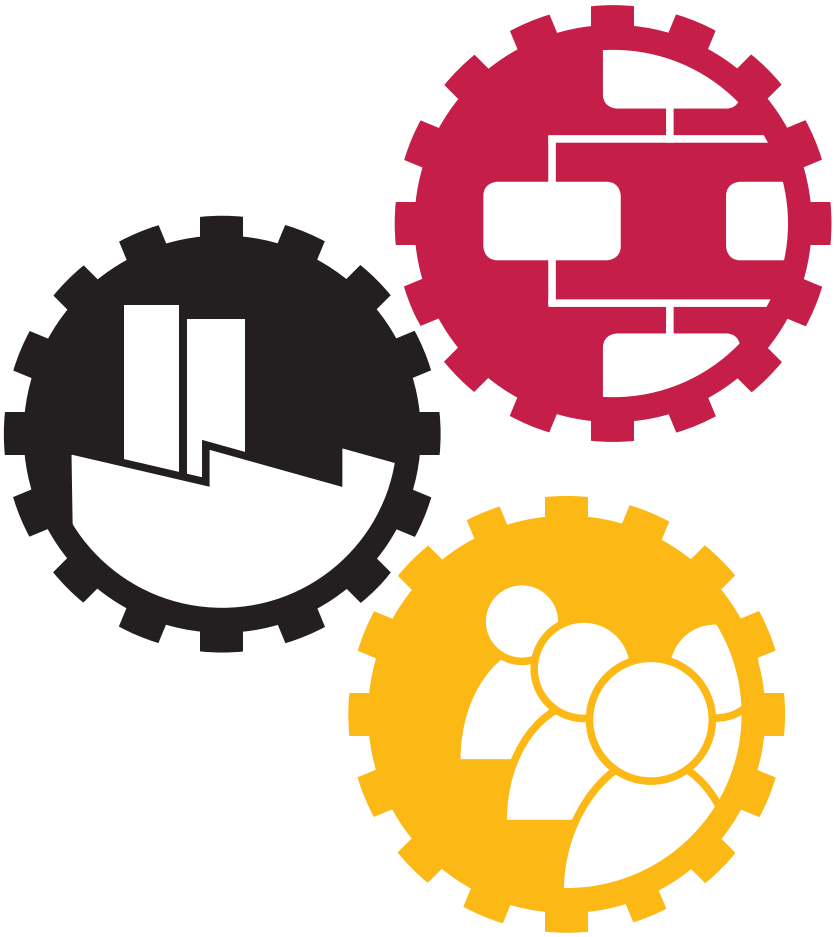
Bundesamt für Verfassungsschutz

Bundesamt für Sicherheit in der Informationstechnik

ASW Bundesverband

Wirtschaftsgrundschutz

Standard 2000-1



Inhaltsverzeichnis

1. Grundlagen des Wirtschaftsschutzes 2

1.1. Kontext des Wirtschaftsschutzes 2

1.2. Festlegungen im Sicherheitsmanagementsystem 3

1.3. Prävention und Reaktion 7

2. Das Sicherheitsmanagementsystem 8

2.1. Einleitung 8

2.2. Führungs-, Steuerungs- und Berichts-/Kontrollprozesse 10

2.3. Themenübergreifende Prozesse 12

2.4. Schulung und Sensibilisierung 12

3. Kontinuierliche Verbesserung 15

Anhang A Spezifische Ergänzungen 17

Anhang B Anwendung des Wirtschaftsgrundschutzes 18

B.1 Allgemeine Hinweise zur Anwendung 18

B.2 Bestimmung des Geltungsbereichs 20

B.3 Strukturvarianten aufgrund des rollenbasierten Ansatzes 21

B.4 Bestimmung der Themengebiete 23

B.5 Bestimmung der relevanten Bausteine 23

B.6 Bestimmung der relevanten Maßnahmenkategorie 24

Anhang C Glossar 26

Anhang D Verzeichnisse 27

D.1 Abbildungsverzeichnis 27

D.2 Tabellenverzeichnis 27

Anhang E Literaturverzeichnis 28

Anhang F Referenz zu ISO/IEC 27001 30

Danksagung 32

1 Grundlagen des Wirtschaftsschutzes

1.1. Kontext des Wirtschaftsschutzes

Technisches Wissen, Forschung und Entwicklung sind die Garanten dafür, dass deutsche Institutionen weltweit an der Spitze ihres jeweiligen Sektors mitspielen. Der **ganzheitliche Schutz der Werte** ist deshalb für diese Institutionen von kritischer Bedeutung. Nur ein **integriertes bzw. ganzheitliches Sicherheitsmanagementsystem** kann die Leitung der Institutionen angemessen in der Wahrnehmung ihrer **Verantwortung für einen sicheren Geschäftsbetrieb** und in ihrer **Fürsorgepflicht** unterstützen.

integriertes Sicherheitsmanagementsystem

Wesentlichen Einfluss auf die konkrete Ausprägung eines solchen Sicherheitsmanagementsystems haben **verschiedene Faktoren**. Diese **ergeben sich aus der Strategie der Institution, ihren Interessengruppen und ihrem individuellen sicherheitsrelevanten Umfeld**. Diese Faktoren analysiert die Institution und leitet die jeweils für sie relevanten Aspekte aus dieser Analyse ab. Mit den Erkenntnissen der Analyse stellt die Institution eine **Organisationsstruktur und Regelprozesse** bereit, mit denen sie ihre **individuellen Sicherheitsrisiken dauerhaft identifiziert, bewertet und behandelt**.

Einflussfaktoren

Das dem Wirtschaftsgrundschutz zugrunde liegende Sicherheitsmanagementsystem bündelt alle sicherheitsrelevanten Themengebiete. Es kann bei Bedarf um weitere Managementsysteme erweitert werden, die einzelne Themengebiete im Rahmen der in diesem Standard beschriebenen Anforderungen regeln. Der Umfang kann von

Bündelung sicherheitsrelevanter Themengebiete

Institution zu Institution unterschiedlich sein und umfasst **stets individuell** und in Abhängigkeit von der Implementierung in der Institution einzelne, spezifische Themengebiete. Im Wirtschaftsgrundschutz gilt dies bspw. für das **Reaktionsmanagement**, das i**n einem eigenen Standard beschrieben** ist (vgl. Standard 2000-3).

Umfang und Ausgestaltung des Sicherheitsmanagementsystems hängen unmittelbar davon ab, welche Themengebiete aufgrund der **individuellen Gefährdungen und der Risikoexposition** als bedeutungsvoll identifiziert wurden. Weiterhin ergeben sich hieraus auch die **organisatorischen Anforderungen**.

Aufgaben der Institutionsleitung

Die Leitung der Institution soll

- die **sicherheitsrelevanten Themengebiete**, die mit dem Sicherheitsmanagementsystem behandelt werden, **festlegen**
- ein **Sicherheitsmanagementsystem definieren und in Kraft setzen**
- **ausreichende Ressourcen** zur Umsetzung des Sicherheitsmanagementsystems mit den identifizierten Themengebieten **bereitstellen**

1.2. Festlegungen im Sicherheitsmanagementsystem

Verantwortung der Leitung

Die Leitung der Institution ist für die Sicherheit und den Schutz der Werte verantwortlich. Sie **delegiert die Umsetzung** der hierfür erforderlichen Maßnahmen **an die Verantwortlichen der jeweiligen Geschäftsbereiche**.

