|  |  |
| --- | --- |
| Version: | 1.0 |
| Status: | Freigegeben |
| Dokumentenklassifizierung: | intern |

Standard "Sicherheitsorganisation"

1. Januar 2020

Allgemeine Informationen zum vorliegenden Dokument

|  |  |  |
| --- | --- | --- |
| Bezeichnung | Inhalt | Bearbeitungshinweis |
| Eigentümer |  | [verantwortlich für die Erstellung und Pflege des Dokuments = Abteilungsleitung] |
| Autor |  | [operative Verantwortung für das Dokument] |
| Status | Freigegeben | [Einstufung des aktuellen Dokumentenstatus <Entwurf, Finaler Entwurf, Final/Freigegeben>] |
| Klassifizierung | intern | [Einstufung der Dokumentenvertraulichkeitoffen, intern, vertraulich, streng vertraulich] |
| Dokumen­tenkennung | ISMS200002 | [Die Dokumenten-Kennung wird von der Dokumentenlenkung vergeben] |
| Name des Dokuments | Standard "Sicherheitsorganisation" | [Bezeichnung des Dokuments wie auf dem Titelblatt beschrieben.] |
| Version  | 1.0 | [zweistellige Versionsnummer] |
| Veröffentlichungsform | digital | [Veröffentlichungsform Papier, digital] |
| Speicherort |  | [Ablageort des Dokumentes] |
| Freigabe am | <TT.MM.YYYY> | [Datum der Freigabe durch den Eigentümer] |
| Freigabe bis | <TT.MM.YYYY> | [Datum der Freigabe bis durch den Eigentümer] |
| Revisionszyklus | Alle zwei Jahre | [Revisionszyklus alle 1, 2 Jahre] |
| Archivierungszeitraum | 10 Jahre | [Archivierungszeitraum nach Ablauf 5, 10 Jahre] |

# Dokumentenhistorie

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Beschreibung | Autor | Datum |
| 0.1 | initiale Erstellung |  |  |
| 0.2 – 0.8 | draft |  |  |
| 0.9 | final draft |  |  |
| 1.0 | final/freigegeben |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Inhaltsverzeichnis

[Allgemeine Informationen zum vorliegenden Dokument 2](#_Toc75086233)

[Dokumentenhistorie 3](#_Toc75086234)

[Inhaltsverzeichnis 4](#_Toc75086235)

[Allgemeine Festlegungen 5](#_Toc75086236)

[Ziel / Zweck 5](#_Toc75086237)

[Geltungsbereich 5](#_Toc75086238)

[Zuständigkeiten 6](#_Toc75086239)

[Genehmigungs- und Änderungsverfahren 6](#_Toc75086240)

[Standard "Sicherheitsorganisation" 6](#_Toc75086241)

[Informationssicherheitsmanagement und Notfallmanagement 6](#_Toc75086242)

[Aufbauorganisation des Informationssicherheitsmanagements 7](#_Toc75086243)

[Die Regelstruktur im ISMS-Dokumenten-Framework 7](#_Toc75086244)

[Informationssicherheitsmanagementprozess 7](#_Toc75086245)

[ISMS gestalten 9](#_Toc75086246)

[Vorgaben definieren 9](#_Toc75086247)

[Vorgaben umsetzen 10](#_Toc75086248)

[Sensibilisierung und Schulung 11](#_Toc75086249)

[Prüfung 11](#_Toc75086250)

[Berichtswesen und Monitoring 12](#_Toc75086251)

[Kontinuierlicher Verbesserungsprozess 12](#_Toc75086252)

[Behandlung von Sicherheitsvorfällen 13](#_Toc75086253)

# Allgemeine Festlegungen

## Ziel / Zweck

Dieses Dokument beschreibt den Aufbau und die wesentliche Funktionsweise des Informationssicherheitsmanagementsystems (ISMS) der <Institution>. Das ISMS hat die Aufgabe, der Geschäftsführung alle notwendigen Informationen zur Informationssicherheit zur Verfügung zu stellen, damit diese die notwendigen Entscheidungen treffen und deren Umsetzung veranlassen kann. Es orientiert sich an den Vorgaben des BSI IT-Grundschutz-Kompendiums und der BSI Standards 200-1 „Managementsysteme für Informationssicherheit (ISMS)“, 200-2 „IT-Grundschutz-Methodik“ und 200-3 „Risikomanagement“.

