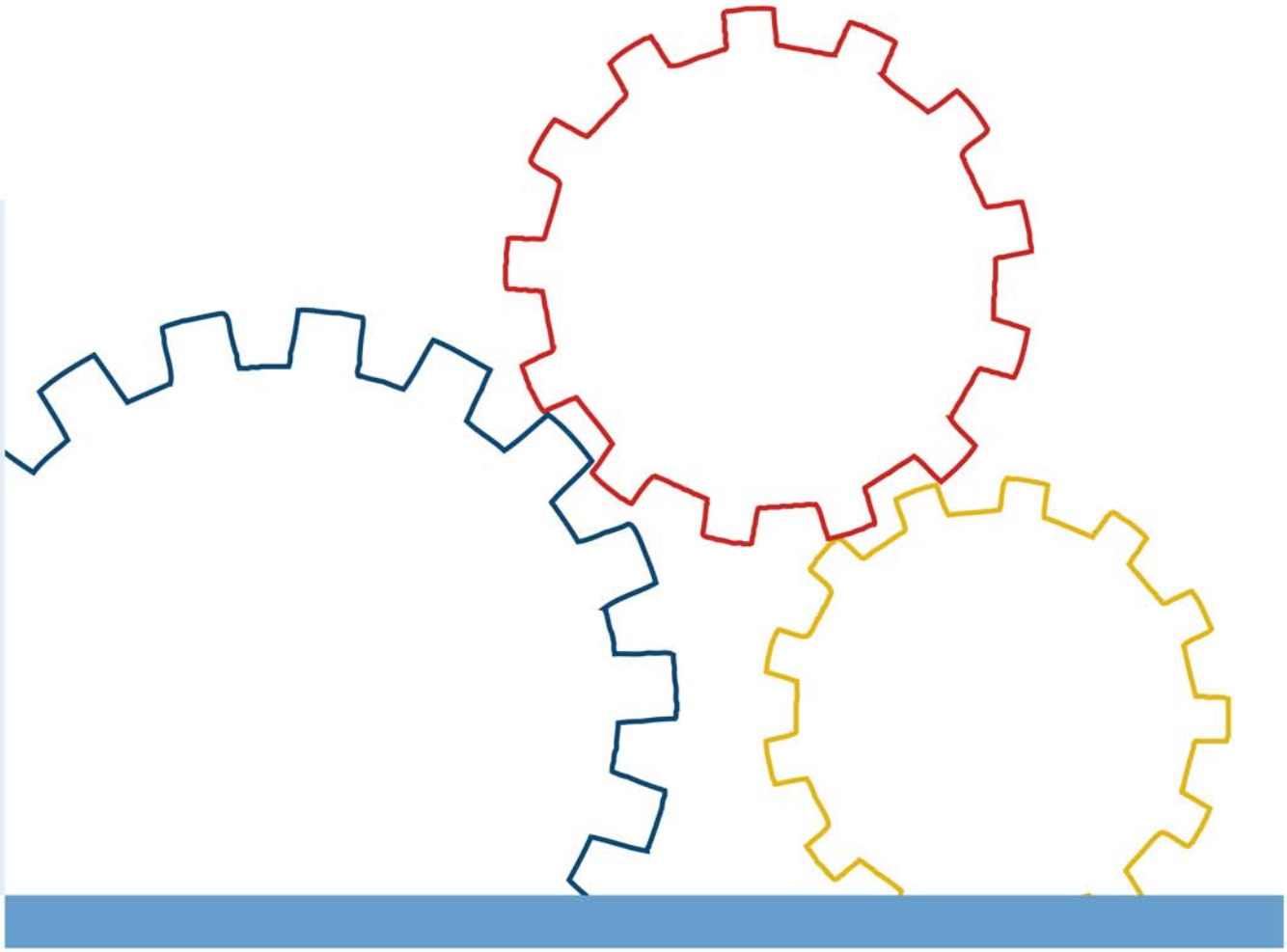
Bundesamt
für Sicherheit in der
Informationstechnik

# BSI-Standard 100-1

## Managementsysteme für Informationssicherheit (ISMS)



www.bsi.bund.de/gshb

Version 1.5

# Inhaltsverzeichnis

# 1 Einleitung

## 1.1 Versionshistorie

| Stand | Version | Änderungen |
|---|---|---|
| Dezember 2005 | 1.0 | BSI |
| Mai 2008 | 1.5 | - Stärkere Betonung der Informationssicherheit statt IT-Sicherheit, daher auch verschiedene Begriffe angepasst<br>- Anpassungen an Fortschreibung der ISO-Standards |

## 1.2 Zielsetzung

Informationen sind wichtige Werte für Unternehmen und Behörden und müssen daher angemessen geschützt werden. Die meisten Informationen werden heutzutage zumindest teilweise mit Informationstechnik (IT) erstellt, gespeichert, transportiert oder weiterverarbeitet. In Wirtschaft und Verwaltung bestreitet niemand mehr die Notwendigkeit, seine IT-Landschaft angemessen zu schützen. Daneben müssen aber auch Informationen in allen anderen Phasen von Geschäftsprozessen adäquat geschützt werden. Sicherheitsvorfälle wie die Offenlegung oder Manipulation von Informationen können weitreichende geschäftsschädigende Auswirkungen haben oder die Erfüllung von Aufgaben behindern und somit hohe Kosten verursachen.

Die Praxis hat gezeigt, dass eine Optimierung des Sicherheitsmanagements oftmals die Informationssicherheit effektiver und nachhaltiger verbessert als Investitionen in Sicherheitstechnik. Maßnahmen, die ursprünglich zur Verbesserung der Informationssicherheit umgesetzt wurden, können aber auch außerhalb des Sicherheitszusammenhangs positive Auswirkungen haben und sich als gewinnbringend erweisen. Investitionen in Informationssicherheit können in vielen Fällen sogar mittelfristig zu Kosteneinsparungen beitragen. Als positive Nebeneffekte sind eine höhere Arbeitsqualität, Steigerung des Kundenvertrauens, Optimierung der IT-Landschaft und organisatorischer Abläufe sowie die Nutzung von Synergieeffekten durch bessere Integration des Informationssicherheitsmanagements in bestehende Strukturen zu erwarten.

Ein angemessenes Sicherheitsniveau ist in erster Linie abhängig vom systematischen Vorgehen und erst in zweiter Linie von einzelnen technischen Maßnahmen. Die folgenden Überlegungen verdeutlichen diese These:

- Die Leitungsebene trägt die Verantwortung, dass gesetzliche Regelungen und Verträge mit Dritten eingehalten werden und dass wichtige Geschäftsprozesse störungsfrei ablaufen.
- Informationssicherheit hat Schnittstellen zu vielen Bereichen einer Institution und betrifft wesentliche Geschäftsprozesse und Aufgaben. Nur die Leitungsebene kann daher für eine reibungslose Integration des Informationssicherheitsmanagements in bestehende Organisationsstrukturen und Prozesse sorgen.
- Die Leitungsebene ist zudem für den wirtschaftlichen Einsatz von Ressourcen verantwortlich.

Der Leitungsebene kommt daher eine hohe Verantwortung für die Informationssicherheit zu. Fehlende Steuerung, eine ungeeignete Sicherheitsstrategie oder falsche Entscheidungen können sowohl durch Sicherheitsvorfälle als auch durch verpasste Chancen und Fehlinvestitionen weitreichende negative Auswirkungen haben.

Dieser Standard beschreibt daher Schritt für Schritt, was ein erfolgreiches Informationssicherheitsmanagement ausmacht und welche Aufgaben der Leitungsebene in Behörden und Unternehmen dabei zukommen.

## 1.3 Adressatenkreis

Dieses Dokument richtet sich an Verantwortliche für den IT-Betrieb und die Informationssicherheit, Sicherheitsbeauftragte, -experten, -berater und alle Interessierte, die mit dem Management von Informationssicherheit betraut sind.

Das effektive und effiziente Management von Informationssicherheit ist nicht nur für große Institutionen, sondern auch für kleine und mittlere Behörden und Unternehmen sowie Selbständige ein wichtiges Thema. Wie ein geeignetes Managementsystem für Informationssicherheit aussieht, hängt natürlich von der Größe der Institution ab. Dieser Standard und vor allem die sehr konkreten Empfehlungen des IT-Grundschutzes helfen jedem Verantwortlichen, der die Informationssicherheit in seinem Einflussbereich verbessern möchte. Im Folgenden werden immer wieder Hinweise gegeben, wie die Empfehlungen dieses Standards je nach Größe einer Institution bedarfsgerecht angepasst werden können.

## 1.4 Anwendungsweise

Der vorliegende Standard beschreibt, wie ein Informationssicherheitsmanagementsystem (ISMS) aufgebaut werden kann. Ein Managementsystem umfasst alle Regelungen, die für die Steuerung und Lenkung für die Zielerreichung der Institution sorgen. Ein Managementsystem für Informationssicherheit legt somit fest, mit welchen Instrumenten und Methoden die Leitungsebene einer Institution die auf Informationssicherheit ausgerichteten Aufgaben und Aktivitäten nachvollziehbar lenkt.

Dieser BSI-Standard beantwortet unter anderem folgende Fragen:

- Was sind die Erfolgsfaktoren beim Management von Informationssicherheit?
- Wie kann der Sicherheitsprozess vom verantwortlichen Management gesteuert und überwacht werden?
- Wie werden Sicherheitsziele und eine angemessene Sicherheitsstrategie entwickelt?
- Wie werden Sicherheitsmaßnahmen ausgewählt und ein Sicherheitskonzept erstellt?
- Wie kann ein einmal erreichtes Sicherheitsniveau dauerhaft erhalten und verbessert werden?

Dieser Management-Standard stellt kurz und übersichtlich die wichtigsten Aufgaben des Sicherheitsmanagements dar. Bei der Umsetzung dieser Empfehlungen hilft das BSI mit der Methodik des IT-Grundschutzes. Der IT-Grundschutz gibt eine Schritt-für-Schritt-Anleitung für die Entwicklung eines Informationssicherheitsmanagements in der Praxis und nennt sehr konkrete Maßnahmen für alle Aspekte der Informationssicherheit. Die Vorgehensweise nach IT-Grundschutz wird im BSI-Standard 100-2 (siehe [BSI2]) beschrieben und ist so gestaltet, dass möglichst kostengünstig ein angemessenes Sicherheitsniveau erreicht werden kann. Ergänzend dazu werden in den IT-Grundschutz-Katalogen Standard-Sicherheitsmaßnahmen für die praktische Implementierung des angemessenen Sicherheitsniveaus empfohlen.

## 1.5 Literaturverzeichnis

[BSI1] Managementsysteme für Informationssicherheit (ISMS), BSI-Standard 100-1, Version 1.5, Mai 2008, www.bsi.bund.de

[BSI2] IT-Grundschutz-Vorgehensweise, BSI-Standard 100-2, Version 2.0, Mai 2008, www.bsi.bund.de

[BSI3] Risikoanalyse auf der Basis von IT-Grundschutz, BSI-Standard 100-3, Version 2.5, Mai 2008, www.bsi.bund.de

[COBIT] CobiT (Control Objectives for Information and Related Technology), Version 4.1, ISACA, http://www.isaca.org/cobit

[GSK] IT-Grundschutz-Kataloge - Standard-Sicherheitsmaßnahmen, BSI, jährlich neu, http://www.bsi.bund.de/gshb

[ITIL] IT Infrastructure Library, Service Management - ITIL (IT Infrastructure Library) http://www.ogc.gov.uk/guidance_itil.asp, Januar 2008

[OECD] Organisation for Economic Co-operation and Development (OECD), Guidelines for the Security of Information Systems and Networks, 2002, www.oecd.org/sti/security-privacy

[SHB] IT-Sicherheitshandbuch - Handbuch für die sichere Anwendung der Informationstechnik, BSI, Version 1.0 - März 1992, Bundesdruckerei

[ZERT] Zertifizierung nach ISO 27001 auf der Basis von IT-Grundschutz - Prüfschema für ISO 27001-Audits, BSI, Version 1.2, März 2008, www.bsi.bund.de/gshb/zert

[ZERT2] Zertifizierungsschema für Auditteamleiter für ISO 27001-Audits auf der Basis von IT-Grundschutz, BSI, März 2008, www.bsi.bund.de/gshb/zert

[27000] ISO/IEC 27000 (3rd CD, 2008) "Information technology - Security techniques - ISMS – Overview and vocabulary", ISO/IEC JTC1/SC27

[27001] ISO/IEC 27001:2005 "Information technology - Security techniques - Information security management systems requirements specification", ISO/IEC JTC1/SC27

[27002] ISO/IEC 27002:2005 "Information technology - Security techniques - Code of practice for information security management", ISO/IEC JTC1/SC27

[27005] ISO/IEC 27005 (2nd FCD, 2008) "Information technology - Security techniques - Information security risk management", ISO/IEC JTC1/SC27

[27006] ISO/IEC 27006:2007 "Information technology - Security techniques - Requirements for bodies providing audit and certification of information security management systems", ISO/IEC JTC1/SC27

# 2 Einführung in Informationssicherheit

**Was ist Informationssicherheit?**

Informationssicherheit hat als Ziel den Schutz von Informationen jeglicher Art und Herkunft. Dabei können Informationen sowohl auf Papier, in Rechnersystemen oder auch in den Köpfen der Nutzer gespeichert sein. IT-Sicherheit beschäftigt sich an erster Stelle mit dem Schutz elektronisch gespeicherter Informationen und deren Verarbeitung.

Die klassischen Grundwerte der Informationssicherheit sind Vertraulichkeit, Integrität und Verfügbarkeit. Viele Anwender ziehen in ihre Betrachtungen weitere Grundwerte mit ein. Dieses kann je nach den individuellen Anwendungsfällen auch sehr hilfreich sein. Weitere generische Oberbegriffe der Informationssicherheit sind beispielsweise Authentizität, Verbindlichkeit, Zuverlässigkeit und Nichtabstreitbarkeit.

