# 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

## 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** vermittle 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.

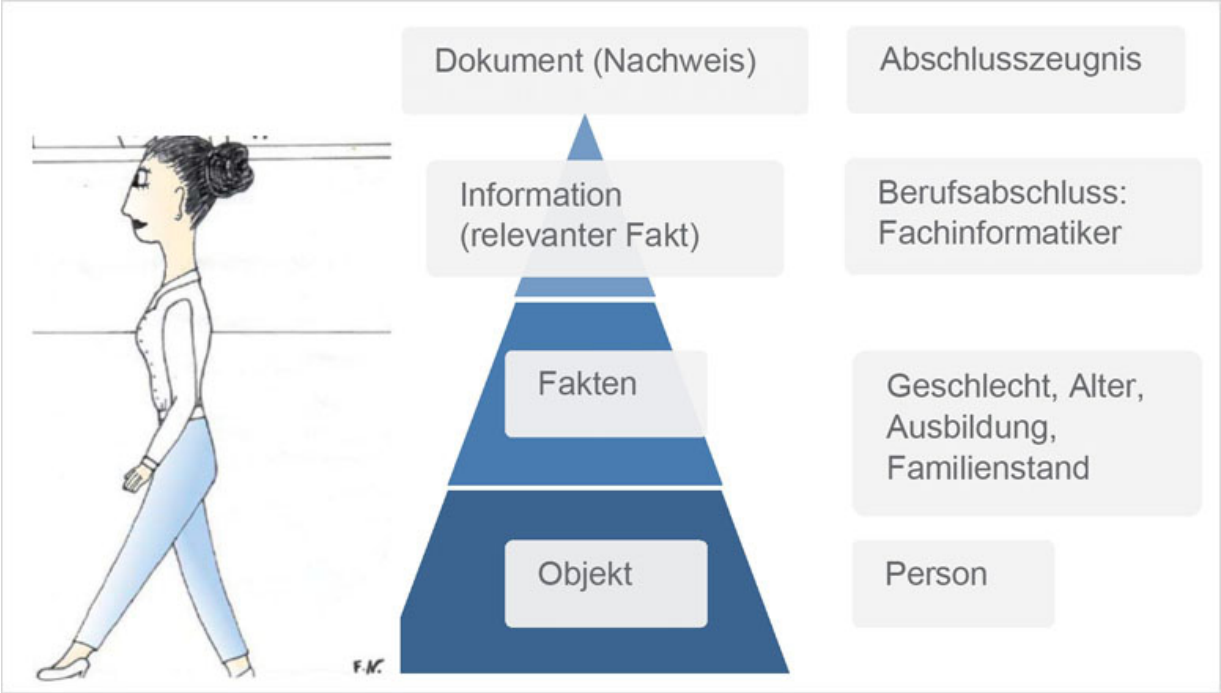


Abbildung 1: Information

## 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 Schnonk zu lesen. Könnte er die Daten dennoch einsehen oder abgreifen, wäre dies eine Verletzung der Vertraulichkeit.

