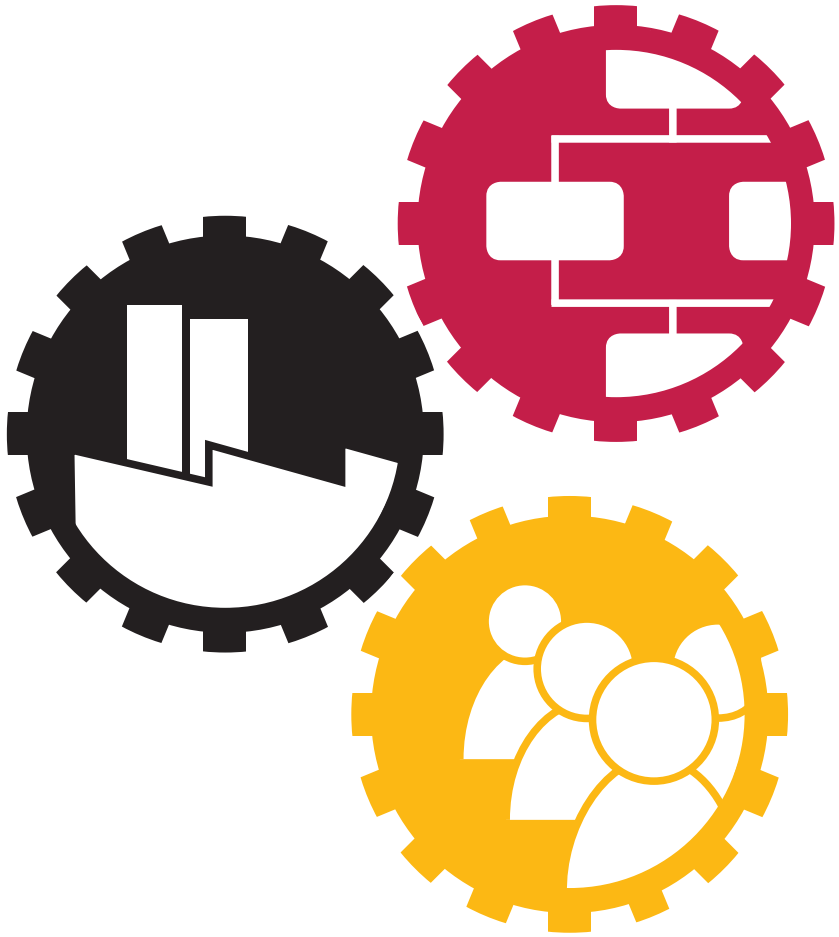
Bundesamt für Verfassungsschutz

Bundesamt für Sicherheit in der Informationstechnik

ASW Bundesverband

Wirtschaftsgrundschutz

Standard 2000-2
Aufbau und Betrieb eines Sicherheitsmanagementsystems



Inhaltsverzeichnis

1. Einleitung ... 2

1.1. Präambel ... 2

1.2. Einordnung dieses Dokuments ... 3

2. Das Sicherheitsmanagementsystem ... 4

2.1. Die grundsätzlichen Ziele des Sicherheitsmanagementsystems ... 4

2.2. Die wesentlichen Aufgaben des Sicherheitsmanagementsystems ... 4

2.3. Die Sicherheitsorganisation ... 6

2.4. Rollen der Sicherheitsorganisation ... 7

2.5. Gremien der Sicherheitsorganisation ... 9

3. Die Prozesse des Sicherheitsmanagementsystems ... 11

3.1. Betrieb des Sicherheitsmanagementsystems ... 11

3.2. Überblick über das Prozessmodell ... 11

3.3. Kontext der Institution ... 13

3.4. Führungsprozesse ... 14

3.5. Berichts- und Kontrollprozesse ... 16

3.6. Themenübergreifende Prozesse ... 17

3.7. Sicherheitsrelevante Themengebiete ... 18

3.8. Umsetzung und Wirksamkeit überprüfen ... 19

3.9. Anpassung und Weiterentwicklung von Sicherheitsmaßnahmen ... 19

Anhang A Themenübergreifende Prozesse ... 21

A.1 Berechtigungsmanagement ... 21

A.2 Schulung und Sensibilisierung ... 21

A.3 Sicherheitsrisikomanagement ... 23

A.4 Sicherheitsvorfallmanagement ... 24

Anhang B Verzeichnisse ... 26

B.1 Abbildungsverzeichniss ... 26

B.2 Tabellenverzeichnis ... 26

Danksagung ... 27

1 Einleitung

1.1. Präambel

Der **Schutz der Werte** der Institution erfolgt in den verschiedenen Themengebieten und ist dabei einer **kontinuierlichen Weiterentwicklung und Kontrolle** unterworfen.

Die **integrative Steuerung der sicherheitsrelevanten Themengebiete** erfordert ein **systematisches Vorgehen** und einen s**trukturierten, wiederholbaren Prozess**. Mit dem **Sicherheitsmanagementsystem** werden genau diese Anforderungen zusammengefasst und in einem System umfassend beschrieben. Der Institution steht mit dem Sicherheitsmanagementsystem ein schlagkräftiges Werkzeug zur Verfügung, mit dem sie **Sicherheit in den relevanten Feldern** aktiv und **dem individuellen Schutzbedarf angemessen** umsetzt.

Dies ist insbesondere deshalb von großer Bedeutung, weil **Sicherheit nicht in einem einzelnen Geschäftsbereich allein realisiert** werden kann, sondern im Regelfall mehrere Bereiche gemeinsam dazu beitragen. Eine **Koordination der Maßnahmen** ist damit ein **zentraler Punkt des Sicherheitsmanagementsystems**. Auf diese Weise stellt die Institution sicher, dass der Schutz der Werte **keine Lücken** aufweist und die Mittel **ressourcenschonend und effektiv** eingesetzt werden.