Eine Vielzahl von Ereignissen kann Einfluss auf die Ausrichtung der Informationssicherheit haben. Diese sind z. B.

1. Gesetzliche, regulatorische, vertragliche und interne Anforderungen
2. Technische und organisatorische Entwicklungen
3. Sicherheitsvorfälle
4. Marktentwicklungen
5. Wirtschaftliche Anforderungen

Diese Ereignisse werden in den Sicherheitsprozessen des ISMS ausgewertet und weiterverarbeitet. Die Ergebnisse sind in der Regel Sicherheitsmaßnahmen für die einzelnen Bereiche oder Anforderungen an die Gestaltung des ISMS. In den nachfolgenden Kapiteln zu den jeweiligen Sicherheitsprozessen wird beschrieben, für welche Ereignisse diese relevant sind.

Parallel zum Sicherheitsmanagement wurde mit der Sicherheitsrichtlinie "Behandlung von Sicherheitsvorfällen“ auch ein Prozess zur Behandlung von Verletzungen der Sicherheitsanforderungen etabliert. Dieser Prozess unterstützt systematisch die Bewältigung von Sicherheitsvorfällen.

## Geltungsbereich

Die Vorgaben des Dokumentes sind für alle Prozessverantwortlichen der <Institution> verbindlich und entsprechend durch die zuständigen Rollenträger umzusetzen.

Anzuwenden sind die Vorgaben für alle durch die <Institution> verantworteten Geschäftsprozesse, Hard- und Softwarekomponenten sowie ihren Konfigurationen. Die Umsetzung dieser Arbeitsanweisung ist durch die entsprechenden Führungskräfte sicherzustellen.

Die im Folgenden beschriebenen Vorgaben sind hingegen nicht bindend für Prozessverantwortliche von Geschäftsprozessen, die nicht durch die <Institution> wahrgenommen werden. In diesen Fällen besitzen die beschriebenen Vorgaben einen empfehlenden Charakter, auf eine Einhaltung muss durch die <Institution> hingewirkt werden.

Interne Regelungen sind geschlechterneutral zu formulieren. Aus Gründen der besseren Lesbarkeit wird auf die gleichzeitige Verwendung männlicher und weiblicher Sprachformen verzichtet. Sämtliche personenbezogenen Bezeichnungen in männlicher Form werden verallgemeinernd verwendet und beziehen sich stets auf alle Geschlechter.

## Zuständigkeiten

Zuständig für die Einhaltung der in diesem Dokument aufgeführten Pflichten und Anforderungen sind:

* Eigene Mitarbeitende und beauftragte Dienstleister, welche administrative Arbeiten an IT- Systemen und Anwendungen von der <Institution> durchführen,
* Eigene Mitarbeitende und beauftragte Dienstleister, welche Applikationsbetreuung mit administrativem Charakter (z. B. Versionspflege, Benutzerverwaltung) betreiben. Die Kontrolle der korrekten Umsetzung der Vorgaben erfolgt durch den <Bereich ???> bei der <Institution>.

## Genehmigungs- und Änderungsverfahren

Der Standard Sicherheitsorganisation wird durch den <Informationssicherheitsbeauftragter> verantwortet. Die Pflege dieses Dokuments unterliegt dem <Bereich ???> vertreten durch den <Informationssicherheitsbeauftragter>. Änderungen werden ausschließlich von dieser Person oder seinem Stellvertreter vorgenommen. Eine Genehmigung und Freigabe erfolgt durch den <Informationssicherheitsbeauftragter>.