Die Sicherheit von Informationen wird nicht nur durch vorsätzliche Handlungen bedroht (z. B. Computer-Viren, Abhören der Kommunikation, Diebstahl von Rechnern). Die folgenden Beispiele verdeutlichen dies:

- Durch höhere Gewalt (z. B. Feuer, Wasser, Sturm, Erdbeben) werden Datenträger und IT-Systeme in Mitleidenschaft gezogen oder der Zugang zum Rechenzentrum versperrt. Dokumente, IT-Systeme oder Dienste stehen damit nicht mehr wie gewünscht zur Verfügung.
- Nach einem missglückten Software-Update funktionieren Anwendungen nicht mehr oder Daten wurden unbemerkt verändert.
- Ein wichtiger Geschäftsprozess verzögert sich, weil die einzigen Mitarbeiter, die mit der Anwendungssoftware vertraut sind, erkrankt sind.
- Vertrauliche Informationen werden versehentlich von einem Mitarbeiter an Unbefugte weitergegeben, weil Dokumente oder Dateien nicht als "vertraulich" gekennzeichnet waren.

**Wortwahl: IT-Sicherheit versus Informationssicherheit**

In der deutschen Literatur werden die Begriffe "Informationstechnik", "Informations- und Kommunikationstechnik" oder "Informations- und Telekommunikationstechnik" häufig synonym benutzt. Aufgrund der Länge dieser Begriffe haben sich die jeweiligen Abkürzungen eingebürgert, so dass meist von IT gesprochen wird. Da die elektronische Verarbeitung von Informationen in nahezu allen Lebensbereichen allgegenwärtig ist, ist die Unterscheidung, ob Informationen mit Informationstechnik, mit Kommunikationstechnik oder auf Papier verarbeitet werden, nicht mehr zeitgemäß. Der Begriff Informationssicherheit statt IT-Sicherheit ist daher umfassender und besser geeignet. Da aber in der Literatur überwiegend noch der Begriff "IT-Sicherheit" verwendet wird (unter anderem, weil er kürzer ist), wird er auch in dieser Publikation sowie in anderen Publikationen des IT-Grundschutzes weiterhin verwendet, allerdings werden die Texte sukzessive stärker auf die Betrachtung von Informationssicherheit ausgerichtet.

## 2.1 Überblick über Standards zur Informationssicherheit

Im Bereich der Informationssicherheit haben sich verschiedene Standards entwickelt, bei denen teilweise andere Zielgruppen oder Themenbereiche im Vordergrund stehen. Der Einsatz von Sicherheitsstandards in Unternehmen oder Behörden verbessert nicht nur das Sicherheitsniveau, er erleichtert auch die Abstimmung zwischen verschiedenen Institutionen darüber, welche Sicherheitsmaßnahmen in welcher Form umzusetzen sind. Der folgende Überblick zeigt die Ausrichtungen der wichtigsten Standards auf.

### 2.1.1 ISO-Standards zur Informationssicherheit

In den internationalen Normungsorganisationen ISO und IEC wurde beschlossen, die Standards zur Informationssicherheit in der 2700x-Reihe zusammenzuführen, die stetig wächst. Die wesentlichen Standards sind hier:

- ISO 27000

  Dieser Standard gibt einen allgemeinen Überblick über Managementsysteme für Informationssicherheit (ISMS) und über die Zusammenhänge der verschiedenen Standards der ISO-2700x-Familie. Hier finden sich außerdem die grundlegenden Prinzipien, Konzepte, Begriffe und Definitionen für ISMS.

- ISO 27001

  Aufgrund der Komplexität von Informationstechnik und der Nachfrage nach Zertifizierungen sind in den letzten Jahren zahlreiche Anleitungen, Standards und nationale Normen zur Informationssicherheit entstanden. Der ISO-Standard 27001 "Information technology - Security techniques - Information security management systems requirements specification" ist der erste internationale Standard zum Management von Informationssicherheit, der auch eine Zertifizierung ermöglicht. ISO 27001 gibt auf ca. 10 Seiten allgemeine Empfehlungen unter anderem zur Einführung, dem Betrieb und der Verbesserung eines dokumentierten Informationssicherheitsmanagementsystems auch unter Berücksichtigung der Risiken. In einem normativen Anhang wird auf die Controls aus ISO/IEC 27002 verwiesen. Die Leser erhalten allerdings keine Hilfe für die praktische Umsetzung.

- ISO 27002

  Das Ziel von ISO 27002 (bisher ISO 17799:2005) "Information technology – Code of practice for information security management" ist es, ein Rahmenwerk für das Informationssicherheitsmanagement zu definieren. ISO 27002 befasst sich daher hauptsächlich mit den erforderlichen Schritten, um ein funktionierendes Sicherheitsmanagement aufzubauen und in der Organisation zu verankern. Die erforderlichen Sicherheitsmaßnahmen werden auf den circa 100 Seiten des ISO-Standards ISO/IEC 27002 nur kurz beschrieben. Die Empfehlungen sind in erster Linie für die Management-Ebene gedacht und enthalten daher kaum konkrete technische Hinweise. Die Umsetzung der Sicherheitsempfehlungen der ISO 27002 ist eine von vielen Möglichkeiten, die Anforderungen des ISO-Standards 27001 zu erfüllen.

  Hinweis: Der Standard ISO 17799 wurde Anfang des Jahres 2007 ohne weitere inhaltliche Änderungen in die ISO 27002 überführt, um die Zugehörigkeit zur ISO-2700x-Reihe zu unterstreichen.

- ISO 27005

  Dieser ISO-Standard "Information security risk management" enthält Rahmenempfehlungen zum Risikomanagement für Informationssicherheit. Unter anderem unterstützt er bei der Umsetzung der Anforderungen aus ISO/IEC 27001. Hierbei wird allerdings keine spezifische Methode für das Risikomanagement vorgegeben. ISO/IEC 27005 löst den bisherigen Standard ISO 13335-2 ab. Dieser Standard, ISO 13335 "Management of information and communications technology security, Part 2: Techniques for information security risk management", gab Anleitungen zum Management von Informationssicherheit.

- ISO 27006

  Der ISO-Standard 27006 "Information technology - Security techniques - Requirements for the accreditation of bodies providing certification of information security management systems" spezifiziert Anforderungen an die Akkreditierung von Zertifizierungsstellen für ISMS und behandelt auch Spezifika der ISMS-Zertifizierungsprozesse.

- Weitere Standards der ISO-2700x-Reihe

  Die Normenreihe ISO 2700x wird voraussichtlich langfristig aus den ISO-Standards 27000–27019 und 27030–27044 bestehen. Alle Standards dieser Reihe behandeln verschiedene Aspekte des Sicherheitsmanagements und beziehen sich auf die Anforderungen der ISO 27001. Die weiteren Standards sollen zum besseren Verständnis und zur praktischen Anwendbarkeit der ISO 27001 beitragen. Diese beschäftigen sich beispielsweise mit der praktischen Umsetzung der ISO 27001, also der Messbarkeit von Risiken oder mit Methoden zum Risikomanagement.

### 2.1.2 Ausgewählte BSI-Publikationen und Standards zur Informationssicherheit

**IT-Grundschutz-Kataloge**

Die bekannteste Publikation des BSI zur Informationssicherheit war bis 2005 das IT-Grundschutzhandbuch, das seit 1994 sehr ausführlich nicht nur das Management von Informationssicherheit, sondern auch detailliert Sicherheitsmaßnahmen aus den Bereichen Technik, Organisation, Personal und Infrastruktur beschrieb. Das IT-Grundschutzhandbuch ist 2005 nicht nur aktualisiert, sondern auch umstrukturiert worden. Dabei sind die Beschreibung der Vorgehensweise nach IT-Grundschutz und die IT-Grundschutz-Kataloge voneinander getrennt worden.

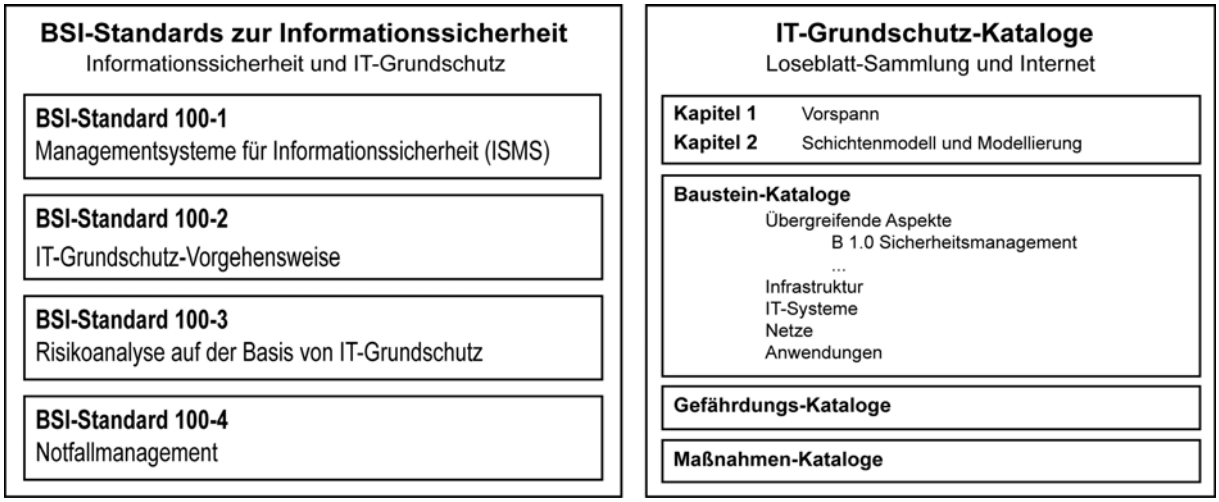



Abbildung 1: Übersicht über BSI-Publikationen zum Sicherheitsmanagement

Die IT-Grundschutz-Kataloge sind modular aufgebaut und enthalten für typische Prozesse, Anwendungen und IT-Komponenten Bausteine. Zu jedem Thema werden nicht nur Sicherheitsmaßnahmen empfohlen, sondern auch die wichtigsten Gefährdungen beschrieben, vor denen sich eine Institution schützen sollte. Anwender können sich somit gezielt auf die Bausteine konzentrieren, die tatsächlich für ihren Bereich relevant sind. Die Bausteine der IT-Grundschutz-Kataloge werden regelmäßig aktualisiert und erweitert und dabei auch neue technische Entwicklungen berücksichtigt. Daher werden sie als Loseblatt-Sammlung, auf CD bzw. DVD und außerdem im Internet veröffentlicht. Die IT-Grundschutz-Vorgehensweise beschreibt, wie auf der Basis von Standard-Sicherheitsmaßnahmen Sicherheitslösungen ausgewählt, aufgebaut und geprüft werden können. Diese Methode ist als BSI-Standard 100-2 in der Standardreihe des BSI zur Informationssicherheit veröffentlicht worden.

**BSI-Standardreihe zur Informationssicherheit: Thema IS-Management**

100-1 Managementsysteme für Informationssicherheit (ISMS)

Der vorliegende Standard definiert allgemeine Anforderungen an ein ISMS. Er ist vollständig kompatibel zum ISO-Standard 27001 und berücksichtigt weiterhin die Empfehlungen der ISO-Standards 27000 und 27002. Er bietet Lesern eine leicht verständliche und systematische Anleitung, unabhängig davon, mit welcher Methode sie die Anforderungen umsetzen möchten.

Das BSI stellt den Inhalt dieser ISO-Standards in einem eigenen BSI-Standard dar, um einige Themen ausführlicher beschreiben zu können und so eine didaktischere Darstellung der Inhalte zu ermöglichen. Zudem wurde die Gliederung so gestaltet, dass sie mit der IT-Grundschutz-Vorgehensweise kompatibel ist. Durch die einheitlichen Überschriften in den zuvor genannten Dokumenten ist eine Orientierung für die Leser sehr einfach möglich.

100-2 IT-Grundschutz-Vorgehensweise

Die IT-Grundschutz-Vorgehensweise beschreibt Schritt für Schritt, wie ein Managementsystem für Informationssicherheit in der Praxis aufgebaut und betrieben werden kann. Die Aufgaben des

Informationssicherheitsmanagements und der Aufbau einer Organisationsstruktur für Informationssicherheit sind dabei wichtige Themen. Die IT-Grundschutz-Vorgehensweise geht sehr ausführlich darauf ein, wie ein Sicherheitskonzept in der Praxis erstellt werden kann, wie angemessene Sicherheitsmaßnahmen ausgewählt werden können und was bei der Umsetzung des Sicherheitskonzeptes zu beachten ist. Auch die Frage, wie die Informationssicherheit im laufenden Betrieb aufrechterhalten und verbessert werden kann, wird ausführlich beantwortet.

IT-Grundschutz in Verbindung mit dem BSI-Standard 100-2 interpretiert damit die sehr allgemein gehaltenen Anforderungen der zuvor genannten ISO-Standards 27000, 27001 und 27002 und hilft den Anwendern in der Praxis bei der Umsetzung mit vielen Hinweisen, Hintergrund-Informationen und Beispielen. Die IT-Grundschutz-Kataloge erklären nicht nur, *was* gemacht werden sollte, sondern geben sehr konkrete Hinweise, *wie* eine Umsetzung (auch auf technischer Ebene) aussehen kann. Ein Vorgehen nach IT-Grundschutz ist somit eine erprobte und effiziente Möglichkeit, allen Anforderungen der oben genannten ISO-Standards nachzukommen.

100-3 Risikoanalyse auf der Basis von IT-Grundschutz

Das BSI hat eine Methodik zur Risikoanalyse auf der Basis des IT-Grundschutzes erarbeitet. Diese Vorgehensweise bietet sich an, wenn Unternehmen oder Behörden bereits erfolgreich mit dem IT-Grundschutz arbeiten und möglichst nahtlos eine ergänzende Sicherheitsanalyse an die IT-Grundschutz-Analyse anschließen möchten.

