ISMS: Sicherheitsmanagement

ISMS.1: Sicherheitsmanagement

1 Beschreibung

1.1 Einleitung

Mit (Informations-)Sicherheitsmanagement wird die Planungs-, Lenkungs- und Kontrollaufgabe bezeichnet, die erforderlich ist, um einen durchdachten und wirksamen Prozess zur Herstellung von Informationssicherheit aufzubauen und kontinuierlich umzusetzen. Ein funktionierendes Sicherheitsmanagement muss in die existierenden Managementstrukturen jeder Institution eingebettet werden. Daher ist es praktisch nicht möglich, eine für jede Institution unmittelbar anwendbare Organisationsstruktur für das Sicherheitsmanagement anzugeben. Vielmehr werden häufig Anpassungen an spezifische Gegebenheiten erforderlich sein.

1.2 Zielsetzung

Ziel dieses Bausteins ist es aufzuzeigen, wie ein funktionierendes Managementsystem für Informationssicherheit (ISMS) eingerichtet und im laufenden Betrieb weiterentwickelt werden kann. Der Baustein beschreibt dazu Schritte eines systematischen Sicherheitsprozesses und gibt Anleitungen zur Erstellung eines Sicherheitskonzeptes.

1.3 Abgrenzung und Modellierung

Der Baustein ISMS.1 *Sicherheitsmanagement* ist auf den Informationsverbund einmal anzuwenden.

Der Baustein baut auf den BSI-Standards 200-1 „Managementsysteme für Informationssicherheit“ und 200-2 „IT-Grundschutz-Methodik“ auf. Er fasst daraus die wichtigsten Aspekte zum Sicherheitsmanagement zusammen.

In der Institution sollten regelmäßig Sicherheitsrevisionen durchgeführt werden. Ausführliche Anforderungen dazu sind nicht in diesem Baustein, sondern im Baustein DER 3.1 *Audits und Revisionen* zu finden. Außerdem sollten alle Mitarbeiter der Institution, sowie sonstige relevante Personen wie extern Beschäftigte oder Projektmitarbeiter, systematisch und zielgruppengerecht zu Sicherheitsrisiken sensibilisiert und zu Fragen der Informationssicherheit geschult werden. Ausführliche Anforderungen dazu sind im Baustein ORP.3 *Sensibilisierung und Schulung zur Informationssicherheit* zu finden.

Dieser Baustein behandelt ebenso keine spezifischen Aspekte zu Personal oder zum Bereich Organisation. Diese Anforderungen werden in den Bausteinen ORP.2 *Personal* bzw. ORP.1 *Organisation* behandelt.

2 Gefährdungslage

Folgende spezifische Bedrohungen und Schwachstellen sind für den Baustein ISMS.1 *Sicherheitsmanagement* von besonderer Bedeutung.

2.1 Fehlende persönliche Verantwortung im Sicherheitsprozess

Sind in einer Institution die Rollen und Zuständigkeiten im Sicherheitsprozess nicht eindeutig festgelegt, dann ist es wahrscheinlich, dass viele Mitarbeiter ihre Verantwortung für die Informationssicherheit mit dem Verweis auf übergeordnete Hierarchie-Ebenen ablehnen oder vergessen. Als Folge werden Sicherheitsmaßnahmen nicht umgesetzt, da diese zunächst fast immer einen Mehraufwand im gewohnten Arbeitsablauf darstellen.

2.2 Mangelnde Unterstützung durch die Institutionsleitung

Werden die Sicherheitsverantwortlichen nicht uneingeschränkt durch die Institutionsleitung unterstützt, kann es schwierig werden, die notwendigen Maßnahmen einzufordern. Dies gilt insbesondere für Personen, die in der Linienstruktur über den Sicherheitsverantwortlichen stehen. In diesem Fall ist der Sicherheitsprozess nicht vollständig durchführbar.

2.3 Unzureichende strategische und konzeptionelle Vorgaben

In vielen Institutionen wird zwar ein Sicherheitskonzept erstellt, dessen Inhalt ist dann aber häufig nur wenigen Eingeweihten bekannt. Dies führt dazu, dass Vorgaben an Stellen, an denen organisatorischer Aufwand zu betreiben wäre, bewusst oder unbewusst nicht eingehalten werden.