# Standard "Sicherheitsorganisation"

## Informationssicherheitsmanagement und Notfallmanagement

Das Sicherheitsziel Verfügbarkeit und die Ergebnisse aus der Risikoanalyse werden sowohl in der Informationssicherheit als auch im Notfallmanagement betrachtet. Die Anforderungen an die Verfügbarkeit und die Risikoanalyse werden gemeinsam erhoben, aber die Umsetzung von Notfallvorsorgemaßnahmen und Risiko minimierenden Maßnahmen erfolgen im Rahmen des Notfallmanagements nach dem BSI-Standard 200-4. Im weiteren Verlauf dieses Dokuments wird beschrieben, wie die Methoden zur Erhebung der Verfügbarkeiten sowohl für das ISMS (Informationssicherheitsmanagementsystem) als auch BCM (Business Continuity Management) definiert sind. Damit werden einheitliche Vorgehensweisen und Ergebnisse erreicht.

Darüber hinaus sind in einem Notfall ebenfalls die Anforderungen an die Informationssicherheit zu gewährleisten. Die Notfallmaßnahmen werden derart ausgestaltet und umgesetzt, dass die Sicherheitsziele auch in einem Notfall erfüllt werden.

### Aufbauorganisation des Informationssicherheitsmanagements

Die Rollen und Verantwortlichkeiten des Informationssicherheitsmanagements gliedern sich in zwei Aufgabenteile:

* Aufgaben innerhalb des Informationssicherheitsmanagements sowie
* Aufgaben innerhalb der Sicherheitsvorfallbehandlung.

## Die Regelstruktur im ISMS-Dokumenten-Framework

Die Vorgaben zur Umsetzung der relevanten Informationssicherheitsmaßnahmen werden im ISM-Dokumenten-Framework zusammengefasst. Zur Vereinfachung werden die Sicherheitsdokumente je nach Fokus in verschiedene Ebenen unterteilt. Dadurch können die unterschiedlichen Zielgruppen (z. B. Mitarbeiter, Administratoren, externe Dienstleister) besser adressiert und deren Verantwortlichkeit eindeutig festgelegt werden. In der <Institution> werden insgesamt vier Ebenen verwendet:

**Ebene 1: Leitlinie zur Informationssicherheit**

Die Leitlinie zur Informationssicherheit beschreibt die Relevanz der Informationssicherheit und den Rahmen der erforderlichen organisatorischen Maßnahmen.

**Ebene 2: Standards**

Die Dokumente in der Ebene 2 „Standards“ beschreiben die normierten und methodischen Vorgehensweisen, Verantwortlichkeiten und Kompetenzen für das ISMS. Die Standards beinhalten alle Vorgaben, die zur Erreichung der Sicherheitsziele des ISMS erforderlich sind.

**Ebene 3: Sicherheitsrichtlinien**

Die Richtliniendokumente beinhalten die allgemeinen Definitionen von Sicherheitsmaßnahmen basierend auf den Vorgaben des BSI IT-Grundschutz-Kompendium.

**Ebene 4: Konzepte, Guidelines und Betriebsdokumentation**

In der Ebene 4 „Konzepte, Guidelines und Betriebsdokumentation“ werden konkrete Beschreibungen und Umsetzungen von technischen und organisatorischen Sicherheitsmaßnahmen basierend auf den ISMS-Dokumenten-Framework-Ebenen 1 bis 3 definiert.

## Informationssicherheitsmanagementprozess

Die nachfolgenden Basismaßnahmen sind vorranging zur Gewährleistung der sicherheitstechnischen Anforderungen aus der Leitlinie umzusetzen.