100-4 Notfallmanagement

Im BSI-Standard 100-4 wird eine Methodik zur Etablierung und Aufrechterhaltung eines behörden- bzw. unternehmensweiten Notfallmanagements erläutert. Die hier beschriebene Methodik baut dabei auf der in BSI-Standard 100-2 beschriebenen IT-Grundschutz-Vorgehensweise auf und ergänzt diese sinnvoll.

**ISO 27001 Zertifizierung auf der Basis von IT-Grundschutz**

Das BSI zertifiziert Informationsverbünde, also das Zusammenspiel von infrastrukturellen, organisatorischen, personellen und technischen Komponenten, die zur Umsetzung von Geschäftsprozessen und Fachaufgaben dienen. Die BSI-Zertifizierung umfasst sowohl eine Prüfung des Managementsystems für Informationssicherheit als auch die Prüfung der konkreten Sicherheitsmaßnahmen auf Basis von IT-Grundschutz. Die BSI-Zertifizierung beinhaltet dabei immer eine offizielle ISO-Zertifizierung nach ISO 27001, ist aber aufgrund der zusätzlich geprüften technischen Aspekte wesentlich aussagekräftiger als eine reine ISO-Zertifizierung. Die wesentlichen Anforderungen zur Prüfung des Sicherheitsmanagements im Rahmen eines Audits ergeben sich aus den Maßnahmen des Grundschutz-Bausteins B 1.0 Sicherheitsmanagement. Die Maßnahmen dieses Bausteins sind so geschrieben, dass die wesentlichen Anforderungen des BSI-Standards für Informationssicherheitsmanagementsysteme sofort identifiziert werden können. Abbildung 1 veranschaulicht die einheitliche Gliederung der BSI-Dokumente.

Zur Anpassung an ISO 27001 wurden auch Anpassungen am Zertifizierungsschema für Informationsverbünde und am Zertifizierungsschema für Auditoren vorgenommen (siehe [ZERT] bzw. [ZERT2]).

### 2.1.3 Weitere Standards

**COBIT**

COBIT (Control Objectives for Information and related Technology) beschreibt eine Methode zur Kontrolle von Risiken, die sich durch den IT-Einsatz zur Unterstützung geschäftsrelevanter Abläufe ergeben. Die COBIT-Dokumente werden herausgegeben vom IT Governance Institute (ITGI) der Information Systems Audit and Control Association (ISACA). Bei der Entwicklung von COBIT orientierten sich die Autoren an bestehenden Standards zum Thema Sicherheitsmanagement wie ISO 27002.

**ITIL**

Die IT Infrastructure Library (ITIL) ist eine Sammlung mehrerer Bücher zum Thema IT-Service-Management. Sie wurde vom United Kingdom's Office Of Government Commerce (OGC) entwickelt. ITIL befasst sich mit dem Management von IT-Services aus Sicht des IT-Dienstleisters. Der IT-Dienstleister kann dabei sowohl eine interne IT-Abteilung als auch ein externer Service-Provider sein. Übergreifendes Ziel ist die Optimierung beziehungswweise Verbesserung der Qualität von IT-Services und der Kosteneffizienz.

# 3 ISMS-Definition und Prozessbeschreibung

## 3.1 Komponenten eines Managementsystems für Informationssicherheit

Jedes Unternehmen und jede Behörde hat ein Management, das im Folgenden mit "Leitungsebene" bezeichnet wird, wenn die verantwortlichen Führungskräfte gemeint sind und Verwechslungsgefahr zum "Management" als Leitungsprozess (Leiten, Lenken und Planen) besteht.

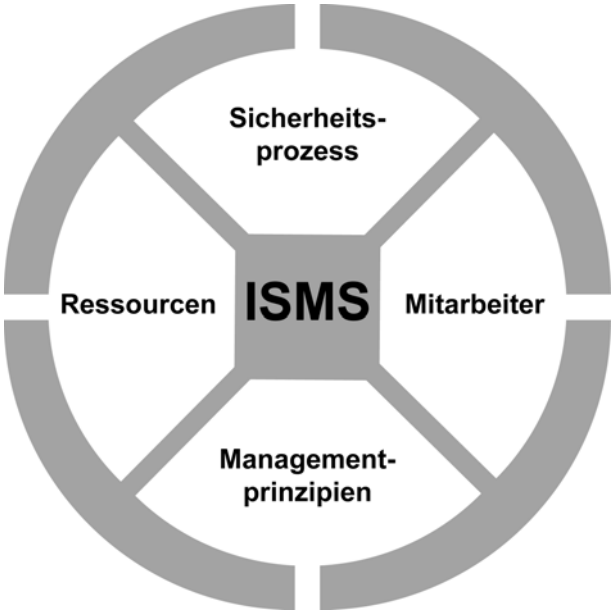



Abbildung 2: Bestandteile eines Managementsystems für Informationssicherheit (ISMS)

Ein Managementsystem umfasst alle Regelungen, die für die Steuerung und Lenkung zur Zielerreichung der Institution sorgen. Der Teil des Managementsystems, der sich mit Informationssicherheit beschäftigt, wird als Informationssicherheitsmanagementsystem (ISMS) bezeichnet. Das ISMS legt fest, mit welchen Instrumenten und Methoden das Management die auf Informationssicherheit ausgerichteten Aufgaben und Aktivitäten nachvollziehbar lenkt (plant, einsetzt, durchführt, überwacht und verbessert). Zu einem ISMS gehören folgende grundlegende Komponenten (siehe Abbildung 2):

- Management-Prinzipien
- Ressourcen
- Mitarbeiter
- Sicherheitsprozess
  - Leitlinie zur Informationssicherheit, in der die Sicherheitsziele und die Strategie zu ihrer Umsetzung dokumentiert sind
  - Sicherheitskonzept
  - Informationssicherheitsorganisation


Abbildung 3: Strategie zur Informationssicherheit als zentrale Komponente des ISMS

Informationssicherheitsorganisation und Sicherheitskonzept sind dabei die Werkzeuge des Managements zur Umsetzung ihrer Sicherheitsstrategie. Abbildung 3 und Abbildung 4 machen diesen Zusammenhang deutlich. Die Kernpunkte der Sicherheitsstrategie werden in der Leitlinie zur Informationssicherheit dokumentiert. Die Sicherheitsleitlinie ist von zentraler Bedeutung, da sie das sichtbare Bekenntnis der Leitungsebene zu ihrer Strategie enthält.


Abbildung 4: Umsetzung der Sicherheitsstrategie mit Hilfe des Sicherheitskonzeptes und einer Informationssicherheitsorganisation

## 3.2 Prozessbeschreibung und Lebenszyklus-Modell

### 3.2.1 Der Lebenszyklus in der Informationssicherheit

Sicherheit ist kein unveränderbarer Zustand, der einmal erreicht wird und sich niemals wieder ändert. Jede Institution ist ständigen dynamischen Veränderungen unterworfen. Viele dieser Veränderungen betreffen über Änderungen der Geschäftsprozesse, Fachaufgaben, Infrastruktur, Organisationsstrukturen und der IT auch die Informationssicherheit. Neben den unübersehbaren Änderungen innerhalb einer Institution können sich außerdem externe Rahmenbedingungen ändern, z. B. gesetzliche oder vertragliche Vorgaben, aber auch die verfügbare Informations- oder

Kommunikationstechnik kann sich einschneidend ändern. Daher ist es notwendig, Sicherheit aktiv zu managen, um ein einmal erreichtes Sicherheitsniveau dauerhaft aufrechtzuerhalten.

Es reicht beispielsweise nicht aus, die Umsetzung von Geschäftsprozessen oder die Einführung eines neuen IT-Systems nur einmalig zu planen und die beschlossenen Sicherheitsmaßnahmen umzusetzen. Nach der Umsetzung müssen die Sicherheitsmaßnahmen regelmäßig auf Wirksamkeit und Angemessenheit, aber auch deren Anwendbarkeit und die tatsächliche Anwendung untersucht werden. Finden sich Schwachpunkte oder Verbesserungsmöglichkeiten, müssen die Maßnahmen angepasst und verbessert werden. Diese durch die notwendigen Anpassungen erforderlichen Änderungen müssen erneut geplant und umgesetzt werden. Werden Geschäftsprozesse beendet oder Komponenten bzw. IT-Systeme ersetzt oder außer Betrieb gestellt, sind auch dabei Sicherheitsaspekte zu beachten (z. B. Entzug von Berechtigungen oder sicheres Löschen von Festplatten). In den IT-Grundschutz-Katalogen werden die Sicherheitsmaßnahmen daher zur besseren Übersicht für die Leser in folgende Phasen eingeteilt:

- Planung und Konzeption,
- Beschaffung (falls erforderlich),
- Umsetzung,
- Betrieb (Maßnahmen zur Aufrechterhaltung der Informationssicherheit im Betrieb, dazu gehört auch die Überwachung und Erfolgskontrolle),
- Aussonderung (falls erforderlich) und
- Notfallvorsorge.

### 3.2.2 Beschreibung des Prozesses Informationssicherheit

Nicht nur Geschäftsprozesse und IT-Systeme haben einen solchen "Lebenszyklus". Auch ein Sicherheitskonzept, eine Informationssicherheitsorganisation und letztendlich der gesamte Sicherheitsprozess unterliegt einem Lebenszyklus. Um die Dynamik des Sicherheitsprozesses möglichst einfach beschreiben zu können, wird der Sicherheitsprozess in der Literatur häufig in die folgenden Phasen eingeteilt:

1. Planung,
2. Umsetzung der Planung bzw. Durchführung des Vorhabens,
3. Erfolgskontrolle bzw. Überwachung der Zielerreichung und
4. Beseitigung von erkannten Mängeln und Schwächen bzw. Optimierung sowie Verbesserung.

Phase 4 beschreibt die umgehende Beseitigung kleinerer Mängel. Bei grundlegenden oder umfangreichen Veränderungen ist natürlich wieder mit der Planungsphase zu beginnen.

Dieses Modell wird nach der englischen Benennung der einzelnen Phasen ("Plan", "Do", "Check", "Act") auch als PDCA-Modell bezeichnet.

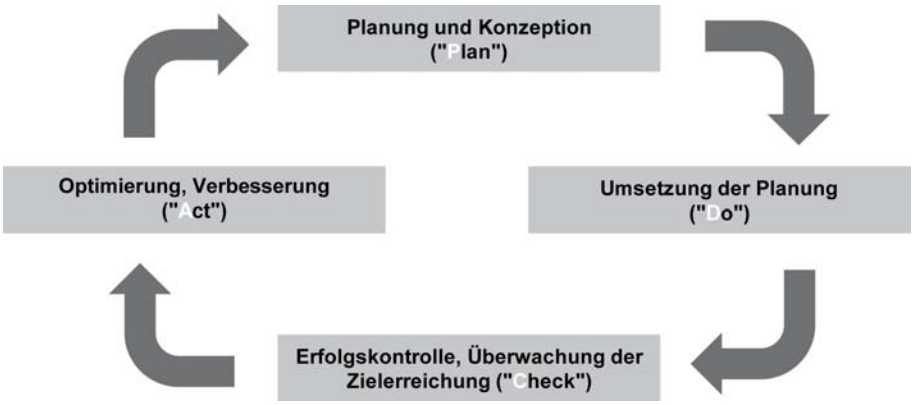



Abbildung 5: Lebenszyklus nach Deming (PDCA-Modell)

Das PDCA-Modell findet sich auch im ISO-Standard 27001. Es lässt sich prinzipiell auf alle Aufgaben innerhalb des Sicherheitsprozesses anwenden. Auch der Lebenszyklus des Sicherheitskonzepts und der Informationssicherheitsorganisation lässt sich so sehr übersichtlich beschreiben. Die entsprechenden Kapitel dieses Dokuments sind daher an die vier Phasen dieses Lebenszyklus-Modells angelehnt.

In der Planungsphase des Prozesses Informationssicherheit werden die Rahmenbedingungen analysiert, die Sicherheitsziele bestimmt und eine Sicherheitsstrategie ausgearbeitet, die grundlegende Aussagen enthält, wie die gesetzten Ziele erreicht werden sollen. Umgesetzt wird die Sicherheitsstrategie mit Hilfe des Sicherheitskonzepts und einer geeigneten Struktur für die Informationssicherheitsorganisation. Sicherheitskonzept und Informationssicherheitsorganisation müssen dann wiederum geplant und umgesetzt sowie einer Erfolgskontrolle unterzogen werden. Bei der Erfolgskontrolle des übergeordneten Sicherheitsprozesses wird dann regelmäßig überprüft, ob sich Rahmenbedingungen (zum Beispiel Gesetze oder Unternehmensziele) geändert haben und ob Sicherheitskonzept und Informationssicherheitsorganisation sich als wirksam und effizient erwiesen haben.

Da unterschiedliche Institutionen jedoch verschiedene Ausgangsbedingungen, Sicherheitsanforderungen und finanzielle Mittel haben, bietet diese Vorgehensweise zwar eine gute Orientierung, muss aber von jeder Behörde und jedem Unternehmen auf die eigenen Bedürfnisse angepasst werden. Jede Institution muss individuell festlegen oder konkretisieren, welche Ausprägung eines Lebenszyklus-Modells für sie angemessen ist.

Kleine Behörden und Unternehmen sollten sich hier nicht abschrecken lassen, da der Aufwand für den Sicherheitsprozess in der Regel von der Größe der Institution abhängt. So ist in einem sehr großen Unternehmen mit vielen beteiligten Abteilungen und Personen wahrscheinlich ein eher formaler Prozess notwendig, der genau festlegt, welche internen und externen Audits notwendig sind, wer an wen berichtet, wer Entscheidungsvorlagen erstellt, und wann die Leitung über den Sicherheitsprozess berät. In einem kleinen Unternehmen hingegen kann eine jährliche Besprechung zwischen dem Geschäftsführer und seinem IT-Dienstleister, in der über Probleme während des letzten Jahres, die entstandenen Kosten, neue technische Entwicklungen und andere Faktoren beraten wird, bereits angemessen sein, um den Erfolg des Sicherheitsprozesses kritisch zu hinterfragen.