Das **Ergebnis** ist das durch die Leitung der Institution vorgegebene **einheitliche Sicherheitsniveau**.

1.2. Einordnung dieses Dokuments

Dieses Dokument stellt die **Rahmenanforderungen an ein Sicherheitsmanagementsystem** dar und **ergänzt** damit die allgemeinen und spezifischen **Definitionen des Wirtschaftsgrundschutzstandards 2000-1**. Der **Standard 2000-2 ist** damit der **Leitfaden zur Einführung eines Sicherheitsmanagementsystems**.

Bei der Einführung eines Sicherheitsmanagementsystems nach Wirtschaftsgrundschutz ist dieses Dokument ebenso bindend wie der Standard 2000-1.

2 Das Sicherheits-managementsystem

2.1. *Die grundsätzlichen Ziele des Sicherheits-managementsystems*

Ein **erfolgreiches und wirksames Sicherheitsmanagementsystem erfordert**, dass die Institution die **Sicherheitsstrategie definiert** hat. Die **Sicherheitsziele** sind **in** einer **Sicherheitsleitlinie dokumentiert**.

Die **Sicherheitsstrategie und** die **Sicherheitsleitlinie** stellen den mit der Leitung der Institution abgestimmten **Rahmen zur Etablierung des Sicherheitsmanagementsystems** bereit. Die Ziele des Sicherheits-managementsystems konkretisieren diese strategischen Vorgaben der Leitung der Institution für die praktische Umsetzung in der Institution.

Aufgabe der Institution

Die **Institution soll**

- die **Ziele** des Sicherheitsmanagementsystems **festlegen**

2.2. *Die wesentlichen Aufgaben des Sicherheits-managementsystems*

Die Institution definiert in ihrem Regelwerk die Aufgaben, die die Sicherheitsorganisation wahrnehmen soll. Sie regelt zudem die mit den Aufgaben verbundenen **Kompetenzen** eindeutig.

Beispiele für Aufgaben und Kompetenzen der Sicherheitsorganisation

In der nachfolgenden Auflistung sind **beispielhaft Aufgaben und Kompetenzen der Sicherheitsorganisation** aufgeführt:

- Erstellen einer **unternehmensweiten Richtlinie und** der **Sicherheitsstrategie**
- **Integrieren** der Sicherheit **in die Ziele, Werte und Kultur** der Institution
- Identifizieren, Bewerten und Behandeln **sicherheitsrelevanter Risiken**
- Bereitstellen **einheitlicher Methoden und Verfahren**
- Schaffen einer **stetigen Kommunikation und** eines **stetigen Austauschs** mit allen Bereichen der Institution
- Etablieren eines **Berichtswesens zum Umsetzungsstand** der Sicherheitsstrategie in den Fachbereichen
- Betreiben eines **Messsystems zum Reifegrad** der Sicherheit der Institution; Festlegen der entsprechenden **Indikatoren und Skalierungen**
- Aufbereiten und Bereitstellen eines **regelmäßigen Sicherheitsreports für den Vorstand**
- Erstellen und regelmäßiges Aktualisieren eines **Sicherheitslagebilds** unter Einbeziehung aller relevanten **internen und externen Quellen**
- Bereitstellen eines **Netzwerks qualifizierter Sicherheitsdienstleister** für bedarfsweise angeforderte spezialisierte und technische Sicherheitsdienstleistungen
- Durchführen **regelmäßiger Überprüfungen im Rahmen eines Auditplans**

Des Weiteren übernimmt die Sicherheitsorganisation **unterstützende Funktion** für weitere Geschäftsbereiche, indem sie

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

Aufgabe der Institution

Die **Institution soll**

- die **Aufgaben** des Sicherheitsmanagementsystems **festlegen und dokumentieren**

2.3. Die Sicherheitsorganisation

Die Sicherheitsorganisation **spiegelt** im Regelfall die **von der Leitung** der Institution **festgelegten sicherheitsrelevanten Themengebiete wider**.

Der **Sicherheitsverantwortliche** ist mit der **organisatorischen Leitung** betraut. Er **berichtet unabhängig** von der organisatorischen Einbindung der Sicherheitsorganisation **direkt an die Leitung** der Institution.

Dem **Sicherheitsverantwortlichen** obliegt im Auftrag der Leitung der Institution die **Ausgestaltung der erforderlichen Organisationsstruktur**. Dies kann bei größeren Institutionen durch die Benennung zuständiger Leiter für die identifizierten Themengebiete und ggf. erforderlicher weiterer Funktionsträger erfolgen. Sofern bspw. die IT-Sicherheit oder der Datenschutz nicht in die Sicherheitsorganisation integriert ist, stellt die Sicherheitsorganisation eine **Schnittstelle** zur Verfügung.

Abbildung 1 verdeutlicht die **anzustrebende Sicherheitsorganisation** beispielhaft.