Die Leitung der Institution lässt sich vom **Sicherheitsverantwortlichen** regelmäßig über den aktuellen Stand des Reifegrads des Sicherheitsmanagementsystems und über die aktuelle Gefährdungslage berichten.

Die Werte einer Institution

Der Schutz der Werte einer Institution ist die zentrale Aufgabe der Sicherheitsorganisation im Rahmen des Wirtschaftsgrundschutzes. Für die **ganzheitliche Betrachtung** dieser steht der **Sicherheitsorganisation** ein **Sicherheitsmanagementsystem** zur Verfügung, das auf den **nachhaltigen Schutz und die kontinuierliche Verbesserung** der identifizierten Themen und Maßnahmen ausgerichtet ist.

Als **zentrale Werte einer Institution** kommen bspw. folgende infrage:

- **Gesundheit und Unversehrtheit** von Leib und Leben der Mitarbeiter, Besucher, Kunden und Geschäftspartner
- **materielle Werte**
  - Sachwerte
  - Vermögenswerte
  - Immobilien
- **immaterielle Werte**
  - Daten und Informationen
  - elementare Geschäftsabläufe (bspw. Entwicklung, Produktion, Vertrieb)
  - Wissen
  - Umwelt
  - Image und Reputation

Aufgaben der Institutionsleitung

Die **Leitung der Institution soll**

- die zu schützenden Werte **identifizieren** und **dokumentieren**

Die Sicherheitsstrategie

Die Institution definiert in einer Sicherheitsstrategie, welche Werte sie auf welche Art und auf welchem Niveau schützen möchte. Sie berücksichtigt hierbei ihre **individuelle Risikoexposition** ebenso wie ihre **allgemeine Institutionsstrategie**.

Die Sicherheitsorganisation leitet aus der Sicherheitsstrategie die **konkreten Sicherheitsziele** für die zu schützenden Werte ab. Sie sorgt dann mit **abgestimmten und angemessenen Sicherheitsmaßnahmen** dafür, dass dieses **einheitliche Sicherheitsniveau** realisiert wird.

Sie trägt damit nachhaltig zum **Investitionsschutz und** zur **Wertschöpfung** bei.

Die **Leitung der Institution soll**

- die **Sicherheitsstrategie** durch einen Verantwortlichen **erstellen** lassen
- die **Sicherheitsstrategie freigeben**

Aufgaben der Institutionsleitung

Die Sicherheitsleitlinie

Die Sicherheitsleitlinie definiert die strategische Ausrichtung des Sicherheitsmanagements. Sie ist **das interne Regelwerk der Institution** und entsteht nach dessen institutionsspezifischen Vorgaben.

Mindestens folgende Sachverhalte regelt die Institution in der Leitlinie:

- Sicherheitsziele
- Struktur der Sicherheitsorganisation
- Rollen
- Verantwortlichkeiten, Aufgaben und Kompetenzen
- Verpflichtung zur Einhaltung
- Vorgaben zu Prozessbeschreibungen und Regelwerken
- kontinuierliche Verbesserung
- Sicherheitsrisikomanagement
- Geltungsbereich

Inhalte einer Sicherheitsleitlinie

Die **Leitung der Institution soll**

- eine **Leitlinie zum Sicherheitsmanagement** durch einen Verantwortlichen **erstellen** lassen
- die **Leitlinie** zum Sicherheitsmanagement **verabschieden**

Aufgaben der Institutionsleitung

Die Sicherheitsorganisation

Die konkrete Ausgestaltung der Sicherheitsorganisation wird durch den individuellen Kontext der Institution (vgl. Kapitel 2.1) bestimmt. Der Kontext ergibt sich aus der **Strategie**, den **Interessengruppen** und der **Gefährdungslage** des sicherheitsrelevanten Umfelds. Er wird des Weiteren durch die relevanten Themenfelder mitbestimmt. Die

personelle Ausprägung und die **Führungsstruktur** der Sicherheitsorganisation sind damit immer **individuell abhängig vom institutionsspezifischen Kontext**.

Verantwortlichkeiten der Sicherheitsorganisation

Die Sicherheitsorganisation ist die zentral verantwortliche Instanz für die angemessene Umsetzung der Sicherheitsstrategie. Sie unterstützt andere Geschäftsbereiche bei der Erstellung und Einführung von Sicherheitskonzepten innerhalb deren Verantwortlichkeit.

Die Institution benennt einen Sicherheitsverantwortlichen. Der Sicherheitsverantwortliche ist mit der **Umsetzung der erforderlichen Maßnahmen** für Einführung und Betrieb eines Sicherheitsmanagementsystems in der Institution betraut. Der Sicherheitsverantwortliche **berichtet unabhängig** von seiner organisatorischen Einbindung direkt **an die Leitung der Institution**.

Aufgaben der Institutionsleitung

Die **Leitung der Institution soll**

- die **Definition einer Sicherheitsorganisation initiieren**
- einen **Sicherheitsverantwortlichen benennen**

Die Sicherheitskonzepte

Die Sicherheitsorganisation definiert grundsätzliche Anforderungen an Sicherheitskonzepte. Sie stellt damit sicher, dass die Sicherheitskonzepte der in den verschiedenen Geschäftsbereichen der Institution verantworteten Werte auf eine einheitliche Weise entstehen.

Die Sicherheitsorganisation initiiert Sicherheitskonzepte zum **ganzheitlichen Schutz der zuvor identifizierten schutzbedürftigen Werte.** Die **Entwicklung, Einführung und Optimierung** der einzelnen Sicherheitskonzepte **obliegt** den jeweils **verantwortlichen Geschäftsbereichen** der Institution. Der verantwortliche Geschäftsbereich ist hierbei in der Regel der jeweilige Eigentümer der betroffenen Ressourcen oder der identifizierten Risiken.

Die Sicherheitsorganisation **unterstützt** die Geschäftsbereiche **bei der Erstellung der Sicherheitskonzepte**. Sie übernimmt die **interne oder externe Koordinierung** der Abstimmung mit anderen Geschäftsberei-

chen innerhalb der Institution. Diese koordinierende Aufgabe ermöglicht es der Institution, das **angestrebte einheitliche Sicherheitsniveau** zu **erreichen**. Die **Geschäftsbereiche** hingegen sind selber **für** die **Umsetzung konkreter Maßnahmen** im operativen Management der Sicherheitsrisiken **verantwortlich**.

Die **Institution soll**

- für definierte Werte **geeignete Sicherheitskonzepte erstellen, abstimmen und pflegen**

Aufgabe der Institution

1.3. Prävention und Reaktion

Zur Erreichung des definierten Sicherheitsniveaus setzt die Institution individuelle präventive und damit risikoreduzierende Maßnahmen um. Trotz aller Umsicht und Vorplanung lassen sich Risiken allerdings nie vollständig vermeiden, so dass es **trotz präventiver Maßnahmen Sicherheitsvorfälle** geben kann.

Etablieren reaktiver Fähigkeiten

Die **Etablierung reaktiver Fähigkeiten** ermöglicht bei angemessener Umsetzung eine **schnelle und effiziente Behandlung des Sicherheitsvorfalls**. Die entstehende Beeinträchtigung der Werte bzw. der daraus entstehende **Schaden** kann damit **begrenzt** sowie eine **weitere Eskalation** in der Regel **vermieden** werden.