# 4 Management-Prinzipien

Mit Informationssicherheitsmanagement oder kurz IS-Management wird die Planungs- und Lenkungsaufgabe bezeichnet, die zum sinnvollen Aufbau, zur praktischen Umsetzbarkeit und zur Sicherstellung der Effektivität eines durchdachten und planmäßigen Sicherheitsprozesses sowie aller dafür erforderlichen Sicherheitsmaßnahmen erforderlich ist. Dies umfasst auch die Erfüllung gesetzlicher Anforderungen und die Einhaltung aller relevanten Rechtsvorschriften. Es gibt verschiedene Konzepte, wie ein effizientes IS-Management aussehen kann und welche Organisationsstrukturen dafür sinnvoll sind. Unabhängig davon, wie die Ausprägung eines IS-Managementsystems aussieht, sind dafür einige grundlegende Prinzipien zu beachten.

Einige der hier vorgestellten Management-Prinzipien mögen banal klingen, ihre Umsetzung werden die meisten Führungskräfte als Selbstverständlichkeit ansehen. Paradoxerweise sind es aber gerade immer wieder die einfachen Dinge, die in der Praxis falsch gemacht oder unterlassen werden. Disziplin, Geduld, Übernahme von Verantwortung sowie realistische und sorgfältige Vorbereitung von Projekten sind in vielen Organisationen zwar theoretisch anerkannte Werte, werden aber in der Praxis nicht immer gelebt. Gerade wenig spektakuläre Maßnahmen wie Prozessoptimierung, Ausbildung und Motivation von Mitarbeitern oder das Anfertigen von verständlichen Dokumentationen verbessern das Sicherheitsniveau in der Praxis sehr deutlich. Komplexe und dadurch teure Maßnahmen, Großprojekte und Investitionen in Technik werden oftmals völlig zu Unrecht als wirksamer dargestellt und sind häufig für den schlechten Ruf von Sicherheitsmaßnahmen als Kostentreiber verantwortlich. Im Folgenden werden daher Management-Prinzipien vorgestellt, deren Beachtung eine gute Grundlage für ein erfolgreiches Informationssicherheitsmanagement ist.

## 4.1 Aufgaben und Pflichten des Managements

Die Aufgaben und Pflichten der Leitungsebene bezüglich Informationssicherheit lassen sich in folgenden Punkten zusammenfassen:

1. Übernahme der Gesamtverantwortung für Informationssicherheit

   Die oberste Managementebene jeder Behörde und jedes Unternehmens ist für das zielgerichtete und ordnungsgemäße Funktionieren der Institution verantwortlich und damit auch für die Gewährleistung der Informationssicherheit nach innen und außen. Dies kann auch je nach Land und nach Organisationsform in verschiedenen Gesetzen geregelt sein. Die Leitungsebene, aber auch jede einzelne Führungskraft, muss sich sichtbar zu ihrer Verantwortung bekennen und allen Mitarbeitern die Bedeutung der Informationssicherheit klar machen.

2. Informationssicherheit integrieren

   Informationssicherheit muss in alle Prozesse und Projekte der Institution integriert werden, bei denen Informationen verarbeitet und IT genutzt werden. Das heißt beispielsweise, dass Sicherheitsanforderungen nicht nur bei der Beschaffung von IT, sondern auch beim Design von Geschäftsprozessen mit zu berücksichtigen sind, ebenso wie bei der Ausbildung von Mitarbeitern.

3. Informationssicherheit steuern und aufrechterhalten

   Die Leitungsebene muss aktiv den Sicherheitsprozess initiieren, steuern und überwachen. Dazu gehören zum Beispiel folgende Aufgaben:

   - Eine Strategie zur Informationssicherheit sowie Sicherheitsziele müssen verabschiedet werden.
   - Die Auswirkungen von Sicherheitsrisiken auf die Geschäftstätigkeit bzw. Aufgabenerfüllung müssen untersucht werden.
   - Es müssen die organisatorischen Rahmenbedingungen für Informationssicherheit geschaffen werden.
   - Für Informationssicherheit müssen ausreichende Ressourcen bereitgestellt werden.

- Die Sicherheitsstrategie muss regelmäßig überprüft und die Zielerreichung überwacht werden. Erkannte Schwachpunkte und Fehler müssen korrigiert werden. Dazu muss ein "innovationsfreudiges" Arbeitsklima geschaffen und der Wille zur ständigen Verbesserung innerhalb der Institution demonstriert werden.
- Mitarbeiter müssen für Sicherheitsbelange motiviert werden und Informationssicherheit als wichtigen Aspekt ihrer Aufgaben betrachten. Hierfür sind unter anderem ausreichende Schulungs- und Sensibilisierungsmaßnahmen anzubieten.

4. Erreichbare Ziele setzen

   Projekte scheitern oft an unrealistischen oder zu ehrgeizigen Zielvorgaben. Dies ist im Bereich Informationssicherheit auch nicht anders. Daher muss die Sicherheitsstrategie mit den zur Verfügung stehenden Ressourcen in Einklang stehen. Um das angemessene Sicherheitsziel zu erreichen, können viele kleine Schritte und ein langfristiger, kontinuierlicher Verbesserungsprozess ohne hohe Investitionskosten zu Beginn effizienter als ein groß angelegtes Projekt sein. So kann es zweckmäßig sein, zunächst nur in ausgewählten Bereichen das erforderliche Sicherheitsniveau umzusetzen. Von diesen Keimzellen ausgehend muss dann aber die Sicherheit in der Institution zügig auf das angestrebte Niveau gebracht werden.

5. Sicherheitskosten gegen Nutzen abwägen

   Eine der schwierigsten Aufgaben ist es, die Kosten für Informationssicherheit gegenüber dem Nutzen und den Risiken abzuwägen. Es ist sehr wichtig, zunächst in Maßnahmen zu investieren, die besonders effektiv sind oder gegen besonders hohe Risiken schützen. Die effektivsten Maßnahmen sind dabei erfahrungsgemäß nicht immer die teuersten. Es ist daher unerlässlich, die Abhängigkeit der Geschäftsprozesse und Aufgaben von der Informationsverarbeitung zu kennen, um angemessene Sicherheitsmaßnahmen auswählen zu können.

   Dabei ist zu betonen, dass Informationssicherheit immer durch ein Zusammenspiel von technischen und organisatorischen Maßnahmen erreicht wird. Die Investitionen in Technik sind unmittelbar am Budget ablesbar. Damit diese Kosten gerechtfertigt sind, müssen die Sicherheitsprodukte so eingesetzt werden, dass sie optimalen Nutzen bieten. Dafür müssen sie aber auch zweckgerichtet ausgewählt worden sein und geeignet bedient werden, also beispielsweise müssen sie in die ganzheitliche Sicherheitskonzeption integriert sein und die Mitarbeiter in deren Nutzung geschult sein. Häufig können technische Lösungen auch durch organisatorische Sicherheitsmaßnahmen ersetzt werden. Erfahrungsgemäß ist es aber schwieriger sicherzustellen, dass organisatorische Maßnahmen konsequent umgesetzt werden. Außerdem steigt dadurch der personelle Aufwand und belastet somit auch die Ressourcen.

6. Vorbildfunktion

   Die Leitungsebene muss auch im Bereich der Informationssicherheit eine Vorbildfunktion übernehmen. Dazu gehört unter anderem, dass auch die Leitungsebene alle vorgegebenen Sicherheitsregeln beachtet und selbst an Schulungsveranstaltungen teilnimmt.

## 4.2 Aufrechterhaltung der Informationssicherheit und kontinuierliche Verbesserung

Die Schaffung von Informationssicherheit ist kein zeitlich begrenztes Projekt, sondern ein kontinuierlicher Prozess. Die Angemessenheit und Wirksamkeit aller Elemente des Managementsystems für Informationssicherheit muss ständig überprüft werden. Das bedeutet, dass nicht nur einzelne Sicherheitsmaßnahmen überprüft werden müssen, sondern auch die Sicherheitsstrategie regelmäßig überdacht werden muss.

Die Umsetzung der Sicherheitsmaßnahmen sollte in regelmäßigen Abständen mit Hilfe von internen Audits ausgewertet werden. Diese dienen auch dazu, die Erfahrungen aus der täglichen Praxis zusammenzutragen und auszuwerten. Neben Audits ist die Durchführung von Übungen und Sensibilisierungsmaßnahmen notwendig, da nur so festgestellt werden kann, ob alle vorgesehenen Abläufe und

das Verhalten in Notfallsituationen auch tatsächlich funktionieren. Erkenntnisse über Schwachstellen und Verbesserungsmöglichkeiten müssen ohne Ausnahme zu Konsequenzen in der Informationssicherheitsorganisation führen. Wichtig ist es außerdem, zukünftige Entwicklungen sowohl bei der eingesetzten Technik als auch in Geschäftsprozessen und Organisationsstrukturen frühzeitig zu erkennen, um rechtzeitig potentielle Gefährdungen identifizieren, Vorkehrungen treffen und Sicherheitsmaßnahmen umsetzen zu können. Wenn sich wesentliche Änderungen in Geschäftsprozessen oder Organisationsstrukturen abzeichnen, muss hier das Informationssicherheitsmanagement eingebunden werden. Auch wenn dies genau so in den Organisationsverfügungen vorgesehen ist, sollte es nicht darauf warten, dass es wie geplant involviert wird, sondern sollte sich rechtzeitig eigenständig in die entsprechenden Prozesse einbinden.

Bei allen Audits sollte darauf geachtet werden, dass sie nicht von denjenigen durchgeführt werden, die an der Planung oder Konzeption von Sicherheitsvorgaben beteiligt waren, da es schwierig ist, eigene Fehler zu finden. Je nach Größe der Institution kann es hilfreich sein, für Audits Externe hinzuzuziehen, um Betriebsblindheit zu vermeiden.

Auch für kleine und mittlere Behörden und Unternehmen ist die Aufrechterhaltung der Informationssicherheit ein wichtiger Punkt. Die Audits werden zwar weniger umfangreich als in großen Institutionen sein, dürfen aber auf keinen Fall unterbleiben. Im Rahmen der jährlichen Managementbewertung muss von der obersten Leitungsebene auch überprüft werden, ob es neue gesetzliche Vorgaben gibt, die beachtet werden müssen, oder ob sich sonstige Rahmenbedingungen geändert haben.

Die Überprüfung des Sicherheitsprozesses dient letztendlich dessen Verbesserung. Die Ergebnisse sollten daher dazu genutzt werden, die Wirksamkeit und Effizienz der gewählten Sicherheitsstrategie zu beurteilen und eventuell anzupassen. Auch bei Veränderung der Sicherheitsziele oder der Rahmenbedingungen muss die Sicherheitsstrategie entsprechend überarbeitet werden. Dieses Thema wird detailliert in Kapitel 7 dieses Standards behandelt.

## 4.3 Kommunikation und Wissen

In allen Phasen des Sicherheitsprozesses ist Kommunikation ein wesentlicher Eckpfeiler, um die gesteckten Sicherheitsziele zu erreichen. Missverständnisse und Wissensmängel sind mit die häufigsten Ursachen für auftretende Sicherheitsprobleme. Daher muss auf allen Ebenen und in allen Bereichen einer Institution für einen reibungslosen Informationsfluss über Sicherheitsvorkommnisse und -maßnahmen gesorgt werden. Dazu gehören die folgenden Punkte:

- Berichte an die Leitungsebene

  Das obere Management muss sich regelmäßig über Probleme, Ergebnisse von Überprüfungen und Audits, aber auch über neue Entwicklungen, geänderte Rahmenbedingungen oder Verbesserungsmöglichkeiten informieren lassen, um seiner Steuerungsfunktion nachkommen zu können.

- Informationsfluss

  Durch mangelhafte Kommunikation und fehlende Informationen kann es zu Sicherheitsproblemen, aber auch zu Fehlentscheidungen oder überflüssigen Arbeitsschritten kommen. Dies muss durch geeignete Maßnahmen und organisatorische Regelungen vermieden werden. Mitarbeiter müssen über Sinn und Zweck von Sicherheitsmaßnahmen aufgeklärt werden, vor allem, wenn diese zusätzliche Arbeit verursachen oder Komforteinbußen zur Folge haben. Des Weiteren sollten Mitarbeiter über die mit ihrer Arbeit verbundenen Rechtsfragen zu Informationssicherheit wie auch zu Datenschutz aufgeklärt werden. Anwender sollten außerdem in die Umsetzungsplanung von Maßnahmen einbezogen werden, um eigene Ideen einzubringen und die Praxistauglichkeit zu beurteilen.

- Dokumentation

  Um die Kontinuität und Konsistenz des gesamten Sicherheitsprozesses sicherzustellen, ist es unabdingbar, diesen zu dokumentieren. Nur so bleiben die verschiedenen Prozessschritte und

Entscheidungen nachvollziehbar. Außerdem stellen aussagekräftige Dokumentationen sicher, dass gleichartige Arbeiten auf vergleichbare Weise durchgeführt werden, also Prozesse messbar und wiederholbar werden. Zusätzlich helfen Dokumentationen dabei, grundsätzliche Schwächen im Prozess zu erkennen und die Wiederholung von Fehlern zu vermeiden. Die erforderlichen Dokumentationen erfüllen bei den verschiedenen Sicherheitsaktivitäten unterschiedliche Funktionen und sind an unterschiedliche Zielgruppen gerichtet. Folgende Dokumentationsarten lassen sich unterscheiden:

1. Technische Dokumentation und Dokumentation von Arbeitsabläufen (Zielgruppe: Experten)

   Es muss bei Störungen oder Sicherheitsvorfällen möglich sein, den gewünschten Soll-Zustand in Geschäftsprozessen sowie der zugehörigen IT wiederherstellen zu können. Technische Einzelheiten und Arbeitsabläufe sind daher so zu dokumentieren, dass dies in angemessener Zeit möglich ist.