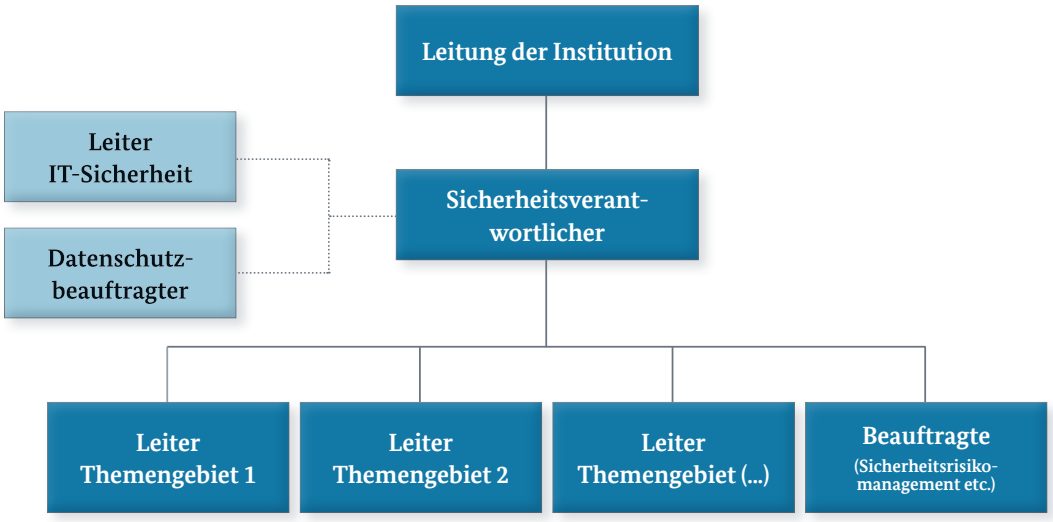


Abbildung 1: Beispielhafte Sicherheitsorganisation

Aufgaben der Institution

Die **Institution soll**

- eine **Sicherheitsorganisation festlegen und in Kraft setzen**
- die Sicherheitsorganisation mit **angemessenen Ressourcen** ausstatten
- die für die Sicherheitsorganisation **relevanten anderen Geschäftsbereiche oder Fachfunktionen** innerhalb und außerhalb der Institution **identifizieren** und **Schnittstellen** zu diesen **beschreiben und etablieren**

2.4. Rollen der Sicherheitsorganisation

Eine angemessene Sicherheitsorganisation erfordert die **Definition von Rollen**. Dies umfasst sowohl die Leitung der Sicherheitsorganisation selber als auch die der definierten Themengebiete und ggf. Beauftragte für einzelne Fachthemen, wie bspw. das Sicherheitsrisikomanagement.

Rollen und Aufgaben

In **Tabelle 1** werden **beispielhaft einige Rollen mit einigen grundsätzlichen Aufgaben** beschrieben.

Rolle	Aufgabe
Sicherheitsverantwortlicher	• Leitung der Sicherheitsorganisation • Freigabe der notwendigen Ressourcen (Budget, Arbeitsmittel, Arbeitszeit und geeignetes Personal) • Entwicklung und laufende Verbesserung der Sicherheitsstrategie • Gestaltung der Aufbau- und Ablauforganisation der Sicherheitsorganisation • Entwicklung und laufende Verbesserung der Richtlinie „Sicherheitsorganisation“
Leiter Themengebiet	• Entwicklung und laufende Verbesserung der Methodik des jeweiligen Themengebiets • Erstellung, regelmäßige Überprüfung und Aktualisierung übergeordneter Sicherheitskonzepte

Rolle	Aufgabe
	• Unterstützung des Sicherheitsrisiko-managements • Konsolidierung der in den Organisations-einheiten entwickelten Maßnahmen zur Behandlung von Sicherheitsrisiken • Koordination bereichsübergreifender Maßnahmen zur Behandlung von Sicher-heitsrisiken und zur Überwachung der Umsetzung • Beratung und Betreuung der Geschäftsbe-reiche und von Projekten
Beauftragter Sicherheitsrisiko-management	• Steuerung und Koordination des Sicher-heitsrisikomanagements • Entwicklung und laufende Verbesserung einer Methodik • Identifikation, Analyse und Bewertung übergreifender Sicherheitsrisiken • Einfordern der Meldung von Sicherheits-risikoerhebungen aus den Themengebie-ten • Kommunikation und Abstimmung der Maßnahmen mit den Themengebieten • Know-how-Transfer und Berichtswesen
Beauftragter weiteres Thema	• Steuerung und Koordination des jeweili-gen Themas • Entwicklung und laufende Verbesserung einer Methodik • Know-how-Transfer und Berichtswesen

Tabelle 1: Rollenübersicht

Neben diesen allgemeinen Aufgaben definiert die Institution gegebenenfalls notwendige weitere Aufgaben. Sie beschreibt zudem die **mit der Rolle verbundenen Kompetenzen und Verantwortungen**.

Aufgaben der Institution

Die **Institution soll**

- die in der Sicherheitsorganisation **erforderlichen Rollen festlegen**

- die Rollen mit **Aufgaben, Kompetenzen und Verantwortung** beschreiben
- das **Rollenmodell** dokumentieren und freigeben

2.5. Gremien der Sicherheitsorganisation

Allgemeines

Gremien unterstützen die institutionsweite Arbeit der Sicherheitsorganisation. Die Sicherheitsorganisation nutzt Gremien, um sowohl **strategische Aspekte** als auch **operationelle Fragen** in und mit den Geschäftsbereichen der Institution **abzustimmen**. Insbesondere in größeren Institutionen **ermöglicht** die **Multiplikation von Wissen** über eine aktive Gremienarbeit eine **große und ressourcensparende Erleichterung in der Arbeit der Sicherheitsorganisation**.

Aufgabe der Institution

Die **Institution soll**

- die für sie **relevanten Gremien festlegen** und mit einem **konkreten Auftrag** beschreiben

Sicherheitslenkungskreis

Die Institution nutzt einen Sicherheitslenkungskreis, um die strategischen Rahmenbedingungen institutionsweit abzustimmen.

