

ISO/IEC 27001
ISO/IEC 27002
und IT-Grundschutz

Schnelleinstieg
Informationssicherheit
2022

Jacqueline Naumann

Autorin



Jacqueline Naumann ist studierte Informatikerin und trainiert Erwachsene seit vielen Jahren zur Informationssicherheit. Im Jahr 2015 gründete sie das IT-Beratungsunternehmen iXactly in Dresden. Seit 2017 ist sie berufener Zertifizierungsauditor für ISO/IEC 27001 und wurde im Oktober 2020 vom BSI zum IT-Grundschutz-Berater zertifiziert.

Regelmäßig laden Organisationen Frau Naumann ein, um interne Sicherheitsprozesse zu überprüfen, zu verbessern oder zu zertifizieren.

Naumann hat bereits einige Bücher zur Informationssicherheit für Erwachsene und Kinder geschrieben. Sie entschied deshalb, ihre Seminare zur ISO/IEC 27001 und ISO/IEC 27002 auch als Buch herauszubringen. Das Ergebnis liegt mit diesem Titel vor.

Inhalt

1 Einleitung

- 1.1 Zum Inhalt
- 1.2 Dankesworte

2 Begriffe zur Informationssicherheit

- 2.1 Information
- 2.2 Vertraulichkeit
- 2.3 Integrität
- 2.4 Verfügbarkeit
- 2.5 Authentizität
- 2.6 Verantwortlichkeit (Zurechenbarkeit)
- 2.7 Verbindlichkeit (Nicht-Abstreitbarkeit)
- 2.8 Verlässlichkeit
- 2.9 Prozesse
- 2.10 System / Managementsystem
- 2.11 Informationssicherheitsmanagementsystem (ISMS)

3 ISO/IEC 27001

- 3.1 Kompatibilität zu anderen Managementsystemen
- 3.2 Historie
- 3.3 Auszug aus der ISO/IEC 27000er-Reihe
- 3.4 Mögliche Motivationen für ein ISMS
- 3.5 Schadensauslöser in der Informationssicherheit
- 3.6 Initiieren des Sicherheitsprozesses

- 3.7 PDCA-Methodik – Deming-Kreislauf
- 3.8 ISO High Level Structure
- 3.9 Anwendungsbereich ISO/IEC 27001
- 3.10 ISMS-Aufbau mit der PDCA-Methodik
- 3.11 PDCA in ISO 27001 und BSI-Standard 200-1
- 3.12 ISMS-Aufbau nach IT-Grundschutz

4 Kontext der Organisation

- 4.1 Geltungsbereich
- 4.2 Zertifizierungsscope

5 Führung

- 5.1 Leitlinie
- 5.2 Rollen und Verantwortlichkeiten

6 Risiken und Chancen

- 6.1 Asset-Inventar
- 6.2 Werte der Organisation
- 6.3 Risikomanagement
 - 6.3.1 Risikobewertungskriterien
 - 6.3.2 Schutzbedarfskategorien
 - 6.3.3 Risikobewertungsmatrix
 - 6.3.4 Risikobeurteilung
- 6.4 Risikosteckbrief
- 6.5 IT-Sicherheitskonzept nach BSI-Standard 200-2
 - 6.5.1 Sächsisches Informationssicherheitsgesetz
- 6.6 Statement of Applicability (SoA)
- 6.7 Maßnahmenplanung
- 6.8 IT-Grundschutz Kompendium

7 Unterstützung

- 7.1 Ressourcen
- 7.2 Kompetenz
- 7.3 Sensibilisierung der Belegschaft
- 7.4 Kommunikation
- 7.5 Dokumentierte Information
 - 7.5.1 Dokumente
 - 7.5.2 Aufzeichnung
 - 7.5.3 Dokumentenlenkung
 - 7.5.4 Umsetzung von ISMS-Dokumentation

8 Betrieb

- 8.1 Prozesslandkarte
- 8.2 Informationssicherheitsereignis
- 8.3 Social Engineering als Sicherheitsrisiko
- 8.4 Meldeprozess
 - 8.4.1 Sofortmaßnahmen
 - 8.4.2 Korrekturmaßnahmen

9 Bewertung der Leistung

- 9.1 Analysieren, Bewerten und Messen
 - 9.1.1 Kennzahlen
 - 9.1.2 Ziele
- 9.2 Interne Audits
 - 9.2.1 Audit
 - 9.2.2 Auditprogramm
 - 9.2.3 Auditplan
 - 9.2.4 Auditor
 - 9.2.5 Auditfrageliste
 - 9.2.6 Konformität und Nichtkonformität
 - 9.2.7 Auditbericht