Auch wenn das Sicherheitskonzept strategische Zielsetzungen enthält, werden diese von der Institutionsleitung vielfach als bloße Sammlung von Absichtserklärungen betrachtet. Häufig werden dann keine ausreichenden Ressourcen zur Umsetzung zur Verfügung gestellt. Oft wird fälschlicherweise auch davon ausgegangen, dass in einer automatisierten Umgebung Sicherheit automatisch hergestellt wird.

Ohne strategische Vorgaben wird bei Schadensfällen häufig unstrukturiert vorgegangen. Dadurch können bestenfalls Teilaspekte verbessert werden.

2.4 Unzureichende oder fehlgeleitete Investitionen

Wenn die Institutionsleitung nicht ausreichend über den Sicherheitszustand sämtlicher Geschäftsprozesse, IT-Systeme und Anwendungen sowie über vorhandene Mängel unterrichtet ist, werden nicht genügend Ressourcen für den Sicherheitsprozess bereitgestellt oder diese nicht sachgerecht eingesetzt. In letzterem Fall kann dies dazu führen, dass einem übertrieben hohen Sicherheitsniveau in einem Teilbereich schwerwiegende Mängel in einem anderen gegenüberstehen.

Häufig ist auch zu beobachten, dass teure technische Sicherheitslösungen falsch eingesetzt werden und somit unwirksam sind oder sogar selbst zur Gefahrenquelle werden.

2.5 Unzureichende Durchsetzbarkeit von Sicherheitsmaßnahmen

Um ein durchgehendes und angemessenes Sicherheitsniveau zu erreichen, müssen unterschiedliche Zuständigkeitsbereiche innerhalb einer Institution miteinander kooperieren. Fehlende strategische Leitaussagen und unklare Zielsetzungen führen mitunter aber zu unterschiedlichen Interpretationen der Bedeutung von Informationssicherheit. Dies kann zur Folge haben, dass die notwendige Kooperation nicht zustande kommt, etwa weil die Aufgabe „Informationssicherheit“ als unnötig angesehen wird oder zumindest keine Priorität hat. Somit könnten Sicherheitsmaßnahmen nicht umgesetzt werden.

2.6 Fehlende Aktualisierung im Sicherheitsprozess

Neue Geschäftsprozesse, Anwendungen und IT-Systeme sowie neue Bedrohungen beeinflussen permanent den Status der Informationssicherheit innerhalb einer Institution. Fehlt ein effektives Revisionskonzept, das auch das Bewusstsein für neue Bedrohungen stärkt, verringert sich das Sicherheitsniveau. Aus der realen Sicherheit wird dann schleichend eine gefährliche Scheinsicherheit.

2.7 Verstoß gegen gesetzliche Regelungen und vertragliche Vereinbarungen

Wenn Informationen, Geschäftsprozesse und IT-Systeme einer Institution unzureichend abgesichert sind, beispielsweise durch ein unzureichendes Sicherheitsmanagement, kann gegen Rechtsvorschriften mit Bezug zur Informationsverarbeitung oder gegen bestehende Verträge mit Geschäftspartnern verstoßen werden. Welche Gesetze jeweils zu beachten sind, hängt von der Art der Institution beziehungsweise ihrer Geschäftsprozesse und Dienstleistungen ab.

Je nachdem, wo sich die Standorte einer Institution befinden, können auch verschiedene nationale und internationale Vorschriften zu beachten sein. Verfügt eine Institution über unzureichende Kenntnisse hinsichtlich internationaler Gesetzesvorgaben, z. B. zu Datenschutz, Informationspflicht, Insolvenzrecht, Haftung oder Informationszugriff für Dritte, erhöht dies das Risiko entsprechender Verstöße. Dann drohen rechtliche Konsequenzen.

In vielen Branchen ist es üblich, dass Anwender ihre Zulieferer und Dienstleister dazu verpflichten, bestimmte Qualitäts- und Sicherheitsstandards einzuhalten. Verstößt ein Vertragspartner gegen vertraglich geregelte Sicherheitsanforderungen, kann dies Vertragsstrafen, Vertragsauflösungen oder sogar den Verlust von Geschäftsbeziehungen nach sich ziehen.