Als wichtige präventive Maßnahmen sind daher auch all die zu verstehen, die der Vorbereitung auf die Reaktion selber dienen. Der **Standard 2000-3** im Wirtschaftsgrundschutz **sowie** die **zugehörigen Bausteine (ÜA2 Sicherheitsvorfallmanagement, ÜA3 Notfallmanagement, ÜA4 Krisenmanagament) liefern** hierfür eine **weitergehende Orientierungshilfe**.

Standard 2000-3

2 Das Sicherheits-managementsystem

2.1. Einleitung

Die Sicherheitsorganisation betreibt ein Sicherheitsmanagement-system. Sie setzt damit das **anforderungsgerechte und einheitliche Sicherheitsniveau** im Rahmen der **Sicherheitsstrategie** um. Damit stellt sie auch sicher, dass das **Sicherheitsniveau kontinuierlich mit dem sich ständig verändernden Bedarf** aufgrund neuer oder sich ändernder Gefährdungen **abgeglichen** wird und **ggf. Anpassungen** erfolgen.

Die **wesentlichen Einflussfaktoren** im Sicherheitsmanagementsys-tem sind die **zu schützenden Werte** und die Sicherheitsstrategie sowie die hieraus abgeleiteten Themengebiete. Diese sind durch die Leitung der Institution definiert.

Die Sicherheitsorganisation definiert für das Sicherheitsmanagement-system ein **zyklisches Prozessmodell**. Das Sicherheitsmanagement-system ist damit **auf** eine **kontinuierliche Verbesserung ausgerichtet**. Abbildung 1 stellt beispielhaft das Prozessmodell dar.

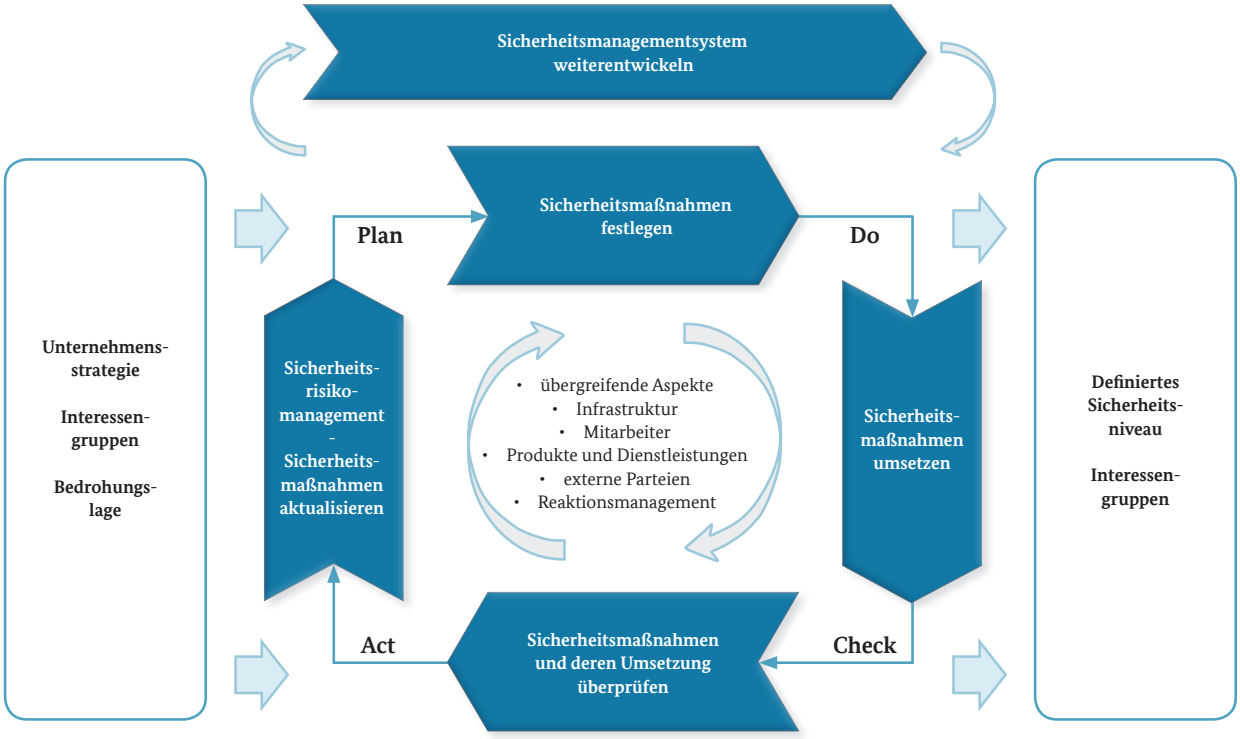


Abbildung 1: PDCA-Zyklus Sicherheitsmanagement

Die **Sicherheitsorganisation nutzt die in der Sicherheitsleitlinie dokumentierten Ziele und Aufgaben**, um ihre eigene strategische Ausrichtung innerhalb der Institution festzulegen.

Grundsätzlich nimmt die Sicherheitsorganisation die **Richtlinien-, Kontroll- und Berichtskompetenz** für die ihr zugeordneten sicherheitsrelevanten Themengebiete wahr.

Die **Geschäftsbereiche** der Institution haben aufgrund ihrer unmittelbaren Nähe zum Tagesgeschäft eine **wichtige Rolle bei der Identifikation und laufenden Überwachung der Sicherheitsrisiken**.

Aufgaben der Sicherheitsorganisation

Die **Sicherheitsorganisation unterstützt** die **Geschäftsbereiche**, indem sie

- die **strategische Steuerung** in sicherheitsrelevanten Fragen übernimmt
- die **Methoden zu allen Sicherheitsthemen zentral und einheitlich** vorgibt
- die Fachbereiche **methodisch** in der Anwendung **unterstützt und berät**

Information und Kommunikation

Die Sicherheitsorganisation **koordiniert die interne und externe Kommunikation** sicherheitsrelevanter Themen und **betreut** die **Kontakte** zu den Behörden und Organisationen mit Sicherheitsaufgaben[1].

Mitarbeiter und Externe nehmen großen Einfluss auf die Sicherheit in der Institution und den Schutz der Institutionswerte. Die Sicherheitsorganisation unterstützt die Mitarbeiter mit einer **aktiven Informations- und Aufklärungspolitik** über bestehende Gefährdungen und den Hintergrund notwendiger Sicherheitsmaßnahmen. **Entsprechend angepasste Informationen** stellt die Sicherheitsorganisation **auch für Externe, Besucher oder Gäste** zur Verfügung. Dies **erhöht die Aufmerksamkeit** und trägt **nachhaltig** zu einer **Vermeidung von Sicherheitsvorfällen** bei.

Die Sicherheitsorganisation erstellt hierfür **Sensibilisierungskampagnen** und führt diese **in regelmäßigen Abständen** durch. Ziel der Kampagnen ist es, Mitarbeiter und Externe bspw. **auf potentielle Sicherheitsrisiken aufmerksam** zu **machen** und sie für sicherheitsrelevante Themen zu **sensibilisieren**.