Das Informationssicherheitsmanagement orientiert sich an den Vorgaben des modernisierten BSI IT-Grundschutzes. Dort wird im BSI-Standard 200-1 „Managementsysteme für Informationssicherheit (ISMS) definiert, welche Anforderungen ein ISMS erfüllen muss. Zusammengefasst ergeben sich die folgenden Prozessschritte, die in einem ISMS-Prozess durchgeführt werden müssen. Veränderte Rahmenbedingungen, wie z. B. Stakeholder-spezifische Vorgaben oder geschäftspolitische Entscheidungen, haben Einfluss auf das aktuelle ISMS. Alle relevanten Anforderungen werden bewertet. Daraus werden gegebenenfalls Informationssicherheitsmaßnahmen abgeleitet sowie deren Umsetzung überwacht. Zusätzlich wird durch den ISMS-Prozess eine kontinuierliche Verbesserung und Weiterentwicklung des Sicherheitsniveaus zur Erhöhung des Reifegrads sichergestellt.

Zur dauerhaften Aufrechterhaltung der Informationssicherheit wird der dargestellte ISMS-Prozess etabliert. Die Aktivitäten werden darin zu einzelnen Prozessschritten zusammengefasst, die dem PDCA-Zyklus (Plan, Do, Check, Act) folgen. Zusätzlich zu diesen definierten Prozessschritten wird ein gesonderter Prozess zur reaktiven Sicherheitsvorfallbehandlung erstellt, um bei etwaigen Sicherheitsvorfällen möglichst effektiv zu agieren.

Die nachfolgende Tabelle stellt die einzelnen Aktivitäten der Prozessschritte zusammengefasst dar. Als letzter Prozess wird die Behandlung von Sicherheitsvorfällen aufgezeigt, da diese nicht direkt mit dem PDCA-Zyklus zusammenhängt.

|  |  |
| --- | --- |
| Prozessschritt gemäß PDCA-Zyklus | Aktivität |
| ISMS gestalten: | Planung und Konzeption desInformationssicherheitsmanagementprozessesBewerten von Auswirkungen auf dieInformationssicherheitIdentifizierung von Änderungen undAbweichungen |
| Vorgaben definieren: | Ermittlung von Informationssicherheitsmaßnahmen |
| Vorgaben umsetzen(inkl. Ausnahmegenehmigungen): | Umsetzen der SicherheitsmaßnahmenDokumentation der Sicherheitsmaßnahmen |
| Sensibilisierung und Schulung: | Sensibilisierung und Schulung der Mitarbeiter |
| Prüfung und Monitoring: | Überprüfung der Einhaltung von VorgabenÜberprüfung der Eignung und Wirksamkeit von Sicherheitsmaßnahmen |
| Berichtswesen: | Berichte an die Geschäftsführung inkl. ggf. Handlungsempfehlungen zur Verbesserung |
| Kontinuierlicher Verbesserungsprozess: | Sicherstellen der kontinuierlichen Verbesserung |
| Sicherheitsvorfallbehandlung: | Reaktiver Prozess zur Bewältigung von Sicherheitsvorfällen |

## ISMS gestalten

Beim Teilprozess „ISMS gestalten“ werden alle internen und externen Anforderungen aufgenommen, bewertet und Anpassungen am ISMS definiert. Der <Informationssicherheitsbeauftragter> prüft regelmäßig Änderungspotenziale und -pflichten, die sich aus den Anforderungen beteiligter Interessengruppen, veränderte Geschäftsprozesse oder -produkte, Standorte oder Interne und externe Anforderungen ergeben. Liegt eine maßgebliche Änderung vor, passt der <Informationssicherheitsbeauftragter> den Informationsverbund an und informiert die Geschäftsführung im Rahmen der Berichterstattung über die Anpassung.

Im Anschluss wird vom <Informationssicherheitsbeauftragter> geprüft, ob Anpassungen bei der konkreten Umsetzung des ISMS notwendig sind. Daraus können neben prozessualen Änderungen auch Umgestaltungen der Inhalte des ISMS-Dokumenten-Frameworks resultieren. Dieser stimmt die prozessualen und dokumentarischen Änderungen mit den betroffenen Fachabteilungen ab, sorgt für die Freigaben, gibt die finalen Dokumente den Mitarbeitenden bekannt und veröffentlich diese zur Transparenz an zentraler für alle Mitarbeitenden zugängliche Stelle. Eine Änderung an der Leitlinie zur Informationssicherheit ist mit der Geschäftsführung abzustimmen.