2.8 Störung der Geschäftsabläufe aufgrund von Sicherheitsvorfällen

Sicherheitsvorfälle können durch ein einzelnes Ereignis oder eine Verkettung unglücklicher Umstände ausgelöst werden. Sie können dazu führen, dass die Vertraulichkeit, Integrität oder Verfügbarkeit von Informationen und IT-Systemen beeinträchtigt werden. Dies wirkt sich dann schnell negativ auf wesentliche Fachaufgaben und Geschäftsprozesse der betroffenen Institution aus. Auch wenn nicht alle Sicherheitsvorfälle in der Öffentlichkeit bekannt werden, können sie trotzdem zu negativen Auswirkungen in den Beziehungen zu Geschäftspartnern und Kunden führen. Auch könnten gesetzliche Vorgaben missachtet werden. Dabei ist es nicht so, dass die schwersten und weitreichendsten Sicherheitsvorfälle durch die größten Sicherheitsschwachstellen ausgelöst wurden. In vielen Fällen führt die Verkettung kleiner Ursachen zu großen Schäden.

2.9 Unwirtschaftlicher Umgang mit Ressourcen durch unzureichendes Sicherheitsmanagement

Ein unzureichendes Sicherheitsmanagement kann dazu führen, dass falsche Prioritäten gesetzt werden und nicht an denjenigen Stellen investiert wird, die den größten Mehrwert für die Institution bringen. Dies kann zu folgenden Fehlern führen:

- Es wird in teure Sicherheitslösungen investiert, ohne dass eine Basis an notwendigen organisatorischen Regelungen vorhanden ist. Nicht geklärte Zuständigkeiten und Verantwortlichkeiten können trotz teurer Investitionen zu schweren Sicherheitsvorfällen führen.
- Es wird in den Bereichen einer Institution in Informationssicherheit investiert, die für Informationssicherheit besonders sensibilisiert sind. Andere Bereiche, die vielleicht für die Erfüllung der Fachaufgaben und die Erreichung der Geschäftsziele wichtiger sind, werden aufgrund von knappen Mitteln oder Desinteresse der Verantwortlichen vernachlässigt. Es wird dann unausgewogen in Teilbereiche investiert, während für das Gesamtsystem besonders bedeutsame Sicherheitsrisiken unbeachtet bleiben.
- Durch die einseitige Erhöhung des Schutzes einzelner Grundwerte kann sich der Gesamtschutz sogar verringern, beispielsweise indem eine Verschlüsselung von Informationen die

Vertraulichkeit zwar erhöht, aber die Verfügbarkeit verringern kann.

- Ein inhomogener und unkoordinierter Einsatz von Sicherheitsprodukten kann zu hohem finanziellen und personellen Ressourceneinsatz führen.

3 Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins ISMS.1 *Sicherheitsmanagement* aufgeführt. Grundsätzlich ist der Informationssicherheitsbeauftragte (ISB) für die Erfüllung der Anforderungen zuständig. Der Informationssicherheitsbeauftragte (ISB) ist bei strategischen Entscheidungen stets einzubeziehen. Außerdem ist der ISB dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Zusätzlich kann es noch andere Rollen geben, die weitere Zuständigkeiten bei der Erfüllung von Anforderungen haben. Diese sind dann jeweils explizit in eckigen Klammern in der Überschrift der jeweiligen Anforderungen aufgeführt.

Zuständigkeiten	**Rollen**
Grundsätzlich zuständig	Informationssicherheitsbeauftragter (ISB)
Weitere Zuständigkeiten	Vorgesetzte, Institutionsleitung

3.1 Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für den Baustein ISMS.1 *Sicherheitsmanagement* vorrangig erfüllt werden:

ISMS.1.A1 Übernahme der Gesamtverantwortung für Informationssicherheit durch die Leitung [Institutionsleitung] (B)

Die Institutionsleitung MUSS die Gesamtverantwortung für Informationssicherheit in der Institution übernehmen. Dies MUSS für alle Beteiligten deutlich erkennbar sein. Die Institutionsleitung MUSS den Sicherheitsprozess initiieren, steuern und kontrollieren. Die Institutionsleitung MUSS Informationssicherheit vorleben.