9.3 Managementbewertung

10 Verbesserung

11 ISO/IEC 27002

11.1 Aufbau ISO/IEC 27002

11.1.1 Steuerungstypen / Maßnahmentyp

11.1.2 Informationssicherheitseigenschaften

11.1.3 Cybersicherheitskonzepte

11.1.4 Operative / Betriebliche Fähigkeiten

11.1.5 Sicherheitsmaßnahmen

11.1.6 Anhänge der ISO/IEC 27002

A.5 Organisatorische Sicherheitsmaßnahmen

.. Interne Organisation

A.5.1 Informationssicherheitsrichtlinien

A.5.2 Informationssicherheitsrollen und Verantwortlichkeiten

A.5.3 Aufgabentrennung

A.5.4 Verantwortlichkeiten der Leitung

A.5.5 Kontakt mit Behörden

A.5.6 Kontakt zu speziellen Interessengruppen

A.5.7 Bedrohungsintelligenz

A.5.8 Informationssicherheit im Projektmanagement

.. Verwaltung von Werten

A.5.9 Inventar der Informationen und anderen damit verbundenen Werten

A.5.10 Zulässiger Gebrauch von Informationen und anderen damit verbundenen Werten

A.5.11 Rückgabe von Werten

A.5.12 Klassifizierung von Information

A.5.13 Kennzeichnung von Information

A.5.14 Informationsübertragung

.. **Verwaltung von Rechten**

A.5.15 Zugangssteuerung

A.5.16 Identitätsmanagement

A.5.17 Informationen zur Authentifizierung

A.5.18 Zugangsrechte

.. **Lieferantenbeziehungen**

A.5.19 Informationssicherheit in
Lieferantenbeziehungen

A.5.20 Behandlung von Informationssicherheit in
Lieferantenvereinbarungen

A.5.21 Umgang mit der Informationssicherheit in
der IKT-Lieferkette

A.5.22 Überwachung, Überprüfung und
Änderungs-management von
Lieferantendienstleistungen

A.5.23 Informationssicherheit für die Nutzung
von Cloud-Diensten

.. **Informationssicherheitsvorfälle**

A.5.24 Planung und Vorbereitung der
Handhabung von
Informationssicherheitsvorfällen

A.5.25 Beurteilung und Entscheidung über
Informationssicherheitsereignisse

A.5.26 Reaktion auf
Informationssicherheitsvorfälle

A.5.27 Erkenntnisse aus
Informationssicherheitsvorfällen

A.5.28 Sammeln von Beweismaterial

A.5.29 Informationssicherheit bei Störungen

A.5.30 IKT-Bereitschaft für Business Continuity

.. **Compliance**

A.5.31 Rechtliche, gesetzliche, regulatorische und vertragliche Anforderungen

A.5.32 Geistige Eigentumsrechte

A.5.33 Schutz von Aufzeichnungen

A.5.34 Datenschutz und Schutz personenbezogener Daten (pbD)

A.5.34 Praxisbeispiel: Chat-Monitoring

.. **Interne Regeln und Dokumentation**

A.5.35 Unabhängige Überprüfung der Informationssicherheit

A.5.36 Einhaltung von Richtlinien, Vorschriften und Normen für die Informationssicherheit