Die Vorgaben für das ISMS sind mindestens alle zwei Jahre auf Aktualität zu prüfen. Dieser Teilprozess ist auch außerplanmäßig bei maßgeblichen Anforderungen an die Informationssicherheit zu starten, wenn die folgenden wesentlichen Änderungen eintreten:

* Relevanten gesetzlichen Vorgaben
* Vertragliche Anforderungen
* Grundlegende Anpassung der internen Produkt- oder IT-Landschaft
* Interne und externe Anforderungen
* Bedrohungslage

## Vorgaben definieren

Im Teilprozess „Vorgaben definieren“ werden die Informationssicherheitsanforderungen für die einzelnen Zielobjekte (IT-Anwendungen, IT-Systeme, Netze, Räume und Gebäude) und die sich daraus ableitenden Informationssicherheitsmaßnahmen analysiert und definiert. In diesem Prozess prüft der <Informationssicherheitsbeauftragter>, ob eine potenzielle Änderung der Bedrohungslage zu verzeichnen ist. Zudem sind Anpassungen am Informationssicherheitsmanagement zu berücksichtigen und die Vorgehensweise entsprechend an den notwendigen Änderungen auszurichten.

Anschließend ist zu prüfen, ob Änderungen an den IT-Anwendungen, IT-Systemen, Netzen oder Gebäuden vorgenommen wurden. Liegen Änderungen vor, sind diese in der Strukturanalyse zu aktualisieren. Sofern Änderungen an den Gebäuden vorgenommen wurden, sind die Änderungen in der Strukturanalyse zu beschreiben.

Im Anschluss werden die Schutzbedarfe (Verfügbarkeit, Vertraulichkeit und Integrität) an den Geschäftsprozessen erhoben und definiert. Insofern Änderungen vorliegen, veranlasst der <Informationssicherheitsbeauftragter> mit Unterstützung der Fachbereiche eine Aktualisierung der Schutzbedarfsfeststellung. Die Schutzbedarfsfeststellung und die Vererbung des Schutzbedarfs erfolgen gemäß den Vorgaben des BSI Standards 200-2 IT-Grundschutz-Methodik.

Falls neue Zielobjekte oder veränderte Vorgaben der relevanten Sicherheitsstandards identifiziert wurden, wird durch den <Informationssicherheitsbeauftragter> die Modellierung angepasst.

Der <Informationssicherheitsbeauftragter> entscheidet über die Notwendigkeit und initiiert die Durchführung einer Risikoanalyse gemäß den Vorgaben aus dem BSI Standard 200-3 „Risikomanagement“. Falls eine Risikoanalyse notwendig ist, werden die entsprechenden Informationen zur Durchführung einer Risikoanalyse an das Risikomanagement übergeben. Die Ergebnisse der Risikoanalyse werden anschließend an den <Informationssicherheitsbeauftragter> zurückgegeben. Dieser aggregiert diese und identifiziert alle zusätzlichen Informationssicherheitsmaßnahmen.

Abschließend werden alle identifizierten Informationssicherheitsmaßnahmen geprüft, inwieweit sie bereits umgesetzt sind. Alle offenen Informationssicherheitsmaßnahmen werden an den nächsten Prozess zur Umsetzung übergeben.

Dieser Teilprozess ist bei relevanten externen Anforderungen zu starten, wie z. B.