Die Institutionsleitung MUSS die Zuständigkeiten für Informationssicherheit festlegen. Die zuständigen Mitarbeiter MÜSSEN mit den erforderlichen Kompetenzen und Ressourcen ausgestattet werden.

Die Institutionsleitung MUSS sich regelmäßig über den Status der Informationssicherheit informieren lassen. Insbesondere MUSS sich die Institutionsleitung über mögliche Risiken und Konsequenzen aufgrund fehlender Sicherheitsmaßnahmen informieren lassen.

ISMS.1.A2 Festlegung der Sicherheitsziele und -strategie [Institutionsleitung] (B)

Die Institutionsleitung MUSS den Sicherheitsprozess initiieren und etablieren. Dafür MUSS die Institutionsleitung angemessene Sicherheitsziele sowie eine Strategie für Informationssicherheit festlegen und dokumentieren. Es MÜSSEN konzeptionelle Vorgaben erarbeitet und organisatorische Rahmenbedingungen geschaffen werden, um den ordnungsgemäßen und sicheren Umgang mit Informationen innerhalb aller Geschäftsprozesse des Unternehmens oder Fachaufgaben der Behörde zu ermöglichen.

Die Institutionsleitung MUSS die Sicherheitsstrategie und die Sicherheitsziele tragen und verantworten. Die Institutionsleitung MUSS die Sicherheitsziele und die Sicherheitsstrategie regelmäßig dahingehend überprüfen, ob sie noch aktuell und angemessen sind und wirksam umgesetzt werden können.

ISMS.1.A3 Erstellung einer Leitlinie zur Informationssicherheit [Institutionsleitung] (B)

Die Institutionsleitung MUSS eine übergeordnete Leitlinie zur Informationssicherheit verabschieden. Diese MUSS den Stellenwert der Informationssicherheit, die Sicherheitsziele, die wichtigsten Aspekte der Sicherheitsstrategie sowie die Organisationsstruktur für Informationssicherheit beschreiben. Für die Sicherheitsleitlinie MUSS ein klarer Geltungsbereich festgelegt sein. In der Leitlinie zur Informationssicherheit MÜSSEN die Sicherheitsziele und der Bezug der Sicherheitsziele zu den Geschäftszielen und Aufgaben der Institution erläutert werden.

Die Institutionsleitung MUSS die Leitlinie zur Informationssicherheit allen Mitarbeitern und sonstigen Mitgliedern der Institution bekannt geben. Die Leitlinie zur Informationssicherheit SOLLTE regelmäßig aktualisiert werden.

ISMS.1.A4 Benennung eines Informationssicherheitsbeauftragten [Institutionsleitung] (B)

Die Institutionsleitung MUSS einen Informationssicherheitsbeauftragten (ISB) benennen. Der ISB MUSS die Informationssicherheit in der Institution fördern und den Sicherheitsprozess mitsteuern und koordinieren.

Die Institutionsleitung MUSS den ISB mit angemessenen Ressourcen ausstatten. Die Institutionsleitung MUSS dem ISB die Möglichkeit einräumen, bei Bedarf direkt an sie selbst zu berichten.

Der ISB MUSS bei allen größeren Projekten sowie bei der Einführung neuer Anwendungen und IT-Systeme frühzeitig beteiligt werden.

ISMS.1.A5 Vertragsgestaltung bei Bestellung eines externen Informationssicherheitsbeauftragten [Institutionsleitung] (B)

Die Institutionsleitung MUSS einen externen Informationssicherheitsbeauftragten (ISB) bestellen, wenn die Rolle des ISB nicht durch einen internen Mitarbeiter besetzt werden kann. Der Vertrag mit einem externen ISB MUSS alle Aufgaben des ISB sowie seine damit verbundenen Rechte und Pflichten umfassen. Der Vertrag MUSS eine geeignete Vertraulichkeitsvereinbarung umfassen. Der Vertrag MUSS eine kontrollierte Beendigung des Vertragsverhältnisses, einschließlich der Übergabe der Aufgaben an den Auftraggeber, gewährleisten.