Die **wesentlichen Inhalte der Sitzungen** des Sicherheitslenkungskreises sind beispielweise:

- Lagebericht
- aktueller Sicherheitsstand
- Übersicht Sicherheitsrisiken
- Bedarf strategischer Änderungen der Ausrichtung
- anstehende Themen oder Projekte

Der Sicherheitslenkungskreis ist **mit der Leitung der Institution, dem Sicherheitsverantwortlichen und weiteren wesentlichen Führungskräften aus der Leitungsebene der Institution besetzt**.

Der Sicherheitslenkungskreis hält **regelmäßige Sitzungen während eines laufenden Geschäftsjahrs** ab.

Sicherheitsfachkreis

Für die operationelle Umsetzung und den Betrieb des Sicherheitsmanagements nutzt die Institution einen Sicherheitsfachkreis. Dessen wesentliche Aufgaben sind der **fachliche Austausch**, die **Abstimmung der taktischen/operativen Umsetzung der strategischen Rahmenbedingungen** sowie die **Sensibilisierung** für neue oder geänderte Gefährdungslagen oder Rahmenanforderungen (z. B. durch Gesetze oder regulatorische Auflagen).

Die **wesentlichen Inhalte der Sitzungen** des Sicherheitsfachkreises sind beispielweise:

- allgemeiner Lagebericht
- Übersicht Sicherheitsrisiken
- Statusberichte der Themengebietsverantwortlichen
- aktuelle Themen oder Projekte
- Trends und Entwicklungen

Der Sicherheitsfachkreis ist **mit Funktionsträgern der wesentlichen Geschäftsbereiche, dem Sicherheitsverantwortlichen und ggf. weiteren Führungskräften** nach Bedarf **besetzt** und hält **regelmäßige Sitzungen** ab.

3 Die Prozesse des Sicherheitsmanagementsystems

3.1. Betrieb des Sicherheitsmanagementsystems

Der **Betrieb des Sicherheitsmanagementsystems** erfolgt **anhand** des in diesem Kapitel beispielhaft beschriebenen **Prozessmodells**. Das Prozessmodell **spiegelt** dabei die **definierten Aufgaben und Themengebiete wider**.

Aufgaben der Institution

Die **Institution soll**

- ein **Prozessmodell des Sicherheitsmanagementsystems** definieren, beschreiben und in Kraft setzen
- die einzelnen **erforderlichen Prozesse** festlegen, dokumentieren und freigeben
- die **themenübergreifenden Prozesse** beschreiben und in das Prozessmodell integrieren
- den **Kontext** bestimmen, in dem das Sicherheitsmanagementsystem aufgebaut wird
- eine **Gefährdungsanalyse** durchführen, um Gefährdungen zu identifizieren und zu bewerten
- ein **Sicherheitsrisikomanagement** etablieren, um die mit den Gefährdungen verbundenen Sicherheitsrisiken zu bestimmen

3.2. Überblick über das Prozessmodell

Das **Prozessmodell** der Unternehmenssicherheit **basiert auf** einem **zyklischen System**, das auf die **kontinuierliche Verbesserung** ausge-

richtet ist. Es erfüllt alle relevanten **internen und externen Anforderungen**.

Abbildung 2 stellt schematisch das **Prozessmodell im Wirtschaftsgrundschutz** dar.