   Beispiele hierfür sind Anleitungen zur Installation von IT-Anwendungen, zur Durchführung von Datensicherungen, zum Rückspielen einer Datensicherung, zur Konfiguration der TK-Anlage, zum Wiederanlauf eines Anwendungsservers nach einem Stromausfall, ebenso wie die Dokumentation von Test- und Freigabeverfahren und Anweisungen für das Verhalten bei Störungen und Sicherheitsvorfällen.

2. Anleitungen für IT-Anwender (Zielgruppe: IT-Anwender)

   Arbeitsabläufe, organisatorische Vorgaben und technische Sicherheitsmaßnahmen müssen so dokumentiert werden, dass Sicherheitsvorfälle durch Unkenntnis oder Fehlhandlungen vermieden werden. Beispiele hierfür sind Sicherheitsrichtlinien für die Nutzung von E-Mail und Internet, Hinweise zur Verhinderung von Virenvorfällen oder zum Erkennen von Social Engineering sowie Verhaltensregeln für Benutzer beim Verdacht eines Sicherheitsvorfalls.

3. Reporte für Managementaufgaben (Zielgruppe: Leitungsebene, Sicherheitsmanagement)

   Alle Informationen, die das Management benötigt, um seinen Lenkungs- und Steuerungsaufgaben nachkommen zu können, sind im erforderlichen Detaillierungsgrad aufzuzeichnen (zum Beispiel Ergebnisse von Audits, Effektivitätsmessungen, Berichte über Sicherheitsvorfälle).

4. Aufzeichnung von Managemententscheidungen (Zielgruppe: Leitungsebene)

   Die Leitungsebene muss die gewählte Sicherheitsstrategie aufzeichnen und begründen. Außerdem müssen auch auf allen anderen Ebenen Entscheidungen, die sicherheitsrelevante Aspekte betreffen, ebenso aufgezeichnet werden, damit diese jederzeit nachvollziehbar und wiederholbar sind.

   In den folgenden Kapiteln ist daher jede Aktion, die geeignet dokumentiert bzw. aufgezeichnet werden muss, mit "[DOK]" gekennzeichnet.

- Formale Anforderungen an Dokumentationen:

  Dokumentationen müssen nicht zwingend in Papierform vorliegen. Das Dokumentationsmedium sollte je nach Bedarf gewählt werden. Beispielsweise kann für das Notfallmanagement der Einsatz eines Softwaretools hilfreich sein, mit dem vorab alle Notfallmaßnahmen und Ansprechpartner erfasst werden und das im Krisenfall mobil eingesetzt werden kann. Dann muss natürlich auch im Notfall dieses Tool, alle erforderlichen Informationen und die benötigten IT-Systeme verfügbar sein, beispielsweise auf einem Laptop. Je nach Krisenfall kann es aber sinnvoller sein, alle Informationen in einem praktischen Handbuch in Papierform griffbereit zu haben.

  Es kann gesetzliche oder vertragliche Anforderungen an Dokumentationen geben, die zu beachten sind, z. B. zu Aufbewahrungsfristen und Detaillierungstiefe. Dokumentationen erfüllen nur dann ihren Zweck, wenn sie regelmäßig erstellt und aktuell gehalten werden. Außerdem müssen sie so bezeichnet und abgelegt werden, dass sie im Bedarfsfall auch nutzbar sind. Es muss klar erkennbar sein, wer wann welche Teile der Dokumentation erstellt hat. Dort, wo auf andere Dokumente

verwiesen wird, müssen die Quellen beschrieben sein. Weiterführende Dokumente müssen außerdem im Bedarfsfall ebenfalls verfügbar sein.

Sicherheitsrelevante Dokumentationen können schutzbedürftige Informationen enthalten und müssen daher angemessen geschützt werden. Neben dem Schutzbedarf müssen die Aufbewahrungsart und -dauer und Optionen für die Vernichtung von Informationen festgelegt werden. In den Prozessbeschreibungen muss beschrieben sein, ob und wie Dokumentationen auszuwerten sind.

- Nutzung verfügbarer Informationsquellen und Erfahrungen

  Informationssicherheit ist ein komplexes Thema, so dass die hierfür Verantwortlichen sich sorgfältig einarbeiten müssen. Es gibt eine Vielzahl verfügbarer Informationsquellen, die dazu genutzt werden können. Hierzu gehören unter anderem bestehende Normen und Standards, Internet-Veröffentlichungen und sonstige Publikationen. Außerdem sollte die Kooperation mit Verbänden, Partnern, Gremien, anderen Unternehmen oder Behörden sowie CERTs zum Erfahrungsaustausch über erfolgreiche Sicherheitsaktionen genutzt werden. Da das Thema Informationssicherheit sehr umfangreich ist, ist es wichtig, die für die jeweilige Institution und Rahmenbedingungen passenden Informationsquellen und Kooperationspartner zu identifizieren und zu dokumentieren.

# 5 Ressourcen für Informationssicherheit

Die Einhaltung eines bestimmten Sicherheitsniveaus erfordert immer finanzielle, personelle und zeitliche Ressourcen, die von der Leitungsebene ausreichend bereitgestellt werden müssen. Wenn Zielvorgaben aufgrund fehlender Ressourcen nicht erreichbar sind, sind hierfür nicht die mit der Umsetzung betrauten Personen verantwortlich, sondern die Vorgesetzten, die unrealistische Ziele gesetzt bzw. die erforderlichen Ressourcen nicht bereitgestellt haben. Um die gesetzten Ziele nicht zu verfehlen, ist es wichtig, schon bei der Festlegung der Ziele eine erste Kosten-Nutzen-Schätzung durchzuführen. Im Laufe des Sicherheitsprozesses sollte dieser Aspekt weiterhin eine entscheidende Rolle spielen, einerseits, um keine Ressourcen zu verschwenden, und andererseits, um die notwendigen Investitionen zur Erreichung des angemessenen Sicherheitsniveaus zu gewährleisten.

Oft werden mit IT-Sicherheit ausschließlich technische Lösungen verbunden. Dies ist ein weiterer Grund, anstatt IT-Sicherheit besser den Begriff Informationssicherheit zu benutzen. Vor allem ist es aber wichtig, darauf hinzuweisen, dass Investitionen in personelle Ressourcen häufig effektiver sind als Investitionen in Sicherheitstechnik. Technik alleine löst keine Probleme, sie muss immer in organisatorische Rahmenbedingungen eingebunden werden. Auch die Überprüfung von Wirksamkeit und Eignung von Sicherheitsmaßnahmen muss durch ausreichende Ressourcen sichergestellt werden.

In der Praxis fehlt den internen Sicherheitsexperten häufig die Zeit, um alle sicherheitsrelevanten Einflussfaktoren und Rahmenbedingungen (z. B. gesetzliche Anforderungen oder technische Fragen) zu analysieren. Teilweise fehlen ihnen auch die entsprechenden Grundlagen. Es ist immer dann sinnvoll, auf externe Experten zurückzugreifen, wenn Fragen und Probleme nicht mit eigenen Mitteln zu klären sind. Dies muss von den internen Sicherheitsexperten dokumentiert werden, damit die Leitungsebene die erforderlichen Ressourcen bereitstellt.

Grundvoraussetzung für einen sicheren IT-Betrieb ist ein gut funktionierender IT-Betrieb. Für den IT-Betrieb müssen daher ausreichende Ressourcen zur Verfügung gestellt werden. Typische Probleme des IT-Betriebs (knappe Ressourcen, überlastete Administratoren oder eine unstrukturierte und schlecht gewartete IT-Landschaft) müssen in der Regel gelöst werden, damit die eigentlichen Sicherheitsmaßnahmen wirksam und effizient umgesetzt werden können.

# 6 Einbindung der Mitarbeiter in den Sicherheitsprozess

Informationssicherheit betrifft ohne Ausnahme alle Mitarbeiter. Jeder Einzelne kann durch verantwortungs- und qualitätsbewusstes Handeln Schäden vermeiden und zum Erfolg beitragen. Sensibilisierung für Informationssicherheit und entsprechende Schulungen der Mitarbeiter sowie aller Führungskräfte sind daher eine Grundvoraussetzung für Informationssicherheit. Um Sicherheitsmaßnahmen wie vorgesehen umsetzen zu können, müssen bei den Mitarbeitern die erforderlichen Grundlagen vorhanden sein. Dazu gehört neben den Kenntnissen, wie Sicherheitsmechanismen bedient werden müssen, auch das Wissen über Sinn und Zweck von Sicherheitsmaßnahmen. Auch Arbeitsklima, gemeinsame Wertvorstellungen und das Engagement der Mitarbeiter beeinflussen die Informationssicherheit entscheidend.

Werden Mitarbeiter neu eingestellt oder erhalten neue Aufgaben, ist eine gründliche Einarbeitung und Ausbildung notwendig. Die Vermittlung sicherheitsrelevanter Aspekte des jeweiligen Arbeitsplatzes muss dabei berücksichtigt werden. Wenn Mitarbeiter die Institution verlassen oder sich ihre Zuständigkeiten verändern, muss dieser Prozess durch geeignete Sicherheitsmaßnahmen begleitet werden (z. B. Entzug von Berechtigungen, Rückgabe von Schlüsseln und Ausweisen).

Mitarbeiter sind auf die Einhaltung aller im jeweiligen Umfeld relevanten Gesetze, Vorschriften und Regelungen zu verpflichten. Dazu müssen sie natürlich mit den bestehenden Regelungen zur Informationssicherheit vertraut gemacht und gleichzeitig zu deren Einhaltung motiviert werden. Des Weiteren sollten die Mitarbeiter wissen, dass jeder erkannte (oder vermutete) Sicherheitsvorfall dem Sicherheitsmanagement gemeldet werden muss und an wen und wie dies zu erfolgen hat.

# 7 Der Informationssicherheitsprozess

Die Leitungsebene muss die Sicherheitsziele in Kenntnis aller relevanten Rahmenbedingungen und basierend auf den Geschäftszielen des Unternehmens bzw. dem Auftrag der Behörde festlegen und die Voraussetzungen für deren Umsetzung schaffen. Mit einer Sicherheitsstrategie wird das Vorgehen geplant, um einen kontinuierlichen Sicherheitsprozess zu etablieren. Umgesetzt wird die Strategie mit Hilfe eines Sicherheitskonzepts und einer Informationssicherheitsorganisation. Im Folgenden werden daher für jede Lebenszyklusphase die relevanten Managementtätigkeiten beschrieben. Aufgrund des Umfangs und der besseren Übersicht werden die Tätigkeiten rund um das Sicherheitskonzept in einem eigenen Kapitel beschrieben.

## 7.1 Planung des Sicherheitsprozesses

**Festlegung des Geltungsbereichs, in dem das ISMS gelten soll [DOK]**

Ein Managementsystem für Informationssicherheit muss nicht zwangsläufig für eine ganze Institution eingeführt werden. Zunächst muss daher der Geltungsbereich festgelegt werden, für den das ISMS zuständig sein soll. Der Geltungsbereich umfasst häufig die gesamte Institution, kann sich aber z. B. auch auf eine oder mehrere Fachaufgaben oder Geschäftsprozess oder eine Organisationseinheit beziehen. Hierbei ist es wichtig, dass die betrachteten Fachaufgaben und Geschäftsprozesse im gewählten Geltungsbereich vollständig enthalten sind. Im Rahmen des IT-Grundschutzes wird für den Geltungsbereich der Begriff "Informationsverbund" verwendet. Er umfasst dann auch alle infrastrukturellen, organisatorischen, personellen und technischen Komponenten, die der Aufgabenerfüllung in diesem Anwendungsbereich der Informationsverarbeitung dienen.

**Ermittlung von Rahmenbedingungen**

Die Schaffung von Informationssicherheit ist kein Selbstzweck. Aktuelle und zuverlässige Informationen sind die Grundlage der meisten Geschäftsprozesse. Informations- und Kommunikationstechnik soll die Ziele einer Institution sinnvoll unterstützen und dient zur Unterstützung von Geschäftsprozessen. Folgende Themen sollten bei der Entwicklung der Informationssicherheitsstrategie mindestens berücksichtigt werden:

- Ziele des Unternehmens bzw. Aufgaben der Behörde,
- gesetzliche Anforderungen und Vorschriften, wie z. B. zum Datenschutz,
- Kundenanforderungen und bestehende Verträge,
- interne Rahmenbedingungen (z. B. organisationsweites Risikomanagement oder IT-Infrastruktur),
- (IT-gestützte) Geschäftsprozesse und Fachaufgaben und
- globale Bedrohungen der Geschäftstätigkeit durch Sicherheitsrisiken (z. B. Imageschäden, Verstöße gegen Gesetze und vertragliche Verpflichtungen, Diebstahl von Forschungsergebnissen).

**Formulierung von Sicherheitszielen und einer Leitlinie zur Informationssicherheit [DOK]**

Es müssen Sicherheitsziele festgelegt und strategische Vorgaben gemacht werden, wie die Ziele erreicht werden sollen. Die Kernaussagen werden in einer Leitlinie zur Informationssicherheit (englisch: information security policy oder IT security policy) dokumentiert. Die Sicherheitsleitlinie sollte mindestens Aussagen zu den folgenden Themen enthalten:

- Sicherheitsziele der Behörde oder des Unternehmens,
- Beziehung der Sicherheitsziele zu den Geschäftszielen oder Aufgaben der Institution,
- angestrebtes Sicherheitsniveau,
- Leitaussagen, wie das angestrebte Sicherheitsniveau erreicht werden soll und
- Leitaussagen, ob und wodurch das Sicherheitsniveau nachgewiesen werden soll.

Die Leitlinie wird vom Management verabschiedet und in der Institution bekannt gegeben.