ISMS.1.A6 Aufbau einer geeigneten Organisationsstruktur für Informationssicherheit [Institutionsleitung] (B)

Eine geeignete übergreifende Organisationsstruktur für Informationssicherheit MUSS vorhanden sein. Dafür MÜSSEN Rollen definiert sein, die konkrete Aufgaben übernehmen, um die Sicherheitsziele zu erreichen. Außerdem MÜSSEN qualifizierte Personen benannt werden, denen ausreichend Ressourcen zur Verfügung stehen, um diese Rollen zu übernehmen. Die Aufgaben, Rollen, Verantwortungen und Kompetenzen im Sicherheitsmanagement MÜSSEN nachvollziehbar definiert und zugewiesen sein. Für alle wichtigen Funktionen der Organisation für Informationssicherheit MUSS es wirksame Vertretungsregelungen geben.

Kommunikationswege MÜSSEN geplant, beschrieben, eingerichtet und bekannt gemacht werden. Es MUSS für alle Aufgaben und Rollen festgelegt sein, wer wen informiert und wer bei welchen Aktionen in welchem Umfang informiert werden muss.

Es MUSS regelmäßig geprüft werden, ob die Organisationsstruktur für Informationssicherheit noch angemessen ist oder ob sie an neue Rahmenbedingungen angepasst werden muss.

ISMS.1.A7 Festlegung von Sicherheitsmaßnahmen (B)

Im Rahmen des Sicherheitsprozesses MÜSSEN für die gesamte Informationsverarbeitung ausführliche und angemessene Sicherheitsmaßnahmen festgelegt werden. Alle Sicherheitsmaßnahmen SOLLTEN systematisch in Sicherheitskonzepten dokumentiert werden. Die Sicherheitsmaßnahmen SOLLTEN

regelmäßig aktualisiert werden.

ISMS.1.A8 Integration der Mitarbeiter in den Sicherheitsprozess [Vorgesetzte] (B)

Alle Mitarbeiter MÜSSEN in den Sicherheitsprozess integriert sein. Hierfür MÜSSEN sie über Hintergründe und die für sie relevanten Gefährdungen informiert sein. Sie MÜSSEN Sicherheitsmaßnahmen kennen und umsetzen, die ihren Arbeitsplatz betreffen.

Alle Mitarbeiter MÜSSEN in die Lage versetzt werden, Sicherheit aktiv mitzugestalten. Daher SOLLTEN die Mitarbeiter frühzeitig beteiligt werden, wenn Sicherheitsmaßnahmen zu planen oder organisatorische Regelungen zu gestalten sind.

Bei der Einführung von Sicherheitsrichtlinien und Sicherheitswerkzeugen MÜSSEN die Mitarbeiter ausreichend informiert sein, wie diese anzuwenden sind.

Die Mitarbeiter MÜSSEN darüber aufgeklärt werden, welche Konsequenzen eine Verletzung der Sicherheitsvorgaben haben kann.

ISMS.1.A9 Integration der Informationssicherheit in organisationsweite Abläufe und Prozesse [Institutionsleitung] (B)

Informationssicherheit MUSS in alle Geschäftsprozesse sowie Fachaufgaben integriert werden. Es MUSS dabei gewährleistet sein, dass nicht nur bei neuen Prozessen und Projekten, sondern auch bei laufenden Aktivitäten alle erforderlichen Sicherheitsaspekte berücksichtigt werden. Der Informationssicherheitsbeauftragte MUSS an sicherheitsrelevanten Entscheidungen ausreichend beteiligt werden.

Informationssicherheit SOLLTE außerdem mit anderen Bereichen in der Institution, die sich mit Sicherheit und Risikomanagement beschäftigen, abgestimmt werden.

3.2 Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für den Baustein ISMS.1 *Sicherheitsmanagement*. Sie SOLLTEN grundsätzlich erfüllt werden.

ISMS.1.A10 Erstellung eines Sicherheitskonzepts (S)

Für den festgelegten Geltungsbereich (Informationsverbund) SOLLTE ein angemessenes Sicherheitskonzept als das zentrale Dokument im Sicherheitsprozess erstellt werden. Es SOLLTE entschieden werden, ob das Sicherheitskonzept aus einem oder aus mehreren Teilkonzepten bestehen soll, die sukzessive erstellt werden, um zunächst in ausgewählten Bereichen das erforderliche Sicherheitsniveau herzustellen.