* relevante gesetzliche Vorgaben
* vertragliche Anforderungen
* grundlegende Anpassung der internen Produkt- oder IT-Landschaft
* Interne und externe Anforderungen
* neue / geänderte Vorgaben von relevanten Sicherheitsstandards (BSI IT-Grundschutz)
* Meldungen über tatsächliche und potenzielle Schwachstellen und Sicherheitsvorfälle

Der Schutzbedarf jedes Zielobjekts (Anwendungen, IT-Systeme, Netze, Räume und Gebäude) muss mindestens einmal in zwei Jahren geprüft werden. Die IT-Grundschutz-Checks für die Zielobjekte sind mindestens einmal im Jahre durchzuführen. Bei Änderungen des ISMS durch den Prozess „ISMS gestalten“ ist zu prüfen, ob dieser Teilprozess ebenfalls gestartet werden muss.

## Vorgaben umsetzen

In diesem Prozess werden alle offenen Informationssicherheitsmaßnahmen aus dem Teilprozess „Vorgaben definieren“ konkretisiert und eine Entscheidung herbeigeführt, ob diese umgesetzt werden.

Der Prozess wird initialisiert, sobald durch den <Informationssicherheitsbeauftragter> im „Vorgaben definieren“ offene Informationssicherheitsmaßnahmen identifiziert wurden, die umgesetzt werden sollen. Diese Sicherheitsmaßnahmen werden konkretisiert, indem für jede jeweils konkrete Umsetzung die notwendigen Ressourcen und Verantwortlichkeiten geplant werden. Die Verantwortlichen der einzelnen Bereiche entscheiden, ob die konkreten Maßnahmen auch tatsächlich umgesetzt werden. Die Entscheidungen über die Umsetzung von Schutzmaßnahmen werden durch den <Informationssicherheitsbeauftragter> nachgehalten.

Die Umsetzungsmöglichkeiten sind mit dem <Informationssicherheitsbeauftragter> und bei der Verarbeitung von personenbezogenen Daten mit der <Data Protection Commissioner> abzustimmen. Bei der Konzeption der Sicherheitsvorgaben sind alle Bereiche zu beteiligen, auf die die Informationssicherheitsvorgaben Auswirkungen haben.

Die Umsetzung der Informationssicherheitsmaßnahme erfolgt durch den jeweiligen thematischen Verantwortlichen. Die thematisch Verantwortlichen für die Umsetzung der abgestimmten Maßnahmen melden an den <Informationssicherheitsbeauftragter> die Fertigstellung. Der Information Security Officer prüft wiederum, ob die in der Umsetzungsplanung vereinbarten Termine eingehalten werden. Abweichungen werden vom <Informationssicherheitsbeauftragter> an die Geschäftsführung berichtet und sobald erforderlich eskaliert, um weitere Unterstützung zu erhalten.

Falls Informationssicherheitsmaßnahmen nicht umgesetzt werden oder die Umsetzung lange dauert, muss das Risikomanagement im ISMS sicherstellen, dass die dadurch entstehenden Risiken identifiziert und mit Risikobehandlungsmaßnahmen hinterlegt werden. Alternative Maßnahmen können einerseits die ursprüngliche Maßnahme komplett ersetzen, da dadurch ein vergleichbares Sicherheitsniveau erreicht wird. Andererseits können auch zusätzliche Maßnahmen, wie beispielsweise die Sensibilisierung von Beteiligten, ergriffen werden, um den Risiken der nicht umgesetzten Maßnahmen entgegenzuwirken.

## Sensibilisierung und Schulung

Beim Teilprozess „Sensibilisierung und Schulung“ werden alle relevanten Sensibilisierungs- und Schulungsmaßnahmen des ISMS geplant, durchgeführt und ausgewertet. Der Schulungs- und Sensibilisierungsplan wird jedes Jahr neu erstellt. Diese Planung wird zudem bei allen Änderungen des Sensibilisierungs- und Schulungsprogramms und bei relevanten Ereignissen auf Aktualität überprüft.