**Aufbau einer Informationssicherheitsorganisation [DOK]**

Zur Planung einer Informationssicherheitsorganisation gehört die Festlegung von Organisationsstrukturen (z. B. Abteilungen, Gruppen, Kompetenzzentren) und die Definition von Rollen und Aufgaben. Es muss ein für Informationssicherheit verantwortlicher Manager der obersten Leitungsebene benannt werden, z. B. ein Mitglied der Geschäftsführung. Außerdem muss mindestens ein IT-Sicherheitsbeauftragter benannt werden. Dieser muss regelmäßig und unabhängig der obersten Leitungsebene berichten können.

## 7.2 Umsetzung der Leitlinie zur Informationssicherheit

Um die gesetzten Sicherheitsziele zu erreichen, muss ein Sicherheitskonzept erstellt werden. Zur besseren Übersichtlichkeit wird in einem eigenen Kapitel dargestellt, wie ein Sicherheitskonzept geplant, umgesetzt und das Informationssicherheitsniveau aufrechterhalten und verbessert werden kann. Die Ergebnisse der Überprüfung der Sicherheitsmaßnahmen gehen dann in die Erfolgskontrolle des Sicherheitsprozesses ein und werden von der Leitungsebene bewertet.

## 7.3 Erfolgskontrolle im Sicherheitsprozess

Eine Erfolgskontrolle und Bewertung des Sicherheitsprozesses durch die Leitungsebene sollte regelmäßig stattfinden (Managementbewertung). Bei Bedarf (z. B. bei der Häufung von Sicherheitsvorfällen oder gravierenden Änderung der Rahmenbedingungen) muss auch zwischen den Routineterminen getagt werden. Alle Ergebnisse und Beschlüsse müssen nachvollziehbar dokumentiert werden [DOK].

Bei der Diskussion sollten unter anderem folgende Fragen betrachtet werden:

- Haben sich Rahmenbedingungen geändert, die dazu führen, dass das Vorgehen in Bezug auf Informationssicherheit geändert werden muss?
- Sind die Sicherheitsziele noch angemessen?
- Ist die Leitlinie zur Informationssicherheit noch aktuell?

Der Schwerpunkt bei der Erfolgskontrolle des Sicherheitsprozesses liegt dabei nicht auf der Überprüfung einzelner Sicherheitsmaßnahmen oder organisatorischer Regelungen, sondern auf einer Gesamtbetrachtung. Beispielsweise könnte sich der sichere Betrieb eines Internetportals als zu teuer für ein kleines Unternehmen herausstellen. Die Leitungsebene könnte dann als Alternative einen Dienstleister mit der Betreuung des Portals beauftragen.

Hierbei ist es hilfreich zu prüfen, wie sich das Sicherheitskonzept und die Informationssicherheitsorganisation bisher bewährt haben. Im Kapitel zum Sicherheitskonzept werden verschiedene Aktivitäten für die Erfolgskontrolle einzelner Sicherheitsmaßnahmen beschrieben. Die dort gesammelten Ergebnisse sollten bei der Erfolgskontrolle der Sicherheitsstrategie berücksichtigt werden. Stellt sich z. B. heraus, dass die Sicherheitsmaßnahmen unwirksam oder ausgesprochen teuer sind, kann dies ein Anlass sein, die gesamte Sicherheitsstrategie zu überdenken und anzupassen. Folgende Fragen sollten gestellt werden:

- Ist die Sicherheitsstrategie noch angemessen?
- Ist das Sicherheitskonzept geeignet, um die gesteckten Ziele zu erreichen? Werden z. B. die gesetzlichen Anforderungen erfüllt?
- Ist die Informationssicherheitsorganisation geeignet, um die Ziele zu erreichen? Muss deren Position in der Institution gestärkt werden oder sie stärker in interne Abläufe eingebunden werden?
- Steht der Aufwand - also Kosten, Personal, Material -, der zur Erreichung der Sicherheitsziele betrieben wird, in einem sinnvollen Verhältnis zum Nutzen für die Institution?

Die Ergebnisse der Erfolgskontrolle müssen konsequent zu angemessenen Korrekturen genutzt werden. Dies kann bedeuten, dass die Sicherheitsziele, die Sicherheitsstrategie oder das Sicherheits-

konzept geändert werden müssen und die Informationssicherheitsorganisation den Erfordernissen angepasst werden muss. Unter Umständen ist es sinnvoll, grundlegende Änderungen an Geschäftsprozessen oder der IT-Landschaft vorzunehmen oder Geschäftsprozesse aufzugeben oder auszulagern, wenn z. B. der sichere Betrieb mit den zur Verfügung stehenden Ressourcen nicht gewährleistet werden kann. Wenn größere Veränderungen vorgenommen und umfangreiche Verbesserungen umgesetzt werden, schließt sich der Management-Kreislauf wieder durch erneuten Beginn der Planungsphase.

# 8 Sicherheitskonzept

## 8.1 Erstellung des Sicherheitskonzepts

Um die Informationssicherheitsziele zu erfüllen und das angestrebte Sicherheitsniveau zu erreichen, muss zunächst verstanden werden, wie die Erfüllung von Aufgaben und Geschäftsprozessen von der Vertraulichkeit, Integrität und Verfügbarkeit von Informationen abhängt. Dazu muss auch betrachtet werden, durch welche Schadensursachen wie höhere Gewalt, organisatorische Mängel, menschliche Fehlhandlungen oder auch IT-Risiken Geschäftsprozesse bedroht werden. Danach muss entschieden werden, wie mit diesen Risiken umgegangen werden soll. Im Einzelnen sind folgende Teilschritte notwendig:

**Auswahl einer Methode zur Risikobewertung [DOK]**

Mögliche Schäden für die Geschäftstätigkeit und Aufgaben einer Institution durch Sicherheitsvorfälle müssen analysiert und bewertet werden. Eine Methode zur Risikobewertung ist daher Bestandteil jedes Managementsystems für Informationssicherheit. Um ein Risiko bestimmen zu können, müssen die Bedrohungen ermittelt und deren Schadenspotential und Eintrittswahrscheinlichkeit bewertet werden. Je nach Anwendungsfall, organisatorischen Randbedingungen, Branchenzugehörigkeit sowie angestrebtem Sicherheitsniveau kommen unterschiedliche Methoden zur Risikobewertung in Frage. Das Informationssicherheitsmanagement muss eine Methode auswählen, die für die Art und Größe der Institution angemessen ist. Die Methodenwahl beeinflusst entscheidend den Arbeitsaufwand für die Erstellung des Sicherheitskonzepts.

Verschiedene Arten der Risikobewertung sind in der Norm ISO/IEC 27005 beschrieben. Das BSI hat hieraus abgeleitet ebenfalls mehrere Methoden entwickelt und in der Praxis erprobt. In der IT-Grundschutz-Vorgehensweise wird dabei eine sehr praxisnahe Methode der Risikobewertung beschrieben, die mit Hilfe der IT-Grundschutz-Kataloge umgesetzt werden kann. Ergänzt wird dieser Ansatz durch den BSI-Standard 100-3 "Risikoanalyse basierend auf IT-Grundschutz".

Die Anwendung von IT-Grundschutz oder anderer Best-Practice-Ansätze hat den Vorteil, dass der eigene Arbeitsaufwand deutlich reduziert wird, weil die Autoren bereits eine konkrete Methode beschreiben und geeignete Sicherheitsmaßnahmen vorschlagen.


Abbildung 6: Überblick über den Lebenszyklus eines Sicherheitskonzepts

**Klassifikation von Risiken bzw. Schäden [DOK]**

Das Informationssicherheitsmanagement muss in Abhängigkeit der gewählten Methode zur Risikobewertung festlegen, wie Bedrohungen, Schadenspotentiale, Eintrittswahrscheinlichkeiten und die daraus resultierenden Risiken klassifiziert und bewertet werden.

Es ist allerdings schwierig, aufwendig und zudem fehleranfällig, für Schäden und Eintrittswahrscheinlichkeiten individuelle Werte zu ermitteln. Es empfiehlt sich, nicht zu viel Zeit in die aufwendige (und fehlerträchtige) exakte Bestimmung von Eintrittswahrscheinlichkeiten und möglichen Schäden zu stecken. In den meisten Fällen ist es praktikabler, sowohl für die Eintrittswahrscheinlichkeit als auch für die potentielle Schadenshöhe mit Kategorien zu arbeiten. Hierbei sollten nicht mehr als 3 bis 5 Kategorien verwendet werden, z. B.

- Eintrittswahrscheinlichkeit: selten, häufig, sehr häufig
- Potentielle Schadenshöhe: mittel, hoch, sehr hoch

Nachdem solche Kategorien in geeigneter Weise in der Institution definiert wurden, können diese als Grundlage für eine qualitative Risikobetrachtung verwendet werden.

**Risikobewertung [DOK]**

Jede Risikobewertung muss die folgenden Schritte umfassen:

- Die zu schützenden Informationen und Geschäftsprozesse müssen identifiziert werden.
- Alle relevanten Bedrohungen für die zu schützenden Informationen und Geschäftsprozesse müssen identifiziert werden.
- Schwachstellen, durch die die Bedrohungen wirken könnten, müssen identifiziert werden.
- Die möglichen Schäden durch Verlust von Vertraulichkeit, Integrität oder Verfügbarkeit müssen identifiziert und bewertet werden.

- Die anzunehmenden Auswirkungen auf die Geschäftstätigkeit oder die Aufgabenerfüllung durch Sicherheitsvorfälle müssen analysiert werden.
- Das Risiko, durch Sicherheitsvorfälle Schäden zu erleiden, muss bewertet werden.

Die hier verwendeten Begriffe "Bedrohung", "Schwachstelle" und "Risiko" werden im Glossar der IT-Grundschutz-Kataloge definiert.

**Entwicklung einer Strategie zur Behandlung von Risiken [DOK]**

Die oberste Leitungsebene muss vorgeben, wie die erkannten Risiken behandelt werden sollen. Diese müssen dafür vom Informationssicherheitsmanagement entsprechend aufbereitet werden. Dazu gibt es folgende Optionen:

- Risiken können vermindert werden, indem adäquate Sicherheitsmaßnahmen ergriffen werden.
- Risiken können vermieden werden, z. B. indem Geschäftsprozesse oder Fachaufgaben umstrukturiert oder aufgegeben werden.
- Risiken können übertragen werden, z. B. durch Outsourcing oder Versicherungen.
- Risiken können akzeptiert werden.

Die Art des Umgangs mit Risiken muss dokumentiert und von der obersten Leitungsebene genehmigt werden. Die notwendigen Ressourcen zur Umsetzung der Strategie müssen geplant und zur Verfügung gestellt werden.

Bei der Ausgestaltung der Strategie ist neben den Kosten das verbleibende Restrisiko ein wesentliches Entscheidungskriterium, das von der Leitungsebene berücksichtigt werden muss. Das Restrisiko muss daher bewertet und ebenfalls dokumentiert werden.

**Auswahl von Sicherheitsmaßnahmen [DOK]**

Aus den allgemeinen Sicherheitszielen und Sicherheitsanforderungen, die die Leitungsebene vorgegeben hat, leiten sich konkrete Sicherheitsmaßnahmen ab. Bei der Auswahl von Sicherheitsmaßnahmen sind neben den Auswirkungen auf das Sicherheitsniveau auch Kosten-Nutzen-Aspekte und die Praxistauglichkeit zu beachten.

Neben technischen Sicherheitsmaßnahmen müssen auch organisatorische Abläufe und Prozesse (wie Benutzerrichtlinien, Rechtevergaben, Sicherheitsschulungen, Test- und Freigabeverfahren) eingerichtet werden. Es müssen dabei unter anderem die folgenden Themen geregelt werden:

- Organisation (inklusive Festlegung von Zuständigkeiten, Aufgabenverteilung und Funktionstrennung, Regelung des Umgangs mit Informationen, Anwendungen und IT-Komponenten, Hard- und Software-Management, Änderungsmanagement etc.),
- Personal (z. B. Einweisung neuer Mitarbeiter, Vertretungsregelungen etc.),
- Schulung und Sensibilisierung zur Informationssicherheit,
- Datensicherung (für alle Informationen, Anwendungen und IT-Komponenten),
- Datenschutz,
- Computer-Virenschutz,
- Schutz von Informationen bei Verarbeitung, Übertragung und Speicherung (z. B. durch Einsatz von Kryptographie),
- Hard- und Softwareentwicklung,
- Verhalten bei Sicherheitsvorfällen (englisch: incident handling),
- Notfallvorsorge und Aufrechterhaltung der Geschäftstätigkeit im Notfall (englisch: business continuity) und

- Outsourcing.

Es muss nachvollziehbar dokumentiert sein, warum die ausgewählten Maßnahmen geeignet sind, die Sicherheitsziele und -anforderungen zu erreichen.

## 8.2 Umsetzung des Sicherheitskonzepts

Nach der Auswahl von Sicherheitsmaßnahmen müssen diese nach einem Realisierungsplan umgesetzt werden. Bei der Umsetzung sollten die folgenden Schritte eingehalten werden:

**Erstellung eines Realisierungsplans für das Sicherheitskonzept [DOK]**

Ein Realisierungsplan muss folgende Themen enthalten:

- Festlegung von Prioritäten (Umsetzungsreihenfolge),
- Festlegung von Verantwortlichkeiten für Initiierung,
- Bereitstellung von Ressourcen durch das Management und
- Umsetzungsplanung einzelner Maßnahmen (Festlegung von Terminen, Kosten sowie Festlegung von Verantwortlichen für die Realisierung und von Verantwortlichen für die Kontrolle der Umsetzung bzw. der Effektivität von Maßnahmen).