Im Sicherheitskonzept MÜSSEN aus den Sicherheitszielen der Institution, dem identifizierten Schutzbedarf und der Risikobewertung konkrete Sicherheitsmaßnahmen passend zum betrachteten Informationsverbund abgeleitet werden. Sicherheitsprozess und Sicherheitskonzept MÜSSEN die individuell geltenden Vorschriften und Regelungen berücksichtigen.

Die im Sicherheitskonzept vorgesehenen Maßnahmen MÜSSEN zeitnah in die Praxis umgesetzt werden. Dies MUSS geplant und die Umsetzung MUSS kontrolliert werden.

ISMS.1.A11 Aufrechterhaltung der Informationssicherheit (S)

Der Sicherheitsprozess, die Sicherheitskonzepte, die Leitlinie zur Informationssicherheit und die Organisationsstruktur für Informationssicherheit SOLLTEN regelmäßig auf Wirksamkeit und Angemessenheit überprüft und aktualisiert werden. Dazu SOLLTEN regelmäßig Vollständigkeits- bzw. Aktualisierungsprüfungen des Sicherheitskonzeptes durchgeführt werden.

Ebenso SOLLTEN regelmäßig Sicherheitsrevisionen durchgeführt werden. Dazu SOLLTE geregelt sein, welche Bereiche und Sicherheitsmaßnahmen wann und von wem zu überprüfen sind. Überprüfungen des Sicherheitsniveaus SOLLTEN regelmäßig (mindestens jährlich) sowie anlassbezogen durchgeführt werden.

Die Prüfungen SOLLTEN von qualifizierten und unabhängigen Personen durchgeführt werden. Die Ergebnisse der Überprüfungen SOLLTEN nachvollziehbar dokumentiert sein. Darauf aufbauend SOLLTEN Mängel beseitigt und Korrekturmaßnahmen ergriffen werden.

ISMS.1.A12 Management-Berichte zur Informationssicherheit [Institutionsleitung] (S)

Die Institutionsleitung SOLLTE sich regelmäßig über den Stand der Informationssicherheit informieren, insbesondere über die aktuelle Gefährdungslage sowie die Wirksamkeit und Effizienz des Sicherheitsprozesses. Dazu SOLLTEN Management-Berichte geschrieben werden, welche die wesentlichen relevanten Informationen über den Sicherheitsprozess enthalten, insbesondere über Probleme, Erfolge und Verbesserungsmöglichkeiten. Die Management-Berichte SOLLTEN klar priorisierte Maßnahmenvorschläge enthalten. Die Maßnahmenvorschläge SOLLTEN mit realistischen Abschätzungen zum erwarteten Umsetzungsaufwand versehen sein. Die Management-Berichte SOLLTEN revisionssicher archiviert werden.

Die Management-Entscheidungen über erforderliche Aktionen, den Umgang mit Restrisiken und mit Veränderungen von sicherheitsrelevanten Prozessen SOLLTEN dokumentiert sein. Die Management-Entscheidungen SOLLTEN revisionssicher archiviert werden.

ISMS.1.A13 Dokumentation des Sicherheitsprozesses (S)

Der Ablauf des Sicherheitsprozesses SOLLTE dokumentiert werden. Wichtige Entscheidungen und die Arbeitsergebnisse der einzelnen Phasen wie Sicherheitskonzept, Richtlinien oder Untersuchungsergebnisse von Sicherheitsvorfällen SOLLTEN ausreichend dokumentiert werden.

Es SOLLTE eine geregelte Vorgehensweise für die Erstellung und Archivierung von Dokumentationen im Rahmen des Sicherheitsprozesses geben. Regelungen SOLLTEN existieren, um die Aktualität und Vertraulichkeit der Dokumentationen zu wahren. Von den vorhandenen Dokumenten SOLLTE die jeweils aktuelle Version kurzfristig zugänglich sein. Außerdem SOLLTEN alle Vorgängerversionen zentral archiviert werden.

ISMS.1.A14 ENTFALLEN (S)

Diese Anforderung ist entfallen.