A.5.37 Dokumentierte Betriebsabläufe

A.5.37 Praxisbeispiel: Unnütze Mappen

A.6 Personenbezogene Sicherheitsmaßnahmen

.. **Vor der Beschäftigung**

A.6.1 Sicherheitsüberprüfung

A.6.2 Beschäftigungs- und Vertragsbedingungen

.. **Während der Beschäftigung**

A.6.3 Informationssicherheitsbewusstsein, -ausbildung und -schulung

A.6.4 Maßregelungsprozess

.. **Nach der Beschäftigung**

A.6.5 Verantwortlichkeiten bei Beendigung oder Änderung der Beschäftigung

A.6.6 Vertraulichkeits- oder Geheimhaltungsvereinbarungen

.. **Mobiles Arbeiten**

A.6.7 Telearbeit

.. **Meldeprozess**

A.6.8 Meldung von
Informationssicherheitsereignissen

A.7 Physische Sicherheitsmaßnahmen

.. **Physische Sicherheit**

A.7.1 Physische Sicherheitsperimeter

A.7.2 Physischer Zutritt

A.7.3 Sicherung von Büros, Räumen und
Einrichtungen

A.7.4 Physische Sicherheitsüberwachung

.. **Bedrohungen**

A.7.5 Schutz vor physischen und
umweltbedingten Bedrohungen

.. **Arbeitsplätze**

A.7.6 Arbeiten in Sicherheitsbereichen

A.7.7 Aufgeräumte Arbeitsumgebung und
Bildschirm Sperren

A.7.7 Praxisbeispiel: Rezepte am offenen Fenster

.. **Umgang mit Werten**

A.7.8 Platzierung und Schutz von Geräten und
Betriebsmitteln

A.7.8 Praxisbeispiel: Wöchentliche Stromausfälle

A.7.9 Sicherheit von Werten außerhalb der
Räumlichkeiten

.. **Betriebsmittel**

A.7.10 Speichermedien

A.7.11 Versorgungseinrichtungen

A.7.12 Sicherheit der Verkabelung

.. **Wartung und Entsorgung**

A.7.13 Instandhaltung von Geräten und Betriebsmitteln

A.7.14 Sichere Entsorgung oder Wiederverwendung von Geräten und Betriebsmitteln

A.8 Technologische Sicherheitsmaßnahmen

.. **Zugangssicherheit**

A.8.1 Endpunktgeräte des Benutzers

A.8.2 Privilegierte Zugangsrechte

A.8.3 Informationszugangsbeschränkung

A.8.4 Zugriff auf den Quellcode

A.8.5 Sichere Authentifizierung

A.8.5 Praxisbeispiel: Drei-Faktor-Authentifizierung

.. **Betriebssicherheit**

A.8.6 Kapazitätssteuerung

A.8.7 Schutz gegen Schadsoftware

A.8.8 Handhabung von technischen Schwachstellen

A.8.9 Konfigurationsmanagement

.. **Datensicherheit**

A.8.10 Löschung von Informationen

A.8.11 Datenmaskierung

A.8.12 Verhinderung von Datenlecks

A.8.13 Sicherung von Information

.. **Administration**

A.8.14 Redundanz von informationsverarbeitenden Einrichtungen

- A.8.15 Protokollierung
- A.8.16 Überwachung von Aktivitäten
- A.8.16 Praxisbeispiel: Naschender Vermieter
- A.8.17 Uhrensynchronisation
- A.8.18 Gebrauch von Hilfsprogrammen mit privilegierten Rechten
- A.8.19 Installation von Software auf Systemen im Betrieb

- .. **Netzicherheit**

- .. ISO/OSI-Schichtenmodell
- A.8.20 Netzwerksicherheit
- A.8.21 Sicherheit von Netzwerkdiensten
- A.8.22 Trennung von Netzwerken

- .. **Netzplan Aufbau**

- Legende-Kachel
- Standort-Kachel
- Schnittstellen-Kachel
- Prozesse außerhalb des Scopes - Kachel
- A.8.23 Webfilterung
- A.8.24 Verwendung von Kryptographie

- .. **Entwicklungssicherheit**

- A.8.25 Lebenszyklus einer sicheren Entwicklung
- A.8.26 Anforderungen an die Anwendungssicherheit
- A.8.27 Sichere Systemarchitektur und technische Grundsätze
- A.8.28 Sicheres Coding
- A.8.29 Sicherheitsüberprüfung in Entwicklung und Abnahme

- .. **Änderungsmanagement**

A.8.30 Ausgegliederte Entwicklung

A.8.31 Trennung von Entwicklungs-, Prüf- und Produktionsumgebungen

A.8.31 Praxisbeispiel: Endlos-Schleife führt zum Flaschenhals

A.8.32 Änderungssteuerung

A.8.33 Prüfinformationen (Testdaten)

.. **Technische Überprüfungen**

A.8.34 Schutz der Informationssysteme während der Überwachungsprüfung

Anhang B.1 der ISO/IEC 27002 - neue Maßnahmen

Anhang B.2 der ISO/IEC 27002 - Zuordnung 2013

12 IT-Grundschatz-Kompendium

12.1 Gefährdungen

12.2 Bausteine

12.3 Basis-Absicherung

12.4 Standard-Absicherung

12.5 Kern-Absicherung

12.6 Kreuzreferenz-Tabellen

12.7 IT-Grundschatz-Profile

13 Zertifizierung nach ISO/IEC 27001

13.1 Vorbereitung zur Zertifizierung

13.2 Ablauf Zertifizierung

13.3 Gültigkeit des ISO/IEC 27001-Zertifikates

Schlusswort

ANLAGE 1: Übersicht DIN ISO/IEC 27001

ANLAGE 2: Übersicht Kapitel 5-8 DIN ISO/IEC 27002

Quellenangaben

Tabellenverzeichnis

Abbildungsverzeichnis

Verzeichnis der Zeichnungen

Index

Literaturempfehlung

1 Einleitung

Dieses Buch unterstützt Sie beim Aufbau Ihres Informationssicherheitsmanagementsystems (ISMS) und bereitet Sie auf eine Zertifizierung nach ISO/IEC 27001:2022 vor.

Für die Kapitelstrukturen sowie deren Bezeichnungen in diesem Buch, habe ich mich an der **DIN ISO/IEC 27001** sowie an der **DIN ISO/IEC 27002** orientiert.

Sie werden für Ihre Arbeit einfache Umsetzungsmöglichkeiten mit vielen Praxisbeispielen in den Kapiteln vorfinden.

1.1 Zum Inhalt

In **Kapitel 2** erläutere ich für absolute Einsteiger Begriffe der Informationssicherheit.

