vorgesehen sind, müssen für die weiterführenden Zertifizierungen noch einige mehr erstellt werden. Es werden jedoch die essentiellen Schritte im Rahmen des ISIS12 eingeführt und die spätere Einführung von ISO 27001 oder IT-Grundschutz wird dadurch erleichtert.

Für eine definierte „Standardbehörde“ mit ca. 500 Mitarbeitern, möglichst homogener IT-Basisinfrastruktur, keinen über öffentliche Netze ungeschützt angebundenen Außenstellen, überwiegend normalem Schutzbedarf, keinen Hochverfügbarkeitsanforderungen an IT-Systeme und keinen kritischen Anwendungen (im Sinne keine kritischen Infrastrukturen) lässt sich schlussfolgern, dass ISIS12 eine geeignete Vorgehensweise darstellt. Vor allem erlaubt dieses Modell Skalierbarkeit, Einführung von grundlegenden IT-Service-Management-Prozessen sowie durch konkrete Handlungsempfehlungen und eine stringente Struktur mit Kontrollfragen eine leichtere Umsetzbarkeit bei kleineren und mittleren Behörden.

# Literaturverzeichnis


[1] „Landtag Nordrhein-Westfalen – Stellungnahme 16/1358 – Whistleblowing und PRISM - Anhörung A09," 6 Februar 2014. [Online]. Available: http://www.landtag.nrw.de/portal/WWW/dokumentenarchiv/Dokument/MMST16-1358.pdf. [Zugriff am 22 September 2014].

[2] „Bayerisches IT-Sicherheitscluster," 10 Juni 2013. [Online]. Available: http://www.it-sicherheit-bayern.de/itsecurity/115153-630-isis12_traegt_zur_verbreitung_von_it_sicherheitsmanagement_systemen_in_kmu_bei,1,0.html. [Zugriff am 22 September 2014].

[3] IT-Planungsrat, „Leitlinie für die Informationssicherheit in der öffentlichen Verwaltung – Hauptdokument," Kooperationsgruppe „Informationssicherheit des IT-PLR", 19.02.2013, Version 1.8.

[4] M. Stemmer und G. Goldacker, Standardisierung für die Öffentliche IT, 1. Auflage Hrsg., Berlin: Kompetenzzentrum Öffentliche Informationstechnologie, Fraunhofer FOKUS, 2014.

[5] BSI, „IT-Grundschutz-Kataloge," Bundesamt für Sicherheit in der Informationstechnik (BSI), 2013. [Online]. Available: https://gsb.download.bva.bund.de/BSI/ITGSK/IT-Grundschutz-Kataloge_2013_EL13_DE.pdf. [Zugriff am 22 September 2014].

[6] DIN, DIN ISO/IEC 27001:2014-02 – Informationstechnik - IT-Sicherheitsverfahren - Informationssicherheits-Managementsysteme - Anforderungen, DIN Deutsches Institut für Normung e.V., 2014.

[7] BSI, BSI-Standard 100-1: Managementsysteme für Informationssicherheit (ISMS), Bonn: Bundesamt für Sicherheit in der Informationstechnik, 2008.

[8] K.-R. Müller, IT-Sicherheit mit System, 4. Auflage Hrsg., Vieweg+Teubner, Hrsg., 2011.

[9] ISO, „ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements," 2013. [Online]. Available: http://www.iso27001security.com/html/27001.html.

[10] DIN, DIN ISO/IEC 27002:2014-02 – Informationstechnik - IT-Sicherheitsverfahren - Leitfaden für das Informationssicherheits-Management, DIN Deutsches Institut für Normung e.V., 2014.

[11] BSI, BSI-Standard 100-2: IT-Grundschutz-Vorgehensweise, Bonn: Bundesamt für Sicherheit in der Informationstechnik, 2008.

[12] BSI, „BSI-Standard 100-3: Risikoanalyse auf der Basis von IT-Grundschutz," 2008. [Online]. Available: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/ITGrundschutzstandards/standard_1003_pdf.pdf?__blob=publicationFile.

[13] BSI, „BSI-Standard 100-4: Notfallmanagement," 2008. [Online]. Available: http://www.bsi.bund.de/cae/servlet/contentblob/471456/publicationFile/30746/standard_1004.pdf.