ISMS.1.A15 Wirtschaftlicher Einsatz von Ressourcen für Informationssicherheit (S)

Die Sicherheitsstrategie SOLLTE wirtschaftliche Aspekte berücksichtigen. Werden Sicherheitsmaßnahmen festgelegt, SOLLTEN die dafür erforderlichen Ressourcen beziffert werden. Die für Informationssicherheit eingeplanten Ressourcen SOLLTEN termingerecht bereitgestellt werden. Bei Arbeitsspitzen oder besonderen Aufgaben SOLLTEN zusätzliche interne Mitarbeiter eingesetzt oder externe Experten hinzugezogen werden.

3.3 Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für den Baustein ISMS.1 *Sicherheitsmanagement* exemplarische Vorschläge für Anforderungen aufgeführt, die über das dem Stand der Technik entsprechende Schutzniveau hinausgehen und BEI ERHÖHTEM SCHUTZBEDARF in Betracht gezogen werden SOLLTEN. Die konkrete Festlegung erfolgt im Rahmen einer Risikoanalyse.

ISMS.1.A16 Erstellung von zielgruppengerechten Sicherheitsrichtlinien (H)

Neben den allgemeinen SOLLTE es auch zielgruppenorientierte Sicherheitsrichtlinien geben, die jeweils bedarfsgerecht die relevanten Sicherheitsthemen abbilden.

ISMS.1.A17 Abschließen von Versicherungen (H)

Es SOLLTE geprüft werden, ob für Restrisiken Versicherungen abgeschlossen werden können. Es SOLLTE regelmäßig überprüft werden, ob die bestehenden Versicherungen der aktuellen Lage entsprechen.

4 Weiterführende Informationen

4.1 Wissenswertes

Der BSI-Standard 200-1 definiert allgemeine Anforderungen an ein Managementsystem für Informationssicherheit (ISMS). Er ist außerdem kompatibel zum ISO-Standard 27001 und berücksichtigt die Empfehlungen vieler anderer ISO-Standards.

Der BSI-Standard 200-2 bildet die Basis der bewährten BSI-Methodik zum Aufbau eines soliden Informationssicherheitsmanagements (ISMS). Er etabliert drei neue Vorgehensweisen bei der Umsetzung des IT-Grundschutzes. Aufgrund der ähnlichen Struktur der beiden Standards 200-1 und 200-2 können Anwender sich gut in beiden Dokumenten zurechtfinden.

Die ISO/IEC 27000 (Information security management systems – Overview and vocabulary) gibt einen Überblick über Managementsysteme für Informationssicherheit (ISMS) und über die Zusammenhänge der verschiedenen Normen der ISO/IEC 2700x-Familie. Hier finden sich außerdem die grundlegenden Begriffe und Definitionen für ISMS.

Die ISO/IEC 27001 (Information security management systems – Requirements) ist eine internationale Norm zum Management von Informationssicherheit, die auch eine Zertifizierung ermöglicht.

Die ISO/IEC 27002 (Code of practice for information security controls) unterstützt bei der Auswahl und Umsetzung von den in der ISO/IEC 27001 beschriebenen Maßnahmen, um ein funktionierendes Sicherheitsmanagement aufzubauen und in der Institution zu verankern.

5 Anlage: Kreuzreferenztabelle zu elementaren Gefährdungen

Die Kreuzreferenztabelle enthält die Zuordnung von elementaren Gefährdungen zu den Anforderungen. Anhand dieser Tabelle lässt sich ermitteln, welche elementaren Gefährdungen durch welche Anforderungen abgedeckt sind. Durch die Umsetzung der aus den Anforderungen abgeleiteten Sicherheitsmaßnahmen wird den entsprechenden elementaren Gefährdungen entgegengewirkt. Die Buchstaben in der zweiten Spalte (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit) zeigen an, welche Grundwerte der Informationssicherheit durch die Anforderung vorrangig geschützt werden. Die folgenden elementaren Gefährdungen sind für den Baustein ISMS.1 *Sicherheitsmanagement* von Bedeutung.

G 0.18 Fehlplanung oder fehlende Anpassung

G 0.27 Ressourcenmangel

G 0.29 Verstoß gegen Gesetze oder Regelungen