**Umsetzung der Sicherheitsmaßnahmen**

Die geplanten Sicherheitsmaßnahmen müssen gemäß des Realisierungsplans umgesetzt werden. Informationssicherheit muss dabei in die organisationsweiten Abläufe und Prozesse integriert werden. Falls sich bei der Umsetzung Schwierigkeiten ergeben, sollten diese sofort kommuniziert werden, damit überlegt werden kann, wie diese behoben werden können. Als typische Lösungswege können beispielsweise sowohl Kommunikationswege oder Rechtezuweisungen geändert als auch technische Verfahren angepasst werden.

**Steuerung und Kontrolle der Umsetzung [DOK]**

Die Einhaltung der Zielvorgaben muss regelmäßig überprüft werden. Falls Zielvorgaben nicht eingehalten werden können, ist das für Informationssicherheit zuständige Mitglied der Leitungsebene zu informieren, um auf Probleme rechtzeitig reagieren zu können.

## 8.3 Erfolgskontrolle und Verbesserung des Sicherheitskonzepts

Zur Aufrechterhaltung des Sicherheitsniveaus müssen einerseits die als angemessen identifizierten Sicherheitsmaßnahmen korrekt angewendet werden und andererseits muss das Sicherheitskonzept fortlaufend aktualisiert werden. Darüber hinaus müssen Sicherheitsvorfälle rechtzeitig entdeckt sowie schnell und angemessen auf diese reagiert werden. Es muss regelmäßig eine Erfolgskontrolle des Sicherheitskonzepts durchgeführt werden. Die Effektivität und Effizienz der umgesetzten Maßnahmen sollte im Rahmen von internen Audits überprüft werden. Wenn nicht genügend Ressourcen zur Verfügung stehen, um solche Audits von erfahrenen internen Mitarbeitern durchführen zu lassen, sollten externe Experten mit der Durchführung von Prüfungsaktivitäten beauftragt werden.

Da der Aufwand bei Audits von der Komplexität und Größe des Informationsverbunds abhängt, sind die Prüfanforderungen für kleine Behörden und Unternehmen entsprechend niedriger als für große und komplexe Institutionen und damit normalerweise sehr gut umzusetzen. Ein jährlicher technischer Check von IT-Systemen, eine Durchsicht vorhandener Dokumentationen, um die Aktualität zu prüfen, und ein Workshop, bei dem Probleme und Erfahrungen mit dem Sicherheitskonzept besprochen werden, kann unter Umständen in kleinen Institutionen schon ausreichend sein.

Im Einzelnen sollten die folgenden Aktivitäten durchgeführt werden:

**Reaktion auf Änderungen im laufenden Betrieb**

Bei Änderungen im laufenden Betrieb (z. B. der Einführung neuer Geschäftsprozesse, Organisationsänderungen oder beim Einsatz neuer IT-Systeme) müssen das Sicherheitskonzept sowie

die damit verbundenen Dokumente (wie auch die Liste der Zuständigkeiten oder der IT-Systeme) aktualisiert werden.

**Detektion von Sicherheitsvorfällen im laufenden Betrieb [DOK]**

Es müssen Maßnahmen umgesetzt sein, die es erlauben, Fehler in der Informationsverarbeitung (die die Vertraulichkeit, Verfügbarkeit oder Integrität beeinträchtigen können), sicherheitskritische Fehlhandlungen und Sicherheitsvorfälle möglichst zu verhindern, in ihrer Auswirkung zu begrenzen oder zumindest frühzeitig zu bemerken. Zur frühzeitigen Erkennung von Sicherheitsproblemen können beispielsweise Tools zu Systemüberwachungen, Integritätsprüfungen, Protokollierung von Zugriffen, Aktionen oder Fehlern, Kontrolle des Zutritts zu Gebäuden und Räumen oder Brand-, Wasser- bzw. Klimasensoren beitragen.

Die Aufzeichnungen und Protokolle der Detektionsmaßnahmen müssen regelmäßig ausgewertet werden.

**Überprüfung der Einhaltung von Vorgaben [DOK]**

Es muss regelmäßig geprüft werden, ob alle Sicherheitsmaßnahmen wie im Sicherheitskonzept vorgesehen angewendet und durchgeführt werden. Hierbei müssen sowohl die Einhaltung der technischen Sicherheitsmaßnahmen (z. B. hinsichtlich der Konfiguration) als auch die der organisatorischen Regelungen (z. B. Prozesse, Verfahren und Abläufe) kontrolliert werden. Es sollte auch überprüft werden, ob die notwendigen Ressourcen zur korrekten Umsetzung der Maßnahmen zur Verfügung stehen und alle Personen, denen bestimmte Rollen zur Umsetzung von Sicherheitsmaßnahmen zugewiesen wurden, ihren Verpflichtungen nachkommen.

**Überprüfung der Eignung und Wirksamkeit von Sicherheitsmaßnahmen [DOK]**

Es muss regelmäßig geprüft werden, ob die Sicherheitsmaßnahmen geeignet sind, die gesetzten Sicherheitsziele zu erreichen. Zur Überprüfung auf ihre Eignung können z. B. zurückliegende Sicherheitsvorfälle ausgewertet, Mitarbeiter befragt oder Penetrationstests durchgeführt werden. Dazu gehört es auch, relevante Entwicklungen im Umfeld der Geschäftsprozesse oder Fachaufgaben des Unternehmens oder der Behörde zu verfolgen. Beispielsweise können sich technische oder regulatorische Rahmenbedingungen geändert haben. Um sich auf dem aktuellen Stand zu halten, sollten die Sicherheitsverantwortlichen beispielsweise externe Wissensquellen nutzen, Fachkonferenzen besuchen sowie Standards und Fachliteratur und Informationen aus dem Internet auswerten. Wenn intern nicht das erforderliche Wissen oder die Zeit dazu vorhanden ist, sollten externe Experten hinzugezogen werden.

In diesem Zusammenhang ist es sinnvoll, zu hinterfragen, ob die eingesetzten Sicherheitsmaßnahmen effizient sind oder die Sicherheitsziele mit anderen Maßnahmen ressourcenschonender erreicht werden könnten. Dabei ist auch zu prüfen, ob Prozesse und organisatorische Regelungen praxistauglich und effizient sind. Häufig ergibt sich hieraus die Gelegenheit, notwendige Organisationsverbesserungen und Restrukturierungen vorzunehmen.

**Managementbewertungen**

Die Leitungsebene muss vom Informationssicherheitsmanagement regelmäßig in angemessener Form über die Ergebnisse der Überprüfungen informiert werden. Dabei sollten Probleme, Erfolge und Verbesserungsmöglichkeiten aufgezeigt werden.

Die Management-Berichte müssen alle für die Leitungsebene notwendigen Informationen zur Steuerung des Sicherheitsprozesses beinhalten. Solche Informationen sind beispielsweise:

- Übersicht über den aktuellen Status im Sicherheitsprozess,
- Begutachtung von Folgemaßnahmen vorangegangener Managementbewertungen,
- Rückmeldungen von Kunden und Mitarbeitern und
- Überblick über neu aufgetretene Bedrohungen und Sicherheitslücken.

Die Leitungsebene nimmt die Management-Berichte zur Kenntnis und trifft die notwendigen Entscheidungen, wie beispielsweise zur Verbesserung des Sicherheitsprozesses, zum Ressourcenbedarf sowie zu den Ergebnissen von Sicherheitsanalysen (z. B. Minimierung, Übernahme oder Akzeptanz von Risiken).

Die regelmäßige Erfolgskontrolle des Sicherheitsprozesses dient dazu, erkannte Fehler und Schwachstellen abzustellen und die Sicherheitsmaßnahmen in Bezug auf Effizienz zu optimieren.

Die Aktivitäten sollten sich dabei nicht auf technische Maßnahmen beschränken. Unter Umständen ist es notwendig, die Mitarbeiter zu schulen und zu sensibilisieren. Ein wichtiger Punkt ist auch die Verbesserung der Praxistauglichkeit von technischen Maßnahmen und organisatorischen Abläufen, um die Akzeptanz der Sicherheitsmaßnahmen zu erhöhen.

# 9 Das ISMS des BSI: IT-Grundschutz

## 9.1 Einleitung

Die Beschreibungen eines Managementsystems für Informationssicherheit sind in diesem Dokument und auch in den ISO-Standards 27000, 27001 und 27002 sehr generisch gehalten und geben lediglich einen Rahmen vor. In der Praxis besteht daher ein großer Gestaltungsspielraum bei der praktischen Umsetzung der generischen Vorgaben. Die große Herausforderung besteht darin, in der eigenen Institution ein ISMS zu etablieren, das nicht nur hilft, die gesteckten Sicherheitsziele zu erreichen, sondern auch noch möglichst kostengünstig und wirtschaftlich ist.

Dabei ist die Frage, wie ein Sicherheitskonzept für die Institution zu erstellen ist, meist am schwierigsten zu lösen. Die zentralen Arbeitsschritte bei der Erstellung eines Sicherheitskonzepts sind dabei die Risikobewertung und die Auswahl der richtigen Sicherheitsmaßnahmen. Der Wahl der Methode zur Risikobewertung kommt dabei eine besondere Bedeutung zu, da die Methodenwahl den Arbeitsaufwand für die Erstellung des Sicherheitskonzepts entscheidend beeinflusst. Die Vorgehensweise nach IT-Grundschutz beschreibt eine Methode, die für die meisten Anwendungsfälle geeignet ist. Sie ist dabei im Vergleich zur klassischen quantitativen Risikoanalyse weitaus kostengünstiger sowie seit vielen Jahren praxiserprobt. Als Mehrwert wird in der IT-Grundschutz-Vorgehensweise nicht nur beschrieben, wie ein ISMS grundsätzlich funktioniert, sondern zusammen mit den IT-Grundschutz-Katalogen wird auch geschildert, wie die Umsetzung von konkreten Maßnahmen in der Praxis aussehen kann.

Dieses Kapitel gibt eine Einführung in die wesentlichen Elemente der IT-Grundschutz-Vorgehensweise und zeigt auf, dass ein Vorgehen nach IT-Grundschutz vollständig kompatibel zum Standard ISO 27001 ([27001]) ist. Eine ausführliche Darstellung der Vorgehensweise nach IT-Grundschutz ist im BSI-Standard 100-2 ([BSI2]) enthalten.

Die IT-Grundschutz-Vorgehensweise beschreibt einen Anwendungsansatz für die Etablierung und Aufrechterhaltung eines Managementsystems für Informationssicherheit basierend auf der IT-Grundschutz-Methodik und den IT-Grundschutz-Katalogen. Dort werden die hier erwähnten Themen ausführlicher und praxisbezogener dargestellt als im vorliegenden Dokument. Jeder Baustein der IT-Grundschutz-Kataloge folgt zudem einem Lebenszyklus-Modell und enthält spezielle Maßnahmen von der Planung bis zur Aussonderung.

## 9.2 Der Sicherheitsprozess nach IT-Grundschutz

Alle gängigen Methoden, Best-Practice-Beispiele und Standards zum Management von Informationssicherheit unterscheiden sich kaum in den Ausführungen, die sich mit dem Sicherheitsprozess oder den Aufgaben des leitenden Managements beschäftigen. Die größten Unterschiede bestehen in der Art und Weise, wie ein Sicherheitskonzept konkret erstellt wird, also bei der Ausgestaltung der Risikobewertung und der Auswahl der Sicherheitsmaßnahmen. Aus diesem Grund wird an dieser Stelle das grundsätzliche Vorgehen bei der Erstellung eines Sicherheitskonzeptes nach IT-Grundschutz dargestellt.

### 9.2.1 Risikobewertung

**Risikobewertung in der Informationssicherheit**

Eine Risikobewertung in der Informationssicherheit unterscheidet sich in wesentlichen Punkten von klassischen Methoden der Versicherungsmathematik oder des Controllings. Die exakte Berechnung von Schadenshöhen und Eintrittswahrscheinlichkeiten bei einer "klassischen" oder quantitativen Risikoanalyse ist meistens nicht möglich, da geeignetes Zahlenmaterial fehlt. Selbst wenn eine Berechnung möglich ist, bleibt die Interpretation der Ergebnisse sehr schwierig.

Beispiel: Bei der klassischen Risikoanalyse berechnet sich das Risiko aus der Schadenshöhe multipliziert mit der Eintrittswahrscheinlichkeit. Wenn also die Zerstörung eines Rechenzentrums durch einen Flugzeugabsturz 20 Millionen Euro kostet und statistisch einmal in 20.000 Jahren passiert,

beträgt das theoretische Risiko 1.000 Euro pro Jahr. Das gleiche Risiko ergibt sich, wenn der Schaden bei Diebstahl eines Notebooks (ohne Datenverlust) mit 2.000 Euro angesetzt wird und dieser rechnerisch einmal in zwei Jahren eintritt. Obwohl das Risiko rein rechnerisch im Wert übereinstimmt, müssen diese beiden Schadensszenarien im Rahmen des Risikomanagements völlig unterschiedlich behandelt werden.

Für viele Szenarien fehlen zudem ausreichende Erfahrungswerte, um die Eintrittswahrscheinlichkeiten fundiert bestimmen zu können, beispielsweise weil neue Technologien eingesetzt werden bzw. wenig fundiertes Basismaterial vorhanden ist. Selbst wenn genügend Daten vorliegen, um Eintrittswahrscheinlichkeiten und Schadenshöhen bestimmter Schadensereignisse einigermaßen seriös bestimmen zu können, ist die Erstellung eines Sicherheitskonzepts auf Basis einer klassischen Risikoanalyse extrem aufwendig und teuer. Eine individuelle Analyse von Schwachstellen für alle wesentlichen Geschäftsprozesse und der damit verknüpften IT-Komponenten und die Zusammenstellung der möglichen Schadensereignisse mit Zuordnung der Parameter Eintrittswahrscheinlichkeit und Schadensausmaß erfordern ein fundiertes Fachwissen und die Verarbeitung großer Datenmengen.