Aufgaben der Institution

Die **Institution soll**

- ein Sicherheitsmanagementsystem **definieren und freigeben**
- ein **Prozessmodell** gemäß den hier beschriebenen Anforderungen **festlegen**
- das Sicherheitsmanagementsystem so ausgestalten, dass ggf. nachrangige **Managementsysteme** (bspw. Reaktionsmanagement) **reibungsfrei integriert** sind

2.2. Führungs-, Steuerungs- und Berichts-/Kontrollprozesse

Das Sicherheitsmanagementsystem unterscheidet zwischen Führungs-, Steuerungs- und Berichts-/Kontrollprozessen. Diese werden in einem **institutionsspezifischen Regelwerk** beschrieben.

Mit den **Führungsprozessen** stellt die Sicherheitsorganisation die **Rahmenbedingungen für das Sicherheitsmanagementsystem** bereit. Mit den **Steuerungsprozessen** sorgt sie für die **Umsetzung in den einzelnen Themengebieten**. Mit den **Berichts- und Kontrollprozes-**

[1] siehe Glossar; bspw. Polizei, Feuerwehr, Rettungsdienst

sen stellt sie die permanente **Überwachung der Umsetzung** mittels geeigneter Kontrollen und das **Berichtswesen gegenüber der Leitung** der Institution **und den Interessengruppen** sicher.

Der **wesentliche Führungsprozess** des Sicherheitsmanagementsystems ist hierbei das **Sicherheitsrisikomanagement**. Die **Sicherheitsorganisation definiert** zentral die **Methodik und wesentliche Aspekte des Sicherheitsrisikomanagements**. Sie stimmt sich dabei auch mit anderen Geschäftsbereichen der Institution, bspw. einem operationellen Risikomanagement, ab.

Ziel der Führungsprozesse

Mit den Führungsprozessen sorgt die Sicherheitsorganisation für

- die Ausrichtung, also das **Erstellen einer** an den individuellen Kontext der Institution angepassten **Sicherheitsstrategie**
- das **Definieren geeigneter Prozesse**
- das **Erstellen von Regelwerken** (Richtlinien, Prozessbeschreibungen usw.)
- die **Einbindung der Leitung** der Institution
- das **Bereitstellen angemessener Ressourcen**, sowohl personell und technisch als auch monetär

Die **sicherheitsrelevanten Themengebiete**, die ggf. auch in einem nachrangigen Managementsystem beschrieben sind, **steuert die Sicherheitsorganisation mit den Steuerungsprozessen**. Die **grundsätzlichen Vorgaben des Sicherheitsmanagements, dokumentiert in der Leitlinie und der Sicherheitsstrategie**, werden so in die einzelnen Themengebiete transferiert. Damit stellt die Sicherheitsorganisation die prozessuale Grundlage für ein **angemessenes, durchgängiges und einheitliches Sicherheitsniveau in der gesamten Institution** bereit.

Die **Berichts- und Kontrollprozesse** definieren die **Überwachung der Umsetzung und** ggf. der daraus abgeleiteten **Verbesserungsmaßnahmen** sowie die **Einbindung der Leitung** der Institution **mittels des Berichtswesens**. Die Sicherheitsorganisation schafft hiermit die **Grundlage für** eine **kontinuierliche Weiterentwicklung** des gesamten Sicherheitsmanagementsystems.

Weitere Detaillierungen zum Sicherheitsmanagementsystem und zu den hierfür erforderlichen Regelungen und Maßnahmen sind **im Standard 2000-2 und** den einzelnen **nachrangigen Bausteinen** festgelegt.

nachgelagerte Detaillierungen

2.3. Themenübergreifende Prozesse

Sicherheit lässt sich nicht durch das Wirken einer einzelnen Einheit realisieren, sondern **bedarf** in der Regel immer des **Zusammenspiels diverser Funktionen und Geschäftsbereiche** einer Institution.

Um dies zu ermöglichen, definiert die Sicherheitsorganisation **themenübergreifende Prozesse**, die gemeinsam mit den Führungs- und Steuerungsprozessen eine **einheitliche Anwendung der Sicherheitsprozesse** in den anderen Geschäftsbereichen ermöglichen. Hierbei werden in der Regel auch Bereichsgrenzen überschritten. Die Sicherheitsorganisation definiert Vorgaben, aber die operative Anwendung vieler dieser Vorgaben erfolgt in anderen Geschäftsbereichen. Die **Sicherheitsorganisation übernimmt** für diese themenübergreifenden Prozesse eine **koordinierende Funktion** und unterstützt so die handelnden Geschäftsbereiche.

Im Wirtschaftsgrundschutz werden die nachfolgenden **themenübergreifenden Prozesse** betrachtet:

- Sicherheitsrisikomanagement
- Sicherheitsvorfallmanagement
- Berechtigungsmanagement
- Schulung und Sensibilisierung

themenübergreifende Prozesse

2.4. Schulung und Sensibilisierung

Einleitung

Dem **Faktor Mensch** misst der Wirtschaftsgrundschutz eine besonders hohe Bedeutung bei, da in der **alltäglichen Arbeit auf operativer Ebene** durch den einzelnen Menschen Maßnahmen umgesetzt oder angewendet werden.

Aber **nur qualifizierte und sensibilisierte Mitarbeiter gehen mit den Werten der Institution** aus Sicht des Wirtschaftsgrundschutzes **angemessen um**. Sie behandeln die Werte in der Regel auch nur dann ihrem Schutzbedarf entsprechend, wenn ihnen **Zusammenhänge und Gefährdungspotentiale bewusst und** sie für sie **nachvollziehbar** sind.

Ein angemessenes Sicherheitsniveau wird innerhalb einer Institution daher nur erfolgreich umgesetzt, wenn entsprechend **geschulte und sensibilisierte Mitarbeiter** dabei helfen, das **Thema Sicherheit auf allen Ebenen erfolgreich umzusetzen**. Der Bedarf an Schulung und Sensibilisierung richtet sich dabei an diversen Faktoren aus, bspw. Kontext, Sensibilität der Geschäftstätigkeit, gesetzliche Anforderungen.

Die Institution vermittelt **in Schulungen grundsätzliche und spezifische Aspekte des Sicherheitsmanagements** und verdeutlicht so bspw. die richtigen Vorgehensweisen. Für **Sensibilisierungsmaßnahmen** nutzt die Institution **aktuelle oder relevante Themen**, um allgemein zu informieren bzw. aufmerksam zu machen. Die Ausgestaltung und die verwendeten Methoden und Hilfsmittel bedürfen zudem einer individuellen Anpassung an die Kultur der jeweiligen Institution.

Aufgaben der Institution

Die **Institution soll**

- ein **Schulungs- und Sensibilisierungskonzept erstellen**
- **regelmäßig** Schulungen und Sensibilisierungs**kampagnen durchführen**
- die **kulturellen Aspekte und** bereits **vorhandene Ressourcen berücksichtigen**

Schulungskonzept

Die kontinuierliche Aus- und Weiterbildung der Mitarbeiter der Institution im Umgang mit Werten ist die Grundlage für das angestrebte einheitliche Sicherheitsniveau. Die Qualifizierung ihrer Mitarbeiter ist für die Institution daher von hoher Bedeutung. Die Institution erstellt ein **institutionsspezifisches Schulungskonzept** und **berücksichtigt** unter anderem **die nachfolgenden Aspekte**:

zu berücksichtigende Aspekte für ein institutionsspezifisches Schulungskonzept

- Es wird ein **einfaches und unkompliziertes Modell** gewählt

mit leicht anwendbaren qualitativen **Messparametern**.