[14] Handbuch zur effizienten Gestaltung von Informationssicherheit im Mittelstand, Regensburg: Bayerischer IT-Sicherheitscluster e.V., August 2014.

[15] ISIS12 - Katalog, Regensburg: Bayerischer IT-Sicherheitscluster e.V., August 2014.

[16] S. Wiesbeck, „ISIS 12: Management der Informationssicherheit für den Mittelstand," 07 11 2011. [Online]. Available: http://www.zdnet.de/41557734/isis-12-management-der-informationssicherheit-fuer-den-mittelstand/. [Zugriff am 22 September 2014].

[17] „Bayerisches IT-Sicherheitscluster," [Online]. Available: http://www.it-sicherheit-bayern.de und http://www.isis12.de. [Zugriff am 22 September 2014].

[18] Zertifizierungs- und Auditierungsschema nach ISIS12, Regensburg: Bayerischer IT-Sicherheitscluster e.V., Dezember 2012.

[19] BSI, „Auditierungsschema, Zertifizierung nach ISO 27001 auf der Basis von IT-Grundschutz," Bundesamt für Sicherheit in der Informationstechnik (BSI), Bonn, 2011.

[20] BSI, „Zertifizierungsschema für ISO 27001-Zertifizierung auf der Basis von IT-Grundschutz," Bundesamt für Sicherheit in der Informationstechnik (BSI), Bonn, 2014.

[21] Gesetz zur Förderung der elektronischen Verwaltung (E-Government-Gesetz - EGovG), Bundesanzeiger, 25.07.2013.

[22] „Kommunale Selbstverwaltung," Bayerisches Staatsministerium des Innern, für Bau und Verkehr, [Online]. Available: http://www.stmi.bayern.de/suk/kommunen/komselbstverwaltung/index.php. [Zugriff am 22 September 2014].

[23] BSI, „ Arbeitshilfe zur Feststellung des Aufwandes und zur Planung des personellen Ressourceneinsatzes für IT-Sicherheitsteams in der öffentlichen Verwaltung," Dezember 2012.

[24] „Bundesakedemiefür öffentliche Verwaltung (BAköV): Jahrestagung 2013 für IT-Sicherheitsbeauftragte," [Online]. Available: http://www.bakoev.bund.de/DE/02_Wir_ueber_uns/25_Organisation/06_Lehrgruppe5/jahrestagung_it_sibe.html. [Zugriff am 22 September 2014].

[25] K. Friedrich, „Zertifikate für IT-Sicherheitsbeauftragte in der öffentlichen Verwaltung," [Online]. Available: http://www.bakoev.bund.de/SharedDocs/Downloads/LG_5/Beitrag_Friedrich_zu_SiBoeV.pdf?__blob=publicationFile.

[26] BSI, Gefährdungskatalog Elementare Gefährdungen, Bonn: Bundesamt für Sicherheit in der Informationstechnik (BSI), 2011.

[27] BSI, „Goldene Regeln," [Online]. Available: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Download/GoldeneRegeln.pdf?__

blob=publicationFile. [Zugriff am 23 September 2014].

[28] BSI, „Zuordnungstabelle ISO/IEC 27001 und 27002 und IT-Grundschutz," [Online]. Available: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Hilfsmittel/Doku/Vergleich_ISO27001_GS.pdf?__blob=publicationFile. [Zugriff am 23 September 2014].

[29] BSI, „Hinweise zur Bereitstellung der Referenzdokumente im Rahmen der Zertifizierung nach ISO 27001 auf der Basis von IT-Grundschutz," Bundesamt für Sicherheit in der Informationstechnik, Bonn, 2011.

[30] BITKOM, „Leitfaden Zertifizierung von Informationssicherheit in Unternehmen – ein Überblick," 2011. [Online]. Available: http://www.bitkom.org/files/documents/Leitfaden_ZISU_2011_final.pdf.

[31] ISO, „ISO survey 2012," 2012. [Online]. Available: http://www.iso.org/iso/home/standards/certification/iso-survey.htm?certificate=ISO/IEC%2027001&countrycode=DE#countrypick.