In der Vorgehensweise nach IT-Grundschutz ist daher bereits eine qualitative Methode zur Risikobewertung enthalten, die die notwendigen Informationen zur Beurteilung von geschäftsschädigenden Sicherheitsvorfällen liefert. Bei der Vorgehensweise nach IT-Grundschutz wird davon ausgegangen, dass unabhängig von der Art und Ausrichtung einer Institution überall geschäftsrelevante Informationen sicher verarbeitet werden müssen, gängige und damit verwandte IT-Systeme eingesetzt werden und vergleichbare Umfeldbedingungen existieren. Damit liegen meistens vergleichbare Bedrohungen vor. Die Sicherheitsanforderungen der Geschäftsprozesse und Fachanwendungen sind zwar individuell und können unterschiedlich sein, in der Praxis führen sie jedoch meist zu ähnlichen und vergleichbaren Sicherheitsanforderungen.

Das BSI analysiert für die Vorgehensweise nach IT-Grundschutz in den IT-Grundschutz-Katalogen Schwachstellen und Bedrohungen für typische Einsatzfelder und Komponenten und ermittelt daraus die resultierenden Gefährdungen. Es werden nur solche Gefährdungen betrachtet, die nach sorgfältiger Analyse eine so hohe Eintrittswahrscheinlichkeit oder so einschneidende Auswirkungen haben, dass Sicherheitsmaßnahmen ergriffen werden müssen. Typische Gefährdungen, gegen die sich jeder schützen muss, sind z. B. Schäden durch Feuer, Einbrecher, Computer-Viren oder Hardware-Defekte. Dieser Ansatz hat den Vorteil, dass Anwender des IT-Grundschutzes für einen Großteil des Informationsverbundes keine Bedrohungs- und Schwachstellenanalyse durchführen oder Eintrittswahrscheinlichkeiten berechnen müssen, weil ihnen damit eine staatliche Stelle diese Arbeit abgenommen hat.

Auf Basis der ermittelten Gefährdungen beschreiben die IT-Grundschutz-Kataloge bewährte technische, infrastrukturelle, personelle und organisatorische Standard-Sicherheitsmaßnahmen für typische Objekte.

Für Informationen und Geschäftsprozesse mit einem hohen oder sehr hohen Schutzbedarf oder für Einsatzumgebungen, die im IT-Grundschutz nicht behandelt werden, muss eine ergänzende Sicherheitsanalyse und gegebenenfalls eine Risikoanalyse durchgeführt werden. Eine vereinfachte Risikoanalyse nach der IT-Grundschutz-Methodik wird in [BSI3] beschrieben.

Sowohl die Risikobewertung nach IT-Grundschutz als auch die in [BSI3] dargestellte Risikoanalyse sind deutlich einfacher und kostengünstiger als eine quantitative Risikoanalyse. Die Risikobewertung nach IT-Grundschutz bietet zudem den Vorteil, dass auch Institutionen aus den verschiedensten Branchen, die nach dieser Methode vorgehen, eine gemeinsame und klar definierte Grundlage für ihre Risikobewertung vorweisen können.

**Klassifikation von Risiken**

Die allgemeine Anforderung, Risiken zu klassifizieren, wird im IT-Grundschutz in folgenden Schritten durchgeführt:

1. Orientierung an Schadensszenarien

Um Schäden und negative Auswirkungen von Sicherheitsvorfällen möglichst anschaulich zu beschreiben, sollten verschiedene Schadensszenarien betrachtet werden, z. B.:

- Verstöße gegen Gesetze, Vorschriften oder Verträge,
- Beeinträchtigung des informationellen Selbstbestimmungsrechts,
- Beeinträchtigung der persönlichen Unversehrtheit,
- Beeinträchtigung der Aufgabenerfüllung,
- negative Innen- oder Außenwirkung und
- finanzielle Auswirkungen.

Beim Durchspielen der Szenarien sollte dabei untersucht werden, welche Schäden beim Verlust von Vertraulichkeit, Integrität oder Verfügbarkeit entstehen können.

Beispielsweise sollte für das Szenario "Verstoß gegen Gesetze" unter anderem erörtert werden, welche Daten aufgrund gesetzlicher Auflagen vertraulich behandelt werden müssen und welche Konsequenzen ein fahrlässiger Verstoß gegen diese Auflagen hätte.

2. Klassifizierung von Schäden: Definition von Schutzbedarfskategorien

Meist ist eine exakte Berechnung von potentiellen Schäden nicht sinnvoll oder sogar unmöglich und für die Auswahl geeigneter Sicherheitsmaßnahmen auch nicht nötig. Daher empfiehlt sich eine Einteilung von Schäden in wenige Klassen. Der Versuch einer "exakten" Schadensberechnung gefährdet in vielen Fällen sogar die Sicherheit, da eine nicht zutreffende Genauigkeit suggeriert wird und die Verantwortlichen dadurch nur von einer "Scheinsicherheit" ausgehen.

Ausgehend von möglichen Schäden werden im Rahmen des IT-Grundschutzes drei Schutzbedarfskategorien definiert, in die später die Schutzobjekte (z. B. IT-Systeme) eingeordnet werden:

| | |
|---|---|
| "normaler Schutzbedarf": | Die Schadensauswirkungen sind begrenzt und überschaubar. |
| "hoher Schutzbedarf": | Die Schadensauswirkungen können beträchtlich sein. |
| "sehr hoher Schutzbedarf": | Die Schadensauswirkungen können ein existentiell bedrohliches, katastrophales Ausmaß erreichen. |

Jede Institution muss für jedes Schadensszenario individuell festgelegen, wie "normal", "hoch" und "sehr hoch" zu interpretieren sind, welche Rahmenbedingungen für die Einteilung in die Schutzbedarfskategorien also zugrunde zu legen sind. Da dies unmittelbare Auswirkungen auf den Umgang mit Risiken und den Bedarf an Ressourcen hat, muss diese Festlegung durch die oberste Leitungsebene der Institution erfolgen. Die Festlegung der Schutzbedarfskategorien kann je nach Art und Größe der Institution sehr unterschiedlich sein und nur die oberste Leitungsebene kann diese in Zusammenarbeit mit dem Sicherheitsmanagement konkret festlegen. Das BSI kann daher nur Beispiele für entsprechende Werte nennen, die an die jeweiligen Bedingungen anzupassen sind.

Beispiel für die Klassifizierung finanzieller Schäden:

Ein normaler Schutzbedarf ist gegeben, wenn ein finanzieller Schaden für die Institution tolerabel ist. Bei einem kleinen Betrieb kann dies bedeuten, dass durch Sicherheitsvorfälle keine Schäden über 10.000 Euro entstehen dürfen. Ein hoher Schutzbedarf besteht, wenn ein Schaden beachtliche finanzielle Verluste nach sich zieht, jedoch nicht existenzbedrohend ist. Bei einem kleinen Betrieb kann dies zwischen 10.000 Euro und 100.000 Euro bedeuten. Ein sehr hoher Schutzbedarf liegt dann vor, wenn der finanzielle Schaden für die Institution existenzbedrohend ist. Bei einem kleinen Betrieb könnte dies bereits bei einem Schadenspotential von über 100.000 Euro gegeben sein. Bei einer großen Geschäftsbank ergeben sich hier natürlich andere Werte.

**Risikobewertung**

1. Strukturanalyse: Identifikation von Schutzobjekten [DOK]

Im Rahmen der Strukturanalyse werden die für den betrachteten Informationsverbund, also Geltungsbereich oder Geschäftsprozess, relevanten Schutzobjekte wie Informationen, Anwendungen, IT-Systeme, Netze, Räume und Gebäude, aber auch zuständige Mitarbeiter ermittelt.

Bei der Strukturanalyse müssen zusätzlich die Beziehungen und Abhängigkeiten zwischen den einzelnen Schutzobjekten dargestellt werden. Die Erfassung von Abhängigkeiten dient vor allem dazu, die Auswirkungen von Sicherheitsvorfällen auf die Geschäftstätigkeit zu erkennen, um dann angemessen reagieren zu können.

Beispiel: Wenn der "Server xy" von einem Sicherheitsvorfall betroffen wird, muss schnell erkannt werden, welche Anwendungen oder Geschäftsprozesse davon betroffen sind.

2. Schutzbedarfsfeststellung: Auswirkungen von Sicherheitsvorfällen auf die betrachteten Geschäftsprozesse analysieren

   Für jeden bei der Strukturanalyse ermittelten Wert wird das Maß an Schutzbedürftigkeit bestimmt.

   Beispiel: Kann der Ausfall eines IT-Systems einen hohen Schaden verursachen, ist der ermittelte Wert hoch, da das IT-System einen dementsprechend hohen Schutzbedarf hat.

   Zuerst muss dazu der Schutzbedarf der Geschäftsprozesse ermittelt werden. Anschließend kann darauf aufbauend der Schutzbedarf der Anwendungen bestimmt werden, die bei der Strukturanalyse erfasst wurden. Dabei muss berücksichtigt werden, welche Informationen mit diesen Anwendungen verarbeitet werden. In den allermeisten Institutionen reicht es an dieser Stelle aus, sehr wenige Informationsgruppen zu betrachten. Beispiele hierfür sind Kundendaten, öffentlich zugängliche Informationen (z. B. Adresse, Öffnungszeiten) oder strategische Daten für die Geschäftsführung. Danach wird betrachtet, welche Informationen wo und mit welchen IT-Systemen verarbeitet werden, um die Geschäftsprozesse erfüllen zu können.

   Der Schutzbedarf der Anwendungen überträgt sich auf die IT-Systeme, die die jeweiligen Anwendungen unterstützen. Der Schutzbedarf der Räume leitet sich aus dem Schutzbedarf der Anwendungen und IT-Systeme, die dort betrieben werden, ab.

   Beispiel: Der Geschäftsprozess Kundendatenverwaltung ist essentiell für die Aufrechterhaltung des Geschäftsbetriebs. Dieser Geschäftsprozess läuft auf dem Server xy, der damit einen hohen Schutzbedarf hat. Der Raum, in dem der Server untergebracht ist, hat daher auch mindestens einen hohen Schutzbedarf.

3. Ergänzende Sicherheitsanalyse [DOK]

   Die Anwendung der Vorgehensweise nach IT-Grundschutz ermöglicht es, ein Sicherheitsniveau zu schaffen, das für den normalen Schutzbedarf ausreichend und angemessen ist. Wenn der Schutzbedarf für einen bestimmten Bereich (beispielsweise eine Anwendung oder IT-System) höher ist oder wenn für einen Bereich keine IT-Grundschutzmaßnahmen existieren, sollte nach der Umsetzung von IT-Grundschutz eine ergänzende Sicherheitsanalyse durchgeführt werden.

   Das BSI hat eine eigene Methode zur Risikoanalyse entwickelt, die auf die Umsetzung von IT-Grundschutz aufbaut. Sie wird in dem BSI-Standard 100-3 [BSI3] beschrieben. Als Methode kann aber auch eine klassische quantitative Risikoanalyse für die betroffenen Bereiche gewählt werden. Wenn nur ein kleiner Bereich der Informationsverarbeitung betroffen ist, ist der Aufwand für eine zusätzliche Risikoanalyse meistens gering. Ist z. B. nur ein spezielles IT-System, für das kein IT-Grundschutz-Baustein vorliegt, betroffen, kann die hierauf beschränkte Beratung durch den Hersteller oder unabhängige Sicherheitsberater in der Regel schon helfen, das Risiko abzuschätzen und geeignete Sicherheitsmaßnahmen auszuwählen.

Die Kombination aus Standard-Sicherheitsmaßnahmen und Risikoanalyse für die Bereiche, deren Schutzbedürftigkeit über normalen Schutzbedarf hinausgeht, ist wesentlich effizienter als eine vollständige quantitative Risikoanalyse. Anschließend müssen dann die jeweils identifizierten Maßnahmen wieder in den restlichen Sicherheitsprozess eingebracht und konsolidiert werden.

### 9.2.2 Erstellung der Sicherheitskonzeption

Die IT-Grundschutz-Kataloge enthalten Kataloge zu typischen Bausteinen, Gefährdungen und Maßnahmen. In den Bausteinen werden für typische Aufgaben des Informationssicherheitsmanagements und Bereiche des IT-Einsatzes Gefährdungen und Standard-Sicherheitsmaßnahmen beschrieben. Dabei werden jeweils organisatorische, personelle, infrastrukturelle und technische Aspekte der Informationssicherheit betrachtet.

Die IT-Grundschutz-Kataloge beinhalten Bausteine aus folgenden Bereichen:

- Übergeordnete Aspekte der Informationssicherheit (z. B. Organisation, Personal, Notfallvorsorge),
- Sicherheit der Infrastruktur (z. B. Gebäude, Rechenzentrum),
- Sicherheit der IT-Systeme (z. B. Server, Clients, Netzkomponenten),
- Sicherheit im Netz (z. B. Netz- und Systemmanagement) und
- Sicherheit in Anwendungen (z. B. E-Mail).

Nach der Strukturanalyse kann somit der Geschäftsbetrieb mit Hilfe dieser Bausteine modelliert werden. Dabei wird dem betrachteten Geltungsbereich eine Sammlung von relevanten IT-Grundschutz-Bausteinen (Informationsverbund) zugeordnet. Daraus resultiert eine Sammlung an Maßnahmenempfehlungen, die als Grundlage für die Erstellung der Sicherheitskonzeption dienen kann.

Bei den in den IT-Grundschutz-Katalogen enthaltenen Maßnahmen handelt es sich sowohl um konkrete Implementierungshilfen zu den generischen Anforderungen aus ISO 27001 bzw. ISO 27002 als auch um zahlreiche technische Maßnahmen für den sicheren Betrieb von typischen IT-Systemen und Anwendungen. Eine genaue Anleitung zur Auswahl der Bausteine (Modellierung nach Grundschutz) hilft dabei, alle sicherheitsrelevanten Aspekte zu berücksichtigen. Mit dieser Hilfe ist es Unternehmen und Behörden möglich, auch ohne oder mit deutlich weniger Hilfe von externen Beratern die angestrebten Sicherheitsziele zu erreichen.