- Das Konzept ist **auf eine längere Laufzeit**, bspw. drei bis fünf Jahre, **ausgelegt**.
- Das Konzept **berücksichtigt die unterschiedlichen Rollen und Funktionen** in der Institution.
- Das Konzept **berücksichtigt die individuellen Bedürfnisse** der verschiedenen Rollen in der Institution.
- Das Konzept **beinhaltet alle** für die Institution **identifizierten Themen und Bausteine**.

Die Sicherheitsorganisation handelt hierbei **in enger Zusammenarbeit mit weiteren relevanten internen Abteilungen**, bspw. Personalwesen und Betriebs-/Personalrat.

Sensibilisierungskonzept

Die **regelmäßige Sensibilisierung** der Mitarbeiter der Institution für bspw. aktuelle Gefährdungen beim Umgang mit den Werten **unterstützt** die **Maßnahmen eines Schulungskonzepts wirksam**. Das Ziel „qualifizierte Mitarbeiter" erreicht die Institution in der Regel nur durch die begleitenden Sensibilisierungsmaßnahmen im Zusammenspiel mit angemessenen Schulungen.

Die Institution erstellt hierfür ein **Sensibilisierungskonzept**, das nachfolgende **Aspekte berücksichtigt**:

- Es werden **institutionsspezifische Sachverhalte** im Umgang mit Gefährdungen oder Risiken vermittelt.
- Die Sachverhalte werden **leicht verständlich dargestellt** und verdeutlichen die damit verbundenen Sicherheitsrisiken der Institution.
- Auch **Konsequenzen** (sowohl arbeitsrechtlich als auch straf- oder zivilrechtlich) werden **transparent gemacht**.
- Die **Sensibilisierungsmaßnahmen sind mit** dem **Schulungskonzept abgestimmt und ergänzen** dieses.

Die Sicherheitsorganisation handelt hierbei **in enger Zusammenarbeit mit weiteren relevanten internen Abteilungen**, bspw. Personalwesen und Betriebs-/Personalrat.

zu berücksichtigende Aspekte für ein institutionsspezifisches Sensibilisierungskonzept

3 Kontinuierliche Verbesserung

Da weder die Gefährdungslage noch die Strategie oder die Geschäftsfelder der Institution dauerhaft gleich bleiben, verändert sich auch das beeinflussende Umfeld des Sicherheitsmanagementsystems ständig. Ein angemessenes Sicherheitsniveau für die identifizierten Werte beruht auf einem **permanenten Abgleich zwischen Gefährdungslage und den Anforderungen** an das Sicherheitsmanagementsystems.

Das gesamte Sicherheitsmanagementsystem und alle ggf. etablierten nachrangigen Managementsysteme müssen daher einer **kontinuierlichen Überprüfung der Wirksamkeit und Verbesserung** unterliegen. Das Prozessmodell des Sicherheitsmanagementsystems berücksichtigt dies mittels eines Regelkreises. Die Sicherheitsorganisation **analysiert** zudem die **relevanten Einflussfaktoren**, bspw.:

relevante Einflussfaktoren für das Sicherheitsmanagementsystem

- geänderte **rechtliche/vertragliche Auflagen oder Regulierungen**
- geänderte **Strategie** der Institution
- **Sicherheitsanalysen** und **Sicherheitsrisikomanagement**
- **Zusammenwirken** mit den Geschäftsbereichen
- **Überprüfung** und **Revision**
- **Sicherheitsvorfälle**

Die Sicherheitsorganisation leitet aus den Erkenntnissen der Analyse die **erforderlichen Änderungsbedarfe** ab. Die Änderungsbedarfe werden anschließend **in die jeweiligen Abläufe und Regelwerke überführt**.

Die Sicherheitsorganisation initiiert zudem die **Aufnahme der Änderungsbedarfe in bestehende Sicherheitskonzepte** der Geschäftsbereiche. Für den Fall, dass noch keine entsprechenden Sicherheitskonzepte bestehen, veranlasst sie die Erstellung in Zusammenarbeit mit den betreffenden Fachbereichen.

Aufgaben der Institution

Die **Institution soll**

- einen **kontinuierlichen Verbesserungsprozess** im Sicherheitsmanagementsystem vorsehen

Spezifische Ergänzungen

Anhang A

Standard 2000-2 Aufbau und Betrieb eines Sicherheitsmanagementsystems
Siehe das entsprechende Dokument in der jeweils aktuellen Version.

Standard 2000-3 Aufbau und Betrieb eines Reaktionsmanagementsystems
Siehe das entsprechende Dokument in der jeweils aktuellen Version.

Anwendung des Wirtschaftsgrundschutzes

Anhang B

B.1 Allgemeine Hinweise zur Anwendung

Der Wirtschaftsgrundschutz soll allen Institutionen als Leitfaden für den Aufbau eines angemessenen Sicherheitsmanagements sowie für die Implementierung der relevanten Bausteine dienen. Diese Zielsetzung besteht insbesondere auch dann, wenn Institutionen sich in Geschäftsfeld, Größe, Struktur, Risikoprofil oder sonstigen Aspekten stark unterscheiden.

Die Standardreihe des Wirtschaftsgrundschutzes greift diese große Herausforderung auf und wurde deshalb als ein **flexibel implementierbares Rahmenwerk** entwickelt. Der Institution eröffnen sich dadurch die erforderlichen Möglichkeiten, um auf die eigenen Rahmenbedingungen und individuellen Bedürfnisse an ein Sicherheitsmanagement einzugehen.

Auf die Umsetzungsmöglichkeiten wird in diesem Anhang grundsätzlich eingegangen. Die Entscheidung, wie und in welchem Umfang ein Sicherheitsmanagement zur Umsetzung des Wirtschaftsgrundschutzes eingeführt wird, hat die Leitung der Institution bzw. der von ihr Beauftragte zu treffen. **Wichtige Einflussfaktoren** sind dabei u. a. Marktposition, Risikoprofil, Exponiertheit, gesetzliche oder regulatorische Auflagen.

Individualisierungsoptionen

Der Institution stehen **diverse Individualisierungsoptionen** zur Verfügung, die in den folgenden Kapiteln ausführlicher dargestellt

werden:

1. Der **Geltungsbereich der** einzelnen **Themengebiete** innerhalb der Institution ermöglicht eine **dem Bedarf angemessene Ausrichtung** des Wirtschaftsgrundschutzes.
2. Der **rollenbasierte Ansatz** ermöglicht es der Institution, die eigene Sicherheitsorganisation **an die spezifischen Bedürfnisse anzupassen**. Durch das Zusammenführen oder Hierarchisieren von Rollen können kleinere wie größere Strukturen gleichermaßen abgebildet werden.
3. Die **Schwerpunktsetzung der** relevanten **Themengebiete** hat unmittelbaren Einfluss auf die Gestaltung und Struktur der Sicherheitsorganisation.
4. Die **Bestimmung der relevanten Bausteine** hat ebenso wie die Themengebiete einen unmittelbaren Einfluss auf die Gestaltung und Struktur der Sicherheitsorganisation.
5. Die **Bestimmung der relevanten Sicherheitsanforderungen** steuert unmittelbar den Aufwand für die **Gewährleistung des gewünschten Sicherheitsniveaus** und damit auch für die Einführung und den Betrieb. Der Wirtschaftsgrundschutz stellt hierbei **drei Maßnahmenkategorien** bereit, **in denen sich das Risikoprofil abbilden lässt** (von Maßnahmenkategorie A bei geringem bis Maßnahmenkategorie C bei hohem Gefährdungsprofil). Diese haben unmittelbare Auswirkung auf die Aufgaben der Sicherheitsorganisation.