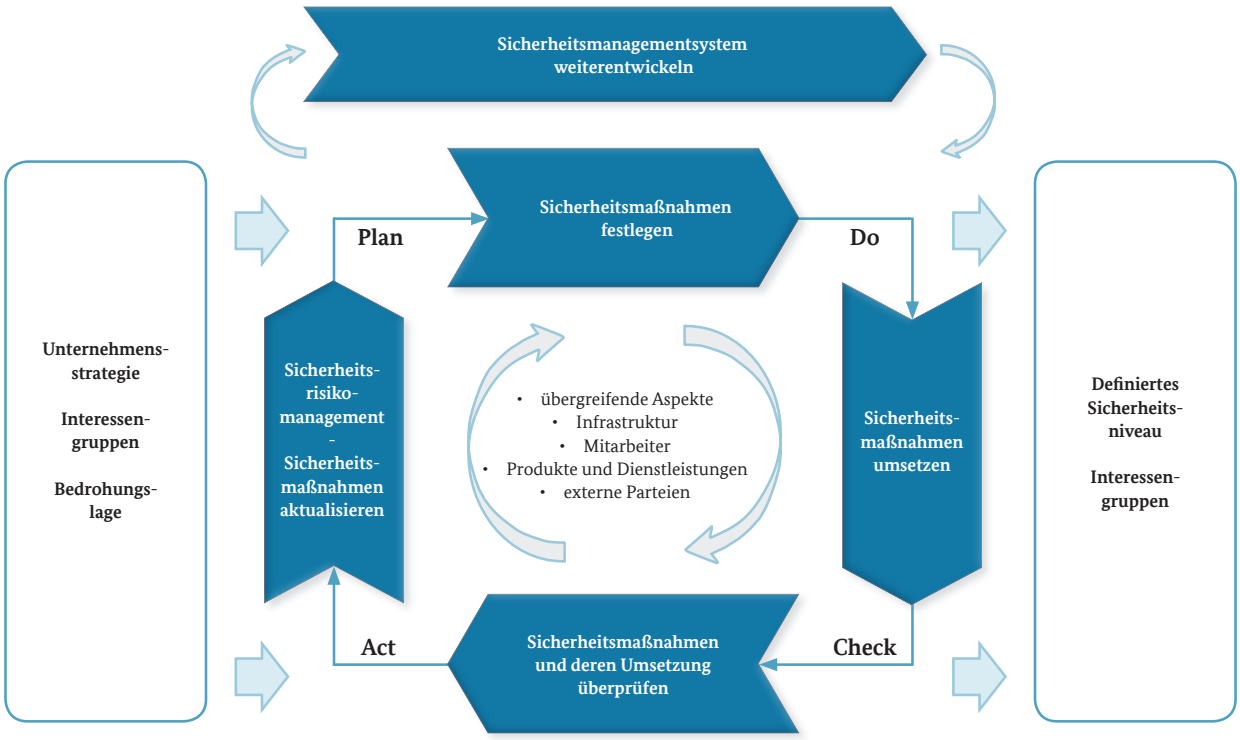


Abbildung 2: PDCA-Zyklus Sicherheitsmanagement

Prozesslandschaft im Sicherheitsmanagement

Die Sicherheitsorganisation nutzt hierfür die **Führungs-, Steuerungs- und Berichts-/Kontrollprozesse** mit den entsprechenden Unterprozessen. Des Weiteren **integriert** sie die **themenübergreifenden Prozesse** in das Prozessmodell. Die Sicherheitsorganisation **integriert** ggf. auch die **definierten nachrangigen Managementsysteme** in das Prozessmodell.

Abbildung 3 gibt einen beispielhaften **Überblick über Haupt- und Unterprozesse** des Sicherheitsmanagementsystems.

Abbildung 3: Prozesslandschaft Sicherheitsmanagement

3.3. *Kontext der Institution*

Jede Institution unterliegt verschiedenen Umfeldfaktoren, und selbst allgemeine Einflüsse haben für jede Institution eine unterschiedliche Bedeutung.

Identifizieren von Einflussfaktoren

Die Institution **analysiert** daher ihren **individuellen Kontext** und bestimmt so, welche Faktoren für das Sicherheitsmanagement relevant sind. Sie bestimmt den Einfluss dieser Faktoren auf die **Funktionsfähigkeit der Geschäftstätigkeit**. Mit diesen Erkenntnissen gewinnt die Institution die wesentlichen Informationen, um **ein an die Institution angepasstes Sicherheitsmanagementsystem** aufzubauen.

Das Ziel der Kontextanalyse ist es, die internen und externen Einflüsse auf das Handeln der Institution zu identifizieren und zu dokumentieren.

Teile einer Kontextanalyse

Die nachfolgend aufgeführten Aspekte sind beispielhaft und **Teile einer Kontextanalyse**:

- die Einflüsse, die sich aus **sozialen, kulturellen, politischen, rechtlichen, regulatorischen, finanziellen, technologischen, ökonomischen, natürlichen und wettbewerblichen Aspek-**

ten ergeben, und dies **auf internationaler, nationaler, regionaler und lokaler Ebene**

- **strategische Entscheidungen und Trends**, die Einfluss auf die Ziele der Institution haben können
- **Beziehungen zu internen und externen Interessengruppen** und deren Erwartungen
- die **Kultur der Institution**
- die Leitung der Institution, die **Institutionsstruktur, Rollen und Verantwortlichkeiten**
- **Institutionsleitlinien und -ziele** und die **Strategien**, um diese zu erreichen
- das **finanzielle und fachliche Leistungsvermögen** der Institution
- **Informationsflüsse** und **Entscheidungsprozesse**
- angewendete **Standards, Richtlinien und Modelle**

Nachdem die Institution den Kontext ermittelt hat, identifiziert sie **darauf basierend die Gefährdungen**. Sie nutzt hierfür den **themenübergreifenden Prozess Sicherheitsrisikomanagement**.

3.4. Führungsprozesse

Regelwerke erstellen

Die Regelwerke sind erforderlich, um das Sicherheitsmanagementsystem nachvollziehbar betreiben zu können.

Das Regelwerk erstellt die Institution **hierarchisch**, wobei die **Sicherheitsleitlinie** das **führende Dokument** ist. In der nachrangigen Dokumentation beschreibt die Institution das **Managementsystem mit den Prozessen und Arbeitsabläufen** gemäß ihren internen Vorgaben des Dokumentenmanagementsystems.

Abbildung 4 stellt beispielhaft eine solche **Dokumentenpyramide** dar.

Abbildung 4: Regelwerk Sicherheitsmanagement

Das Regelwerk definiert den **Handlungsraum und die Arbeitsweisen** der Sicherheitsorganisation verbindlich.

Rollen festlegen

Die Institution definiert die **Rollen** in der Sicherheitsorganisation und beschreibt sie mit **Aufgaben, Kompetenzen und Verantwortungen**.

Sind Rollen außerhalb der Sicherheitsorganisation in anderen Geschäftsbereichen **zur Erfüllung der Sicherheitsziele** erforderlich, identifiziert die Institution diese. Sie stimmt sich inhaltlich mit dem betroffenen Geschäftsbereich über diese **Schnittstelle** ab.

Budget und Personal bereitstellen

Die Institution erstellt **auf Grundlage der Sicherheitsstrategie** und des individuellen Kontextes einen **Budget- und Personalplan**, auf dessen Grundlage sie die Umsetzung der Sicherheitsziele erreichen kann.

Die Leitung der Institution ist für die **angemessene Bereitstellung der Ressourcen** verantwortlich. Sie gibt den Budget- und Personalplan frei.

Leitung der Institution einbinden

Die Leitung der Institution trägt die Gesamtverantwortung für die Sicherheit in der Institution und für die Institution ebenso wie für den Schutz ihrer Werte.

Die Leitung der Institution **delegiert** die **Umsetzung** der hierfür erforderlichen Maßnahmen **an die Sicherheitsorganisation** und stellt **angemessene Rahmenbedingungen** bereit. Sie lässt sich von der Sicherheitsorganisation regelmäßig den **aktuellen Status** des Sicherheitsmanagements **berichten**.

Kontinuierliche Verbesserung umsetzen

Das gesamte Sicherheitsmanagementsystem ist auf eine kontinuierliche Verbesserung und eine permanente Weiterentwicklung ausgelegt.