Die aktuelle Bedrohungslage, die umgesetzten beziehungsweise noch umzusetzenden Informationssicherheitsmaßnahmen aus den Teilprozessen „Vorgaben definieren“ und „Vorgaben umsetzen“ sowie die aus der Risikoanalyse ermittelten Risiken verdeutlichen die relevanten Themen für zukünftige Sensibilisierungs- und Schulungsmaßnahmen. Aus den Ergebnissen von Audits und Sicherheitsüberprüfungen lassen sich weitere Sensibilisierungs- und Schulungsmaßnahmen herleiten. Das Sensibilisierungs- und Schulungsprogramm wird bei relevanten Ereignissen durch den <Informationssicherheitsbeauftragter> auf Aktualität geprüft.

Jährlich werden auf Basis des Sensibilisierungs- und Schulungsprogramms durch den <Informationssicherheitsbeauftragter> die erforderlichen Sensibilisierungs- und Schulungsmaßnahmen abgleitet und um aktuelle Bedrohungen ergänzt.

Die Mittel für die geplanten Sensibilisierungs- und Schulungsmaßnahmen sind im Budget der Informationssicherheit enthalten. Der <Informationssicherheitsbeauftragter> koordiniert die Umsetzung der Sensibilisierungs- und Schulungsmaßnahmen.

## Prüfung

Im Teilprozess „Prüfung“ werden alle relevanten Prüfungen und die regelmäßige Überwachung (Monitoring) des ISMS geplant, durchgeführt und ausgewertet. Das Prüfprogramm wird in einem dreijährigen Rhythmus neu erstellt und mindestens einmal jährlich oder bei relevanten Ereignissen auf Aktualität geprüft.

Für die Erstellung des Prüfprogramms werden die relevanten Themen aus den folgenden Aspekten abgeleitet:

* Schutzbedarf von Geschäftsprozessen beziehungsweise Anwendungen
* Auslagerungen mit hohen identifizierten Schutzbedarfen
* Umgesetzte oder umzusetzende Informationssicherheitsmaßnahmen
* Sicherheitsrelevante Ereignisse

Für jedes Jahr erfolgt eine Detailplanung durch den <Informationssicherheitsbeauftragter> auf Basis des Prüfprogramms und die Durchführung/Begleitung der tatsächlichen Prüfungen. Es sind Mittel für die abgestimmten Maßnahmen in der Mittelfristplanung zusammen mit der Geschäftsführung einzuplanen und freizugeben.

Falls bei einer der Prüfungen ein potenzieller Sicherheitsvorfall identifiziert wird, werden angemessene Maßnahmen initiiert und umgesetzt. Durch die Auswertung der Prüfungen können Erkenntnisse gewonnen werden, welche auch in die Planung zukünftiger Prüfungen einfließen. Die Ergebnisse werden der Geschäftsführung erläutert und auf mögliche Risiken wird hingewiesen, um angemessene Entscheidungen zur weiteren Vorgehensweise zu ermöglichen.

## Berichtswesen und Monitoring

Über den Teilprozess „Berichtwesen und Monitoring“ werden allen berechtigten Interessengruppen relevante Informationen des ISMS zur Verfügung gestellt, auf deren Grundlage betriebliche Entscheidungen getroffen werden können.

Zu den berechtigten Interessengruppen gehören unter anderem:

* Geschäftsführung
* Revision
* Wirtschaftsprüfer
* Auditoren
* <Investoren>
* <Kunden>

Die Geschäftsführung erhält einen jährlichen Bericht zur Informationssicherheit. Dieser Bericht wird in der Managementrunde vorgestellt und erläutert.

Zudem dokumentiert der <Informationssicherheitsbeauftragter> besondere Ereignisse (z. B. Sicherheitsvorfälle) und erstellt Berichte für berechtigte Interessengruppen.

## Kontinuierlicher Verbesserungsprozess

Der „Kontinuierliche Verbesserungsprozess“ prüft, ob das ISMS und die Informationssicherheitsprozesse erwartungskonform funktionieren und ob diese gegebenenfalls noch erweitert werden sollen. Auf Basis dieser Erkenntnisse werden Verbesserungspotenziale definiert und an den Prozess „ISMS gestalten“ übergeben.