In **Kapitel 3** vermittele ich Ihnen die Grundlagen, den Aufbau und die Historie zum normativen Standard **ISO/IEC 27001**. Außerdem erläutere ich Ihnen, wie Sie mit BSI-Standards ein ISMS nach IT-Grundschutz umsetzen könnten.

Die anschließenden **Kapitel 4** bis **10** entsprechen den Normkapiteln der ISO/IEC 27001. Hier erkläre ich Ihnen die Mindestanforderungen und zeige Ihnen einfache praktische Umsetzungsbeispiele.

In **Kapitel 11** erläutere ich Ihnen den Aufbau des informativen Standards **DIN ISO/IEC 27002**.

Unmittelbar danach folgen vier Kapitel, die den Hauptkapiteln der ISO/IEC 27002 und somit dem **Anhang A** der ISO/IEC 27001 entsprechen. Es handelt sich um die Kapitel **A.5 Organisatorische Sicherheitsmaßnahmen**, **A.6 Personenbezogene Sicherheitsmaßnahmen**, **A.7 Physische Sicherheitsmaßnahmen** und **A.8 Technologische Sicherheitsmaßnahmen**. In diesen vier Kapiteln zeige ich Ihnen die Eigenschaften aller 93 Sicherheitsmaßnahmen sowie die jeweils konkret empfohlenen Maßnahmen. Außerdem nenne ich Ihnen in stark komprimierter Form zu jeder Maßnahme einige Umsetzungsempfehlungen. Zusätzlich habe ich allen Maßnahmen einige Piktogramme zur besseren visuellen Merkbarkeit zugeordnet.

Im Anschluss folgt ein knapper Auszug aus dem **Anhang B.1** der ISO/IEC 27002. Ich zeige Ihnen an der Stelle die Maßnahmen, die im Jahr 2022 hinzugekommen sind. Darauf folgen ebenfalls stark gekürzt einige Beispiele aus dem **Anhang B.2** der ISO/IEC 27002. Hier stelle ich einige Maßnahmennummern aus 2013 denen im Jahr 2022 gegenüber.

In **Kapitel 12** widme ich mich dem **IT-Grundschutz-Kompendium** und zeige Ihnen Umsetzungsbeispiele und erkläre Anforderungen für eine Zertifizierung nach IT-Grundschutz.

Kapitel 13 ist das letzte Kapitel im Buch. In diesem Abschnitt erläutere ich Ihnen, wie eine **Zertifizierung** nach ISO/IEC 27001:2022 abläuft und wie lange Zertifikate gültig sind.

Ich hoffe, die Lektüre dieses Buches bereitet Ihnen genauso viel Vergnügen, wie mir sein Schreiben und Gestalten und

Sie werden für die nahenden ISMS-Aufgaben gut gecoacht und fühlen sich anschließend bereichert.

1.2 Dankesworte

Als erstes möchte ich dem **DIN** (Deutsches Institut für Normung) danken, für die Erlaubnis, Auszüge aus DIN-Normen zu zitieren.

Außerdem möchte ich dem **BSI** (Bundesamt für Sicherheit in der Informationstechnik) danken, für die freie Zugänglichkeit zu den **BSI-Standards**, zum immer aktuell gehaltenen **IT-Grundschutz-Kompendium** sowie zu den **IT-Grundschutz-Profilen** auf der BSI-Webseite.

Kein Buch lebt von grauer Theorie, deshalb werden Sie in diesem Buch viele farbige Praxisbeispiele entdecken. Da allerdings nicht alle Beispiele oder Zeichnungen von mir sind, möchte ich mich nun bei den ursprünglichen Autoren bedanken.

Mein ganz besonderer Dank gilt **David Müller** von der *Dresden-IT* sowie **André Schiller** und **Kristin Völker** von der *Dresdner Verkehrsbetriebe*. Diese drei Informationssicherheitsbeauftragten entwickelten einen aufgeräumten und einfach erklärbaren Netzplan, der alle BSI-Anforderungen erfüllt. Auf Seite → zeige ich Ihnen ein leicht abgewandeltes und anonymisiertes Beispiel dieses Netzplans und nenne ihn **Müller-Schiller-Völker-Netzplan**, kurz **MSV-Netzplan**.

Der nächste Dank gilt **Sven Müller** von der *gevekom ONE*, der eine übersichtliche Risikobeurteilung und Bewertung in einer Score-Tabelle entwickelt hat. Im Buch zeige ich Ihnen eine leicht angepasste Version auf Seite → von ihm.

Zuletzt möchte ich **Florentine Naumann** danken. Sie zeichnete für die Buchreihe »*Die ganze Härte der ISO 27001*« Bilder, von denen ich auch in diesem Buch einige einsetze.

2 Begriffe zur Informationssicherheit

Im zweiten Kapitel dieses Buches erläutere ich Ihnen anhand von Zeichnungen Begriffe zur Informationssicherheit.