Die Sicherheitsorganisation definiert das **Prozessmodell** so, dass eine kontinuierliche Verbesserung sichergestellt ist. Das Prozessmodell **lehnt sich** hierbei **an das international anerkannte Modell des PDCA -Regelkreises**[1] **an**.

3.5. Berichts- und Kontrollprozesse

Berichtswesen umsetzen

Die **Sicherheitsorganisation informiert die Leitung** der Institution **und definierte Interessengruppen regelmäßig über Status und Fortschritt** des Sicherheitsmanagements. Hierfür nutzt sie die nachfolgend aufgeführten **Berichtsarten**:

Berichtsarten

- Quartalsberichte
- Jahresberichte
- Ad-hoc-Berichte (bei sich gravierend ändernder Sicherheitslage)
- Vorfallberichte

[1] PDCA – Plan, Do, Check, Act: Planen, Betreiben, Überprüfen, Anpassen

Die **Institution definiert** die **Zielgruppe der jeweiligen Berichte** und legt die **Inhalte zielgruppengerecht** fest.

Kontrollsystem betreiben

Leistungsindikatoren

Die Institution definiert für das Sicherheitsmanagementsystem und ggf. alle installierten nachrangigen Managementsysteme **Kontrollen und Leistungsindikatoren**. Die Kontrollen und Leistungsindikatoren wertet die Institution regelmäßig aus. So kann sie jederzeit Auskunft über den **Status des Sicherheitsmanagementsystems** und auch des **Sicherheitsniveaus** erteilen.

Die Institution unterzieht alle Regelwerke, Sicherheitskonzepte und weiteren erzeugten Dokumente einem **jährlichen Management-review**.

Die **Revision** bzw. der mit dieser Aufgabe betraute Geschäftsbereich der Institution überprüft **als unabhängige Instanz** in regelmäßigen Abständen das Sicherheitsmanagementsystem.

Die Institution sammelt und analysiert alle **Erkenntnisse aus Kontrollen, Review und Revision**. Sie **leitet** daraus **Handlungsbedarfe** für Verbesserungen des Sicherheitsmanagementsystems **ab**.

3.6. Themenübergreifende Prozesse

Zur **Wahrung eines einheitlichen Sicherheitsniveaus** sind **themenübergreifende Prozesse** erforderlich. Diese wirken sich sowohl in mehreren Themengebieten des Sicherheitsmanagementsystems als auch in anderen Geschäftsbereichen aus.

Die nachstehende Auflistung stellt die **themenübergreifenden Prozesse im Wirtschaftsschutz** dar:

- Sicherheitsrisikomanagement
- Berechtigungsmanagement
- Sicherheitsvorfallmanagement
- Schulung und Sensibilisierung

Die Institution definiert und beschreibt die themenübergreifenden Prozesse. Sie stellt sicher, dass die themenübergreifenden Prozesse **sowohl innerhalb der Institution als auch bei Dienstleistern angewendet** werden.

3.7. Sicherheitsrelevante Themengebiete

Definition und Ausprägung

Die Institution bestimmt die für sie relevanten Themengebiete. Sie definiert damit den **fachlichen Rahmen des Sicherheitsmanagements entsprechend** ihren **individuellen Bedürfnissen und** der **Bedrohungslage**.

Dieser Standard gruppiert die **Themengebiete** wie folgt:

- übergreifende Aspekte
- Infrastruktur
- Mitarbeiter
- Produkte und Dienstleistungen
- externe Parteien

In den einzelnen Themengebieten sind **Bausteine für dedizierte fachliche Aspekte** definiert. Die Institution verwendet die Bausteine, um die Fachthemen umzusetzen.

Sicherheitskonzepte erstellen und Sicherheitsmaßnahmen festlegen

Die Institution erstellt **Sicherheitskonzepte** und legt in diesen **konkrete Sicherheitsmaßnahmen** fest, um die zuvor **definierten Sicherheitsziele für die jeweiligen Werte** zu erreichen. Mit Hilfe des Sicherheitsrisikomanagements **identifiziert** die Institution zuerst die **Sicherheitsrisiken**. Auf Basis dieser Erkenntnisse erstellt die Institution **optimal** auf ihre individuelle Gefährdungslage **abgestimmte Sicherheitskonzepte**.

Die vorhandenen Erkenntnisse aus Überprüfungen und Sicherheitsvorfällen nutzt die Institution, um die **Sicherheitskonzepte und**

-maßnahmen an die **praktischen Erfahrungen aus dem Betrieb anzupassen**.

Betreiben der sicherheitsrelevanten Themengebiete

Die Institution betreibt die für sie relevanten Themengebiete **mittels** der **Sicherheitsorganisation** und weiterer spezifischer Regelungen für die Themengebiete.

Die spezifischen Regelungen können bei Bedarf auch in eigenen, nachrangigen Managementsystemen geführt werden.

3.8. Umsetzung und Wirksamkeit überprüfen

Die Institution überprüft mittels **regelmäßiger Kontrollen** die Sicherheitskonzepte und einzelnen Sicherheitsmaßnahmen **im Hinblick auf** den **Grad ihrer Umsetzung und Wirksamkeit**. Insbesondere überprüft die Institution, **ob** die **Sicherheitskonzepte und Sicherheitsmaßnahmen angemessen sind** und der **Erreichung der Sicherheitsziele** dienen.