Dieser Anhang dient dazu, der Leitung der Institution **Anhaltspunkte aufzuzeigen, wie sie** für ihre Institution **einen angemessenen Rahmen und Umfang des Wirtschaftsgrundschutzes festgelegen kann.** Dabei spielen neben der eigentlichen Gefährdungslage und Exposition natürlich auch **Aspekte des Risikoappetits** der Institution eine wichtige Rolle. Der Institution wird daher eine **grundsätzliche Vorgehensweise** nahegelegt.

Aufgaben der Institutionsleitung

Die **Leitung der Institution sollte**

- die **individuellen Anforderungen** an das Sicherheitsmanagement **definieren** (vgl. Kapitel 2.1)
- das **eigene Gefährdungsprofil** bzw. das vorhandene dem Sicherheitsmanagement **zugrunde legen**

- einen **Umsetzungsplan für die Einführung** des Sicherheitsmanagements auf Grundlage des Wirtschaftsgrundschutzes **erstellen**, **der wesentliche Rahmenbedingungen**, bspw. Organisationsstruktur, Ressourcen, Zeitachsen und zu erreichendes Sicherheitsniveau, **beschreibt**
- **ausreichende Ressourcen** für die Einführung und den Regelbetrieb **vorsehen**
- die **Einführung als Projekt** aufsetzen und anschließend **in den Regelbetrieb überführen**

Die hier aufgezeigten grundsätzlichen **Schritte** dienen **als Basis für** die erforderliche **individuelle Planung der Einführung** eines Sicherheitsmanagements **oder** für die **Umgestaltung** eines bestehenden.

B.2 Bestimmung des Geltungsbereichs

Bevor die relevanten Themengebiete und damit die Ausprägung der Sicherheitsorganisation identifiziert werden, wird **zuerst** der **Geltungsbereich** des Wirtschaftsgrundschutzes **festgelegt**. Beispielsweise kann es für Institutionen sinnvoll sein, Teile des Wirtschaftsgrundschutzes auf ausgewählte Standorte oder Geschäftsbereiche zu begrenzen. Im Ergebnis dokumentiert die Institution, welche Bereiche oder Standorte in welchem Umfang im Wirtschaftsgrundschutz betrachtet werden.

Faktoren zur Bestimmung des Anwendungsbereichs

Bei der **Bestimmung des Anwendungsbereichs** werden folgende Faktoren berücksichtigt:

- **Betrachtung aller Bereiche, Werte und Aspekte** einer Institution, die der **Unterstützung oder Durchführung der Geschäftstätigkeiten bzw. Aufgabenerfüllung dienen** und durch die Institution selbst verantwortet werden
- ist die Institution im Rahmen ihrer Geschäftstätigkeiten bzw. Aufgabenerfüllung auf externe Stellen oder Partner angewiesen (z. B. Outsourcing), sind die **Schnittstellen klar** zu **definieren**, damit diese durch den Wirtschaftsgrundschutz **angemessen berücksichtigt** werden können

B.3 Strukturvarianten aufgrund des rollenbasierten Ansatzes

Der **rollenbasierte Ansatz** der Sicherheitsorganisation **ermöglicht** eine **flexible Ausprägung unter Berücksichtigung der jeweils individuellen Randbedingungen** der Institution, bspw. Kultur oder Größe. Da Rollen personenungebunden sind, kann auf diese Weise die Sicherheitsorganisation in einem ersten Schritt grob anhand bspw. der relevanten Themengebiete definiert werden.

Aus den Aufgaben, für die die Sicherheitsorganisation zukünftig verantwortlich sein soll, leiten sich anschließend die **tatsächlichen personellen Ressourcenanforderungen** ab. Dies kann zu einer Aufteilung einer Rolle auf mehrere Personen oder zu einer Bündelung mehrerer Rollen in einer Person führen.

Beispiele für Institutionen unterschiedlicher Größe und Struktur

Der **Wirtschaftsgrundschutz lässt sich** damit grundsätzlich **auf Institutionen unterschiedlicher Größe und Struktur abbilden**. Dies wird anhand der zwei nachfolgenden Beispiele kurz erläutert.

Beispiel 1

Beispiel 1: Die **mittelständische Institution** A hat ihren **Hauptsitz und weitere Standorte in Deutschland**. Darüber hinaus ist sie **global tätig** und hat **mehrere internationale Standorte**. Die Institutionsstruktur erfordert unter anderem die Berücksichtigung verschiedener Rechtsräume, einen hohen Reisebedarf und Informationstransfer zwischen den Standorten und die Wahrung von Produkt- und Markenrechten. Mit dem Leitfaden des Wirtschaftsgrundschutzes etabliert Institution A eine zentralisierte Sicherheitsorganisation, die die Vorgaben und Regeln für die gesamte Institution definiert und weiterentwickelt. Die zentrale Stelle koordiniert hierbei andere Bereiche der Institution über definierte Schnittstellen und Ansprechpartner, die aus Sicht ihres Verantwortungsbereichs ihren Beitrag zum Sicherheitsmanagement leisten. Dies sind bspw. Personal und Gebäudemanagement sowie natürlich die Informationstechnik. Es wird hierbei möglichst auf vorhandene Ressourcen zurückgegriffen. An den Standorten definiert Institution A lokale Verantwortliche, die unter Koordination der zentralen Stelle lokale Maßnahmen umsetzen. Auf diese Weise entsteht eine zentral gesteuerte Sicherheitsorganisation (vergleichbar einer Matrixorganisation) mit wenig festen und geringen zusätzlichen

Ressourcen.

Beispiel 2: Die verhältnismäßig **kleinere mittelständische Institution** B beschäftigt **ca. 100 Mitarbeiter an einem Standort in Deutschland**. Sie ist Innovationsträger und ein hochspezialisierter Zulieferer für andere Institutionen. Die Institutionsstruktur erfordert eine sehr schlanke Sicherheitsorganisation, die dennoch die Anforderungen ggf. international operierender Auftraggeber angemessen berücksichtigt. Institution B nutzt den Leitfaden des Wirtschaftsgrundschutzes, um die relevanten Themengebiete zu identifizieren und zu priorisieren. Bspw. ist neben dem Schutz von Informationen insbesondere der Produktschutz von wesentlicher Bedeutung. Institution B bestimmt einen Sicherheitsverantwortlichen und etabliert ein Gremium, in dem die Führungskräfte der relevanten Fachbereiche regelmäßig zusammenkommen. In diesem Kreis werden die erforderlichen Sicherheitsmaßnahmen diskutiert und beschlossen. Auf diese Weise wird eine Sicherheitsorganisation geschaffen, die sehr stark auf den vorhandenen Personen basiert und mit sehr wenig zusätzlichem Ressourcenbedarf auskommen kann.