Falls bei den Teilprozessen offensichtlich wird, dass die gewünschte Funktionsweise nicht gewährleistet werden kann, werden diese Rückmeldungen im „Kontinuierlichen Verbesserungsprozess“ bearbeitet. Zusätzlich wird mindestens alle drei Jahre das ISMS überprüft und analysiert, ob die Teilprozesse und deren Umsetzung noch angemessen sind oder möglicherweise weiter verbessert werden können.

Der <Informationssicherheitsbeauftragter> überprüft, ob das ISMS und der Informationssicherheitsprozess noch angemessen sind. Falls Abweichungen von der gewünschten Funktionsweise des Informationssicherheitsprozesses oder mögliche Verbesserungen im ISMS identifiziert sind, werden Anpassungen am Prozess geprüft und zur Weiterentwicklung des ISMS an den Teilprozess „ISMS gestalten“ übergeben.

## Behandlung von Sicherheitsvorfällen

Im Teilprozess „Behandlung von Sicherheitsvorfällen“ werden alle potenziellen Sicherheitsvorfälle aufgenommen, bewertet und entsprechend behandelt. Da bei einem Sicherheitsvorfall in der Regel schnelles Handeln notwendig ist, befindet sich die detaillierte Beschreibung der Vorgänge in der separaten Sicherheitsrichtlinie „Behandlung von Sicherheitsvorfällen“.

Da die Meldungen über potentielle Schnittstellen von verschiedenen Interessengruppen (z. B. Mitarbeiter, Kunden, Dienstleister), IT-Systemen oder Anwendungen kommen können, müssen geeignete Meldestellen für die Kommunikation etabliert werden. Über diese Meldestellen sind schnellstmöglich die verantwortlichen Mitarbeiter zu informieren. Diese bewerten die Meldungen und leiten alle kritischen Sicherheitsvorfälle unverzüglich an den <Informationssicherheitsbeauftragter> weiter. Dieser meldet diese an die Geschäftsführung.

Anschließend wird sichergestellt, dass durch den Sicherheitsvorfall keine weiteren Schäden entstehen können. Dabei ist abzuwägen, inwieweit eine Beweismittelsicherung notwendig ist. Bei der Beweismittelsicherung ist darauf zu achten, dass keine relevanten Beweismittel bei der Eindämmung zerstört werden. Die Eindämmung wird durch die für das betroffene Zielobjekt verantwortlichen Mitarbeiter durchgeführt. Bei Bedarf können für die Eindämmung zusätzliche Bereiche mit eingebunden werden.

Nachdem ein Sicherheitsvorfall eingedämmt wurde, sind Untersuchungen durchzuführen, um die Ursachen zu finden. Falls gerichtsverwertbare Informationen notwendig sind, sollte eine forensische Untersuchung durchgeführt werden. Die Entscheidung darüber wird durch das Sicherheitsvorfallteam getroffen. Die forensischen Untersuchungen können sowohl durch entsprechend geschulte Mitarbeitende als auch durch externe Dienstleister durchgeführt werden.

Durch die Systemverantwortlichen wird anschließend die Ursachenuntersuchung (u. a. Problem Management) und die Rückkehr in den Normalbetrieb bzw. zur Arbeitsfähigkeit durch Workarounds (Incident-Management) durchgeführt. Alle relevanten Entscheidungen und Aktivitäten sind gemäß der Sicherheitsrichtlinie „Behandlung von Sicherheitsvorfällen“ dokumentiert.

Im Anschluss an die Behebung der Sicherheitsvorfälle wertet der Information Security Officer alle dokumentierten Ereignisse zu den Sicherheitsvorfällen aus. Er prüft, ob in den einzelnen Phasen Verbesserungspotenzial für die zukünftige Behandlung von Sicherheitsvorfällen vorhanden ist und entwickelt Verbesserungsvorschläge.