Überprüfungsmöglichkeiten

Der Institution stehen hierzu verschiedene **Überprüfungsmöglichkeiten** zur Verfügung, die sie fallspezifisch einsetzt. Diese sind bspw.:

- Dokumentations- und Organisationsüberprüfung
- technische Überprüfung
- Schwachstellentest
- Penetrationstest
- Test von Vorsorgeeinrichtungen technischer Systeme
- Übungen des Reaktionsmanagements (Notfall- & Krisenmanagement)

Alle Erkenntnisse aus der Überprüfung der Sicherheitskonzepte **sammelt** die Institution **und dokumentiert** sie bspw. **in einem Katalog**.

3.9. Anpassung und Weiterentwicklung von Sicherheitsmaßnahmen

Die Institution nutzt die **Erkenntnisse aus den Überprüfungen,**

(Sicherheits-)Risikoanalysen und Sicherheitsvorfällen, um die bisher definierten **Sicherheitskonzepte und -maßnahmen** an die neu gewonnenen Erkenntnisse **anzupassen**. Hierzu definiert sie **Handlungsoptionen und** bestimmt **Verantwortliche** für die Umsetzung.

Die Institution **dokumentiert** alle identifizierten **Verbesserungspotentiale und** die daraus abgeleiteten **Optimierungsmaßnahmen** in einem Katalog. Der Katalog enthält auch die **definierten Verantwortlichen**, den **Umsetzungszeitraum** und den **aktuellen Status jeder Optimierungsmaßnahme**.

Themenübergreifende Prozesse

Anhang A

A.1 Berechtigungsmanagement

Die Institution definiert einen **institutionsübergreifenden Prozess**, der sicherstellt, dass die erteilten Berechtigungen für Mitarbeiter oder Externe

- nach Bedarf und auf Antrag erteilt werden
- nach Wegfall des Bedarfs wieder entzogen werden
- abgestimmt sind zwischen Zugriffsberechtigungen für technische Systeme und den physischen Zutrittsberechtigungen
- jederzeit dokumentiert und nachvollziehbar sind

Die Sicherheitsorganisation stimmt sich hierzu mit den Bereichen Personalwesen und Informationsverarbeitung sowie ggf. weiteren Geschäftsbereichen ab.

A.2 Schulung und Sensibilisierung

Nur gut ausgebildete und ausreichend sensibilisierte Mitarbeiter verhalten sich entsprechend den Vorgaben des Sicherheitsmanagements und schützen so die Werte der Institution. Ebenso sind sie aufmerksamer gegenüber Veränderungen und damit möglichen Sicherheitsvorfällen.

Schulungskonzept

Die Institution erstellt ein **Schulungskonzept** und spezifiziert inhaltlich verschiedene vorgesehene **Schulungsmodule**. Mit dem Schulungskonzept ermöglicht die Institution allen Beteiligten einen **guten**

Kenntnisstand, ausreichende Fertigkeiten und eine sich wiederholende **einfache Möglichkeit zur praktischen Anwendung** des Gelernten.

Das **Schulungskonzept** wird **basierend auf dem erforderlichen Schulungsbedarf** erstellt und enthält **mehrere aufeinander aufbauende Schulungsmodule**. Dies sind bspw., mit entsprechender fachlicher Ausprägung:

- Einführung und Grundlagen
- methodische Fertigkeiten
- praktische Anwendung der erlernten Methodik
- Auffrischung

Zielgruppe der Schulungen sind alle Mitarbeiter der Institution. Die **Schulungen** werden jedoch **zielgruppengerecht aufbereitet und durchgeführt**. Somit gibt es neben allgemeinen Schulungen auch **spezielle Schulungen für bestimmte Funktionen**, z. B. zu den Themen Sicherheitsrisikomanagement, Notfall- und Krisenmanagement oder Sicherheit auf Reisen.

Das **Schulungskonzept definiert** die gesamten erforderlichen **Abläufe für Anmeldung, Auswertung zu Nachweiszwecken und Kommunikation** mit den Teilnehmern.

langfristiger Schulungsplan

Ein **langfristiger Schulungsplan**, beispielsweise für drei Jahre, **erlaubt** es der Institution, **Schulungen inhaltlich aufeinander aufzubauen**. Damit ermöglicht sie eine gezielte Ausbildung bspw. von Rollenträgern des Sicherheitsmanagements.

Die Institution achtet zudem auf eine **mit dem Übungsplan des Notfall- und Krisenmanagements abgestimmte Vorgehensweise**, damit Schulung und Übung ideal miteinander verzahnt werden können.

Definition der Rahmenbedingungen

In dem Schulungskonzept definiert die Institution somit die **Rahmenbedingungen und grundsätzliche konzeptionelle Regelungen**, wie in der nachfolgenden Liste beispielhaft aufgeführt:

- Teilnahmebedingungen
- verpflichtende Schulungen

- Häufigkeit und Wiederholungen
- Vollständigkeit der besuchten Schulungsmodule
- Schulungszyklus über eine bestimmte Laufzeit (z. B. drei Jahre)
- Verantwortung für Erstellung und Durchführung

A.3 Sicherheitsrisikomanagement

Definition Sicherheitsrisiko-management

Das Sicherheitsmanagementsystem identifiziert, bewertet und initiiert die Behandlung von Sicherheitsrisiken. Unter dem Begriff Sicherheitsrisikomanagement wird hierbei die Identifikation und Bewertung von Gefährdungen verstanden, die sich nachteilig auf die definierten **Sicherheitsziele von Personen, Prozessen, Informationen, Vermögenswerten, Dienstleistern und Infrastrukturen** auswirken können.

Um eine **einheitliche Sichtweise und Wertung** sicherzustellen, nutzt die Institution eine **zentral definierte Vorgehensweise und Methodik**.