Meine Zeichnungen zeigen fiktive Charaktere und ich möchte an dieser Stelle einmalig erwähnen, das Buch ist für alle vorstellbaren menschlichen Identitäten gedacht.

Da es sich bei diesem Buch um ein Fachbuch handelt, werde ich, wenn ich über Individuen schreibe, immer die kürzest mögliche derzeit gültige Form verwenden.

Damit möchte ich Ihre Aufmerksamkeit beim Lesen besonders auf die fachlichen Inhalte lenken.

Hinweis:

Wenn Sie bereits Grundlagen-Kenntnisse zur Informationssicherheit besitzen, können Sie dieses Kapitel schnell überfliegen oder direkt zum Kapitel »3 ISO/IEC 27001« auf Seite [→](#) springen.

2.1 Information

Zu Beginn definiere ich den Begriff ›Information‹ mit meinen Worten.

Die Welt besteht aus Objekten. Diese können Lebewesen oder Gegenstände sein. Zu jedem Objekt gibt es unterschiedliche Fakten, also Eigenschaften. Aber nur einige dieser Fakten sind für uns im Unternehmen relevant. Relevante Fakten werden Information genannt. Und wenn diese Informationen zusätzlich dokumentiert sind, können wir von dokumentierten Informationen sprechen.

Im Bild unten sehen wir eine Person, die ebenfalls einige Eigenschaften besitzt. Aber für eine Personalabteilung wird lediglich der dokumentierte Nachweis des Abschlusszeugnisses relevant sein.

Achten Sie bei der Dokumentation stets auf relevante Fakten.

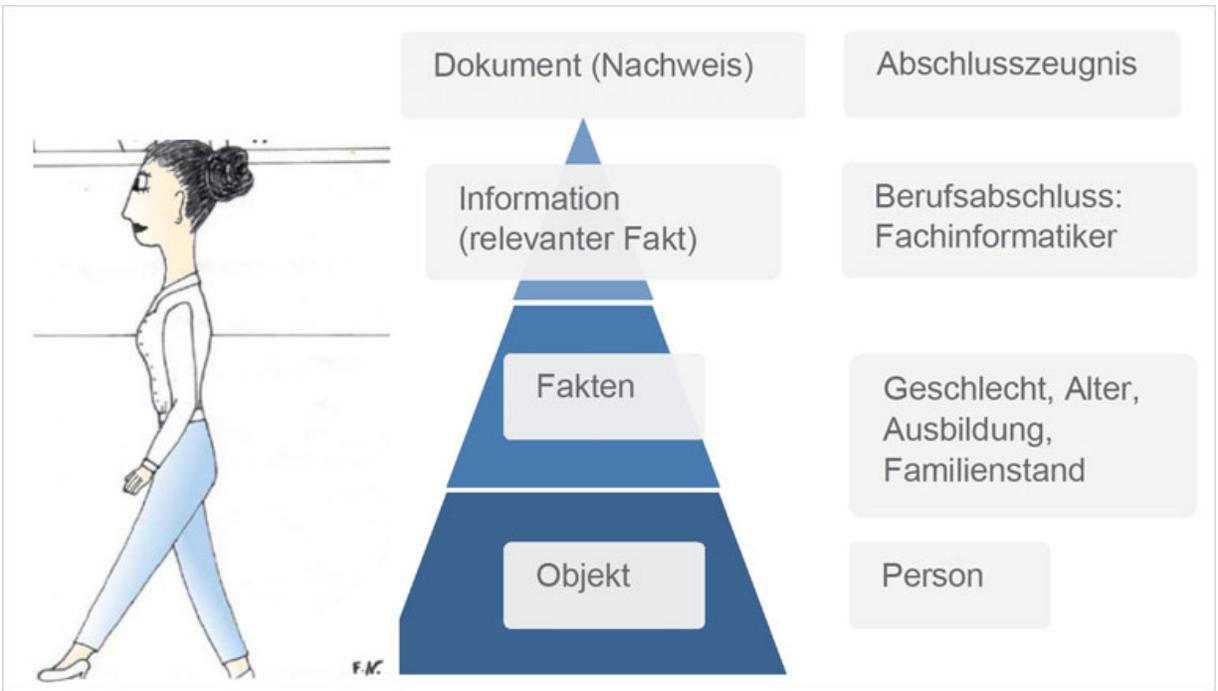


Abbildung 1: Information

2.2 Vertraulichkeit

Der Begriff ›Vertraulichkeit‹ bedeutet, Informationen oder Werte dürfen nur von Berechtigten eingesehen werden.

Eine Verletzung gegen die Vertraulichkeit wäre beispielsweise die Offenlegung geheimer Informationen oder der Missbrauch personenbezogener Daten.

Beispiel für einen Verstoß: Vorname, Nachname, Geburtsdatum und Geburtsort werden durch Unbefugte für Internetgeschäfte genutzt.