Beispiel 2

Die beiden Beispiele zeigen auf, dass mit dem Wirtschaftsgrundschutz sehr unterschiedliche Sicherheitsorganisationen abgebildet werden können.

Bei der Planung der Sicherheitsorganisation gilt es daher, bereits zu einem frühen Zeitpunkt eine **Entscheidung zwischen** einer **zentralisierten Sicherheitsorganisation oder** einer eher **dezentralen mit zentraler Führung organisierten Sicherheitsorganisation** zu **treffen**. Die jeweiligen Ablaufprozesse sollten dies ebenso widerspiegeln, damit die Sicherheitsorganisation **effizient** ihre **Ziele umsetzen** kann. Entsprechend dem gewählten Ansatz beschreibt die Institution daher die Aufgaben der beteiligten Rollen eindeutig und stimmt sie mit den beteiligten Bereichen ab. Werden Aufgaben in die Linie delegiert, stellt die Institution sicher, dass diese durch die bestehende Bereichsorganisation auch tatsächlich geleistet werden können.

grundsätzliche Parameter für die Ausrichtung der Sicherheitsorganisation

Im **Grundsatz** gelten hierbei folgende **Aussagen**:

- **Je größer und komplexer** die Institution ist, **desto vielfäl-**

tiger sind **die Aufgaben**, die die Sicherheitsorganisation zu bedienen hat.

- **Je größer und komplexer** die Institution ist, **desto wichtiger** ist eine **zentralisierte und einheitliche Steuerung**, damit institutionsweit das definierte einheitliche Sicherheitsniveau gewährleistet wird.
- **Je mehr Standorte** und ggf. auch Länder von der Institution genutzt werden, **desto umfangreicher** sind **die Anforderungen an** die jeweiligen **lokalen Organisationsbereiche**.
- **Je größer die Exponiertheit** und je ausgeprägter das Risikoprofil, **desto umfassender** sind das S**icherheitsrisikomanagement und** der **Maßnahmenumfang**.

Die Leitung der Institution sollte daher eine **angemessene Ausgewogenheit zwischen erforderlichen Aufgaben und personeller Ausstattung** der Sicherheitsorganisation finden.

B.4 Bestimmung der Themengebiete

Der Wirtschaftsgrundschutz ist so aufgebaut, dass **grundsätzlich alle Themengebiete** eine **Relevanz** für die Institution haben werden. Allerdings kann es von Institution zu Institution **unterschiedliche Schwerpunkte** in den einzelnen Themengebieten geben. Dies sollte die Institution in ihrer **individuellen Umsetzung** berücksichtigen.

Die Institution bestimmt daher die für sie **relevanten Themengebiete** und definiert die **Schwerpunkte für die Sicherheitsorganisation**. Aus den priorisierten Themengebieten wird anschließend der **erforderliche Regelungsbedarf** abgeleitet. Aufgrund der festgelegten Schwerpunkte ergeben sich Anforderungen an die Ausprägung der Sicherheitsorganisation in Form von **Wissen und Ressourcen**.

B.5 Bestimmung der relevanten Bausteine

Die Institution bestimmt die für sie relevanten Bausteine **aufgrund** ihrer **individuellen Geschäftstätigkeit und** des **festgelegten Anwendungsbereichs**. Als Grundlage für die Einschätzung der Relevanz der Bausteine für die Institution dienen die **Entscheidungshilfen in den**

jeweiligen Bausteinen. Den zuvor **identifizierten Werten werden** somit über die Zuordnung der Bausteine die jeweiligen **Maßnahmen zugeordnet**.

Nicht relevante Bausteine werden eindeutig **benannt und** aus der Umsetzungsplanung **ausgenommen**. Bspw. wird der Baustein Produkt- und Know-how-Schutz für nicht produzierende Institutionen weniger Relevanz besitzen als für produzierende, und Institutionen, die ausschließlich in Deutschland tätig sind, werden eine geringe Relevanz für den Baustein Reisesicherheit erkennen.

Sollte sich die Geschäftstätigkeit oder das Geschäftsfeld zukünftig jedoch ändern, soll die Institution diese **Betrachtung überprüfen**, da anderenfalls Lücken im Sicherheitsmanagement entstehen könnten.

B.6 Bestimmung der relevanten Maßnahmenkategorie

Die im Wirtschaftsgrundschutz enthaltenen **Bausteine beinhalten** hinsichtlich der Umsetzung **unterschiedliche Kategorien von Maßnahmenempfehlungen**. Die dort enthaltenen Beschreibungen tragen den **unterschiedlichen Sicherheitsanforderungen** der Institution sowie der damit korrespondierenden Ausprägung des jeweiligen Themengebiets Rechnung. Diese können sich auch aus der **Sicherheitsstrategie** und den **konkreten Sicherheitszielen** der Werte (vgl. Kapitel 2.2.2) ergeben.

Im Wirtschaftsgrundschutz kommen insgesamt die **drei Kategorien Basismaßnahmen, Standardmaßnahmen und erweiterte Maßnahmen** zur Anwendung. Diese sind so strukturiert, dass die nächsthöhere Kategorie auf den Maßnahmen der vorherigen Kategorie aufbaut und diese sinnvoll erweitert. Zum Beispiel sind in der spezifischen Ausprägung eines Themengebiets bei den erweiterten Maßnahmen (Kategorie C) neben den neu hinzukommenden Maßnahmen ebenfalls die der Kategorien A und B enthalten.

Institutionen **überprüfen regelmäßig die Angemessenheit des Sicherheitsmanagementsystems** und bewerten dabei, ob alle identifizierten Gefährdungen angemessen berücksichtigt wurden. Sie bewer-

tet ebenfalls, ob die bereits umgesetzten Maßnahmen ausreichen, um die Sicherheitsziele zu erfüllen. Zum Beispiel kann sich die Risikoexposition der Institution verändern oder besondere Einsatzszenarien dazukommen, die zu einer Steigerung der Sicherheitsanforderung führen und zusätzliche Maßnahmen erforderlich machen.

Die nachfolgende Tabelle enthält eine B**eschreibung der unterschiedlichen Kategorien** sowie wesentliche **Aspekte zur Orientierung** für die **Bestimmung des Umsetzungsgrads**.

Kategorie	Beschreibung	Aspekte für die Bestimmung
A - Basismaßnahmen	Die in den Basismaßnahmen enthaltenen grundlegenden Mechanismen stellen die Grundlage für den Einstieg in das Themengebiet dar. Sie müssen grundsätzlich von allen Institutionen implementiert werden und sind essentiell für die Gewährleistung eines basalen Sicherheitsniveaus innerhalb des betrachteten Bausteins.	• Basisschutz • geringe bis mittlere Risikoexposition
B - Standardmaßnahmen	Die Standardmaßnahmen stellen die erste Aufbaustufe dar und sollten in Betracht gezogen werden, wenn Institutionen einen höheren Reifegrad innerhalb eines Themengebiets erzielen möchten oder mit der Erfüllung der Basismaßnahmen die identifizierten Gefährdungen nicht ausreichend abgedeckt sind.	• erhöhter Schutz • mittlere bis hohe Risikoexposition • besondere Einsatzszenarien
C - erweiterte Maßnahmen	Die in dieser Kategorie enthaltenen Maßnahmen sind wichtig für die ganzheitliche Betrachtung eines Themengebiets. Sie stellen darüber hinaus die notwendige Ergänzung der aus einem erhöhten Schutzbedarf resultierenden höheren Sicherheitsanforderungen dar.	• erweiterter Schutz • sehr hohe Risikoexposition

Tabelle 1: Beschreibung der unterschiedlichen Maßnahmenkategorien

Glossar

Anhang C

Siehe das Glossar zum Wirtschaftsgrundschutz in der jeweils aktuellen Version.