Identifikation und Bewertung von Gefährdungen

Hierzu **analysiert** sie die **Gefährdungen**. Diese können auf Ressourcen innerhalb der Institution, aber ebenso auch auf Dritte oder auf eingebundene Partner der Institution wirken. Die identifizierten Gefährdungen führt die Institution dann einer **Risikoanalyse** unter **Berücksichtigung einer anzunehmenden Eintrittswahrscheinlichkeit und Schadenhöhe** zu. Für die sich hieraus ergebenden Sicherheitsrisiken legt die Institution **Maßnahmen im Rahmen der Risikobehandlung** fest. Mit **zugeordneten definierten Leistungskriterien** führt die Institution diese dann einer **dauerhaften Bewertung** zu.

Die Erkenntnisse fließen in die **Sicherheitskonzepte** der Institution ein. Für die Leistungskriterien definiert die Institution geeignete **Metriken, um das Sicherheitsrisiko dauerhaft messbar und kontrollierbar zu machen**.

Abbildung 5 stellt diesen Ablauf, als ein mögliches **Beispiel für den Risikomanagementprozess**, schematisch dar.

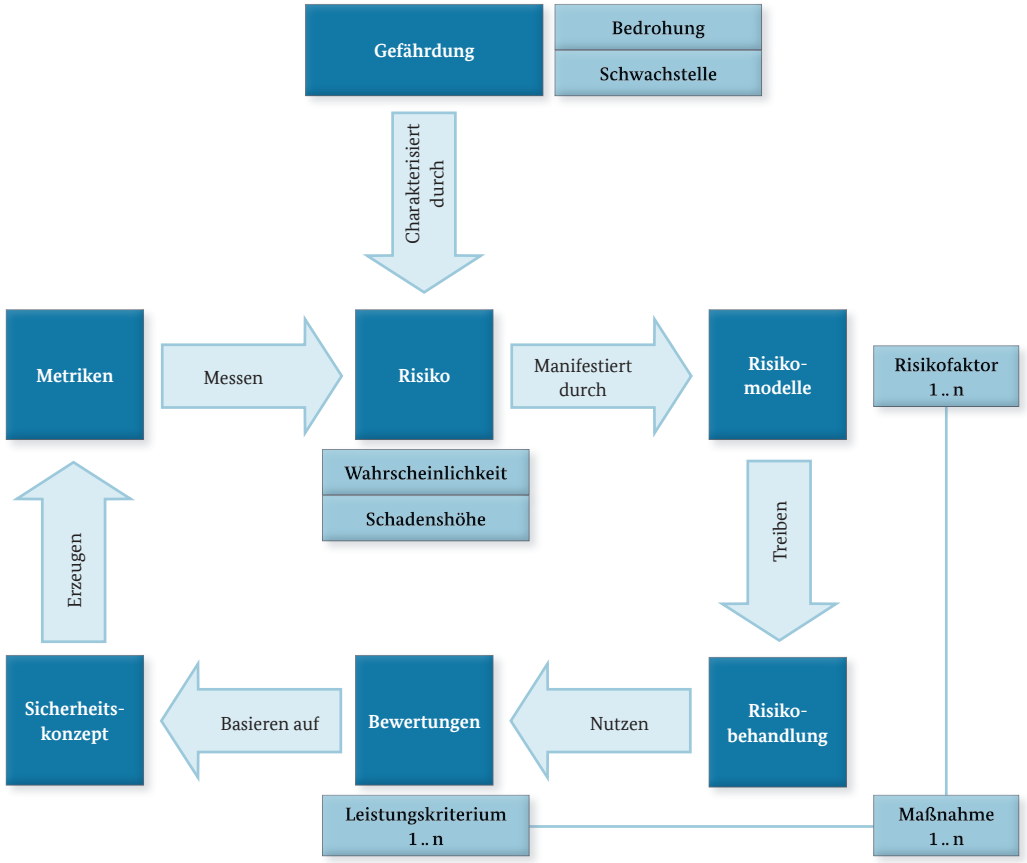


Abbildung 5: Sicherheitsrisikomanagement - Prozessablauf

Das Sicherheitsrisikomanagement etabliert die Institution in Abstimmung mit einem (operationellen) Risikomanagement. Durch **Angleichung der Parameter** erfolgt eine e**inheitliche Bewertung aller Risiken** der Institution. Die Sicherheitsrisiken fließen mit der gleichen Mess- und Bewertungsgrundlage in das **zentrale Risikomanagement** ein und bedürfen keiner fehleranfälligen und ressourcenkostenden Anpassung oder Umrechnung.

A.4 Sicherheitsvorfallmanagement

Die Institution schafft eine **zentrale Instanz, der auftretende Sicherheitsvorfälle gemeldet werden**, die diese qualifiziert und dann die weiteren notwendigen Maßnahmen zur **Bewältigung des Sicherheitsvorfalls** einleitet.

Im Rahmen des Wirtschaftsgrundschutzes vertiefen der **Standard 2000-3 „Aufbau und Betrieb eines Notfall- und Krisenmanagementsystems“** und ein dedizierter **Baustein „Sicherheitsvorfallmanagement“** dieses Thema.

Verzeichnisse

Anhang B

B.1 Abbildungsverzeichnis

Abbildung 1: Beispielhafte Sicherheitsorganisation 6
Abbildung 2: PDCA-Zyklus Sicherheitsmanagement 12
Abbildung 3: Prozesslandschaft Sicherheitsmanagement 13
Abbildung 4: Regelwerk Sicherheitsmanagement 15
Abbildung 5: Sicherheitsrisikomanagement - Prozessablauf 24

B.2 Tabellenverzeichnis

Tabelle 1: Rollenübersicht 7

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

Diese Broschüre ist Teil der Öffentlichkeitsarbeit der Bundesregierung. Sie wird kostenlos abgegeben und ist nicht zum Verkauf bestimmt.