Die folgende Abbildung zeigt, Freddy ist nicht befugt, die Informationen von Schnokk zu lesen. Könnte er die Daten dennoch einsehen oder abgreifen, wäre dies eine Verletzung der Vertraulichkeit.

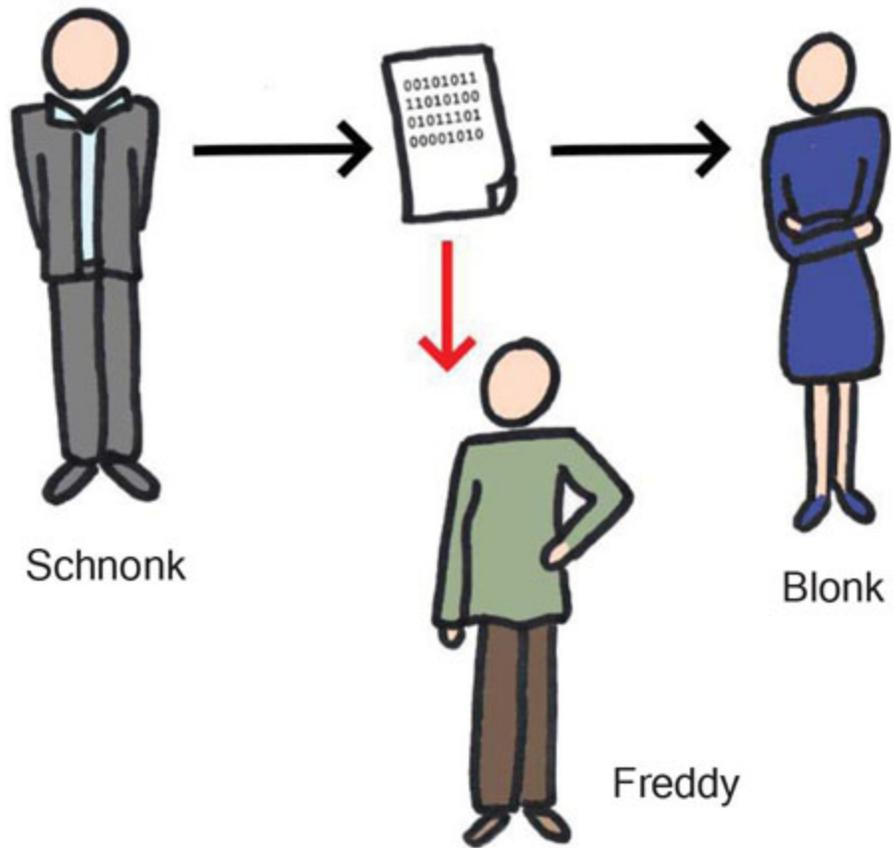


Abbildung 2: Vertraulichkeit

2.3 Integrität

Der Begriff ›Integrität‹ bedeutet, Daten und Informationen liegen unverändert vor. Integrität ist der Schutz von Informationen vor Modifikation, Einfügung, Löschung, Umordnung oder Duplikaten.

Eine Verletzung gegen die Integrität wäre zum Beispiel das Einfügen zusätzlicher Angaben in Nachweisdokumenten.

Beispiel für einen Verstoß: Die Änderung von Vornamen, Nachnamen, Geburtsdatum, Geburtsort oder Zensuren auf einem Abschlusszeugnis.

Die folgende Abbildung zeigt, Freddy hat das Dokument von Schonk abgefangen und vor der Weiterleitung manipuliert.

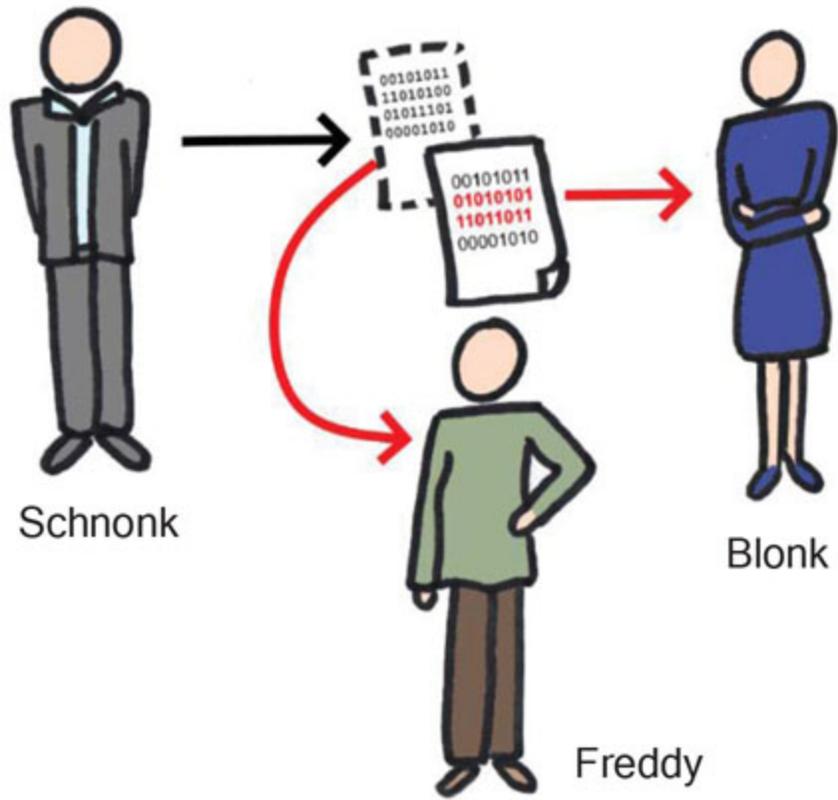


Abbildung 3: Integrität

2.4 Verfügbarkeit

Der Begriff ›Verfügbarkeit‹ besagt, Berechtigte können zu jeder Zeit auf Informationen, Daten oder beliebige Systeme zugreifen.

Eine Verletzung der Verfügbarkeitsansprüche bestünde, wenn Berechtigte keine Möglichkeit des Zugreifens oder Ansehens bekämen.

Beispiel für einen Verstoß: Das Abschlusszeugnis ist als verschlüsselte Datei abgelegt und kann nicht eingesehen werden, weil der Schlüssel verloren ging.

Die folgende Abbildung soll darstellen, Schonk ist berechtigt, auf Dokumente im Tresor permanent zuzugreifen.

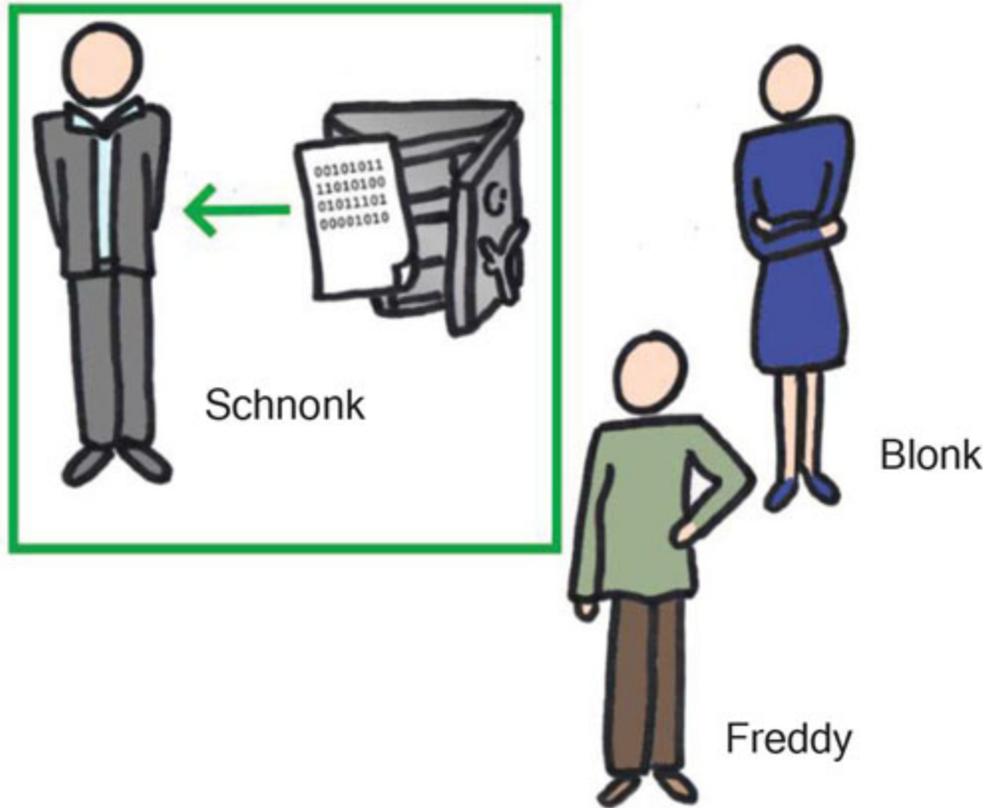


Abbildung 4: Verfügbarkeit

2.5 Authentizität

Der Begriff ›Authentizität‹ gibt an, die Echtheit von Informationen oder Identitäten ist gewährleistet.

Eine Verletzung der Authentizität wäre beispielsweise die Vortäuschung einer falschen Identität, indem eine Person die EC-Karte einer anderen Person mit dem richtigen Kennwort erfolgreich einsetzt.

Beispiel für einen Verstoß: Ein Angestellter verwendet erfolgreich die Zugangskarte seines Kollegen, um selbst in den Serverraum einzutreten.

- **Authentisierung** ist der Vorgang zum Nachweis der eigenen Identität durch eine Person oder eine Entität.
- **Authentifizierung** ist die Prüfung und der Nachweis der Identität einer Person oder einer Entität.

Die folgende Abbildung zeigt, Freddy gibt sich gegenüber Blonk mit einer gefälschten Identität aus.

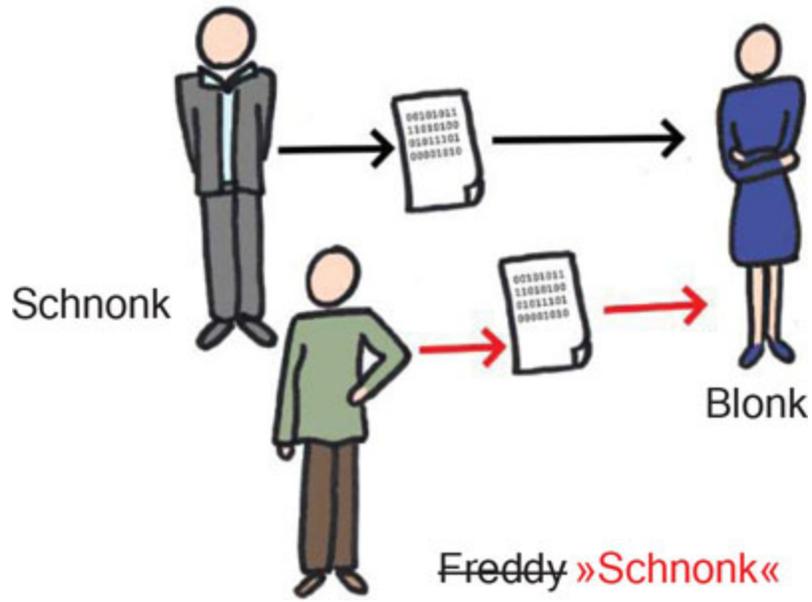


Abbildung 5: Authentizität

2.6 Verantwortlichkeit (Zurechenbarkeit)

Der Begriff ›Verantwortlichkeit‹ bedeutet, eine Person oder eine Institution hat die Verantwortung, Rechenschaft und/oder Haftung für Informationswerte (»information assets«) übernommen.

Eine Verletzung der Verantwortlichkeit wäre zum Beispiel die fehlende zugewiesene Verantwortung für Räume oder Systeme.

Beispiel für einen Verstoß: Für ein am Drucker liegen gebliebenes Dokument fühlt sich keiner verantwortlich.

Die folgende Abbildung zeigt, Schonk besitzt die Verantwortung für ein Dokument. Wenn in diesem Dokument Fehler entdeckt werden, muss dies Person sich darum kümmern.

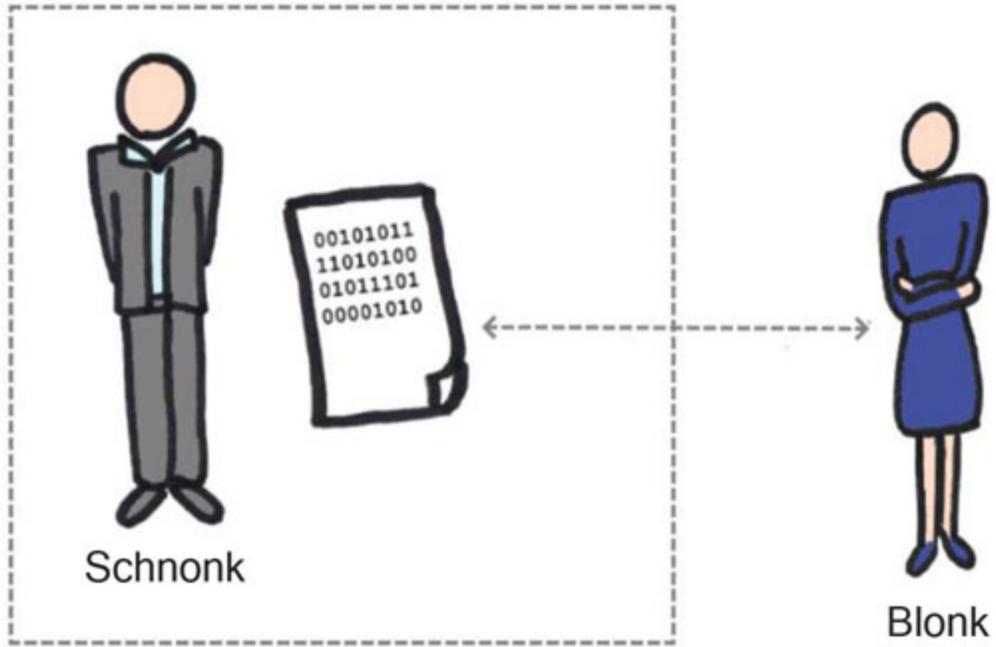


Abbildung 6: Verantwortlichkeit