Verzeichnisse

Anhang D

D.1 Abbildungsverzeichnis

Abbildung 1: PDCA-Zyklus Sicherheitsmanagement 9

D.2 Tabellenverzeichnis

Tabelle 1: Beschreibung der unterschiedlichen Maßnahmenkategorien 25
Tabelle 2: Querverweise ISO 27001 30

Literaturverzeichnis

Anhang E

- *American National Standards Institute 2009: ANSI/ASIS PAP.1-2009, Organizational Resilience: Security, Preparedness, and Continuity Management Systems – Requirements with Guidance for Use*
- *American National Standards Institute 2012: ANSI/ASIS PAP.1-2012, Security Management Standard: Physical Asset Protection*
- *British Standards Institute 2014: BS 11200:2014 Crisis Management – Guidance and Good Practice*
- *Bundesministerium des Innern 2009: Nationale Strategie zum Schutz kritischer Infrastrukturen (KRITIS-Strategie)*
- *Bundesministerium des Innern 2005: Schutz kritischer Infrastrukturen – Basisschutzkonzept*
- *Bundesministerium des Innern 2011: Schutz kritischer Infrastrukturen – Risiko- und Krisenmanagement*
- *Bundesamt für Bevölkerungsschutz und Katastrophenhilfe 2011: Leitfaden für strategische Krisenmanagement-Übungen*
- *Bundesamt für Sicherheit in der Informationstechnik 2008: BSI-Standard 100-4 Notfallmanagement*
- *Gesamtverband der deutschen Versicherungswirtschaft e.V. 2012: VdS 3143 : 2012-09 Sicherungsleitfaden Perimeter*
- *International Electrotechnical Commission: IEC/TS 62443 Industrial Communication Networks*
- *International Organization for Standardization 2009: ISO 31000:2009 Risk Management – Principles and Guidelines*
- *International Organization for Standardization 2011: ISO 22320:2011 Societal Security – Emergency Management – Requirements for Incident Response*
- *International Organization for Standardization 2012: ISO 22301:2012 Societal Security – Business Continuity Management Systems - Requirements*
- *International Organization for Standardization 2012: ISO 22398:2012 Societal Security – Guidelines for Exercises and Testing*
- *International Organization for Standardization 2013: ISO 27001:2013 Information Technology – Security Techniques – Information Security Management Systems – Requirements*
- *International Organization for Standardization 2005: ISO/IEC 27002:2005 Information Technology - Securi-*

ty Techniques - Code of Practice for Information Security Management

- *International Organization for Standardization 2008: ISO 24762:2008 Information Technology – Security Techniques – Guidelines for Information and Communications Technology Disaster Recovery Services*
- *Österreichisches Normungsinstitut 2009: ÖNORM S 2400:2009 Business Continuity und Corporate Security Management*

Referenz zu ISO/IEC 27001

Anhang F

Viele Institutionen betreiben zum Schutz elektronischer Informationen bereits ein Informationssicherheitsmanagementsystem.

Der Wirtschaftsgrundschutz folgt der grundsätzlichen Struktur aktueller Managementsysteme, wie sie bspw. durch die International Organization for Standardization (ISO) beschrieben werden. Dadurch ergeben sich vergleichbare Regelungsbedarfe, auf die in dieser Referenztabelle zur ISO/IEC 27001 hingewiesen wird. Für eine ressourcenschonende Einführung empfiehlt der Wirtschaftsgrundschutz, diese vergleichbaren Regelungsbedarfe zu identifizieren und aneinander anzupassen.

ISO-Control		Kapitel	Referenzstandard
4.1.	Verständnis der Organisation und ihres Kontexts	2.3.1 3.2	2000-1
4.2.	Verständnis der Bedürfnisse und Erwartungen interessierter Parteien	2.3.3	2000-1
4.3.	Festlegung des Geltungsbereichs des Informationssicherheitsmanagementsystems	2.3.3	2000-1
4.4.	Informationssicherheitsmanagementsystem	3	2000-2
5.1.	Führung und Engagement	2.4	2000-1
5.2.	Leitlinie	2.3.3	2000-1
5.3.	Organisatorische Aufgaben, Zuständigkeiten und Befugnisse	2.3.4	2000-1
6.1.1.	Allgemeines	3.2	2000-2
6.1.2.	Informationssicherheitsrisikoeinschätzung	3.2	2000-2
6.1.3.	Informationssicherheitsrisikobehandlung	3.2	2000-2
6.2.	Informationssicherheitsziele und Pläne für deren Erreichung	2.3.2	2000-1
7.1.	Ressourcen	3.2	2000-1

7.2.	Kompetenz	4.2	2000-1
7.3.	Bewusstsein	4.3	2000-1
7.4.	Kommunikation	4.4	2000-1
7.5.	Dokumentierte Informationen	3	2000-2
8.1.	Einsatzplanung und -kontrolle	3	2000-2
8.2.	Informationssicherheitsrisikoeinschätzung	3	2000-2
8.3.	Informationssicherheitsrisikobehandlung	3	2000-2
9.1.	Überwachung, Messung, Analyse und Auswertung	3	2000-2
9.2.	Internes Audit	3	2000-2
9.3.	Prüfung durch die Leitung	3	2000-2
10.1.	Fehler und Korrekturmaßnahmen	5	2000-1
10.2.	Laufende Verbesserung	5	2000-1

Tabelle 2: Querverweise ISO 27001

Danksagung

Wir bedanken uns bei den vielen Experten, die ihr Fachwissen bei der Erstellung dieses Standards einfließen ließen und durch ihr Engagement die Entstehung erst ermöglicht haben. Insbesondere gilt unser Dank folgenden Autoren und Mitwirkenden: Herr Mathias Köppe und Herr Matthias Müller (HiSolutions AG) sowie Herr Prof. Martin Langer (FH Campus Wien).

Impressum

Herausgeber
Bundesamt für Verfassungsschutz
Merianstraße 100, 50765 Köln
www.verfassungsschutz.de

Herausgeber
Bundesamt für Sicherheit in der Informationstechnik (BSI)
Godesberger Allee 185-189, 53175 Bonn
www.bsi.bund.de

Herausgeber
ASW Bundesverband
Allianz für Sicherheit in der Wirtschaft e.V.
Rosenstraße 2, 10178 Berlin
asw-bundesverband.de

Redaktion/Bezugsquelle/Ansprechpartner
Prof. Timo Kob (Gesamtprojektleitung)

Gestaltung, Produktion
HiSolutions AG

Druck
SunCopy GmbH, Berlin

Stand
August 2016

Auflage
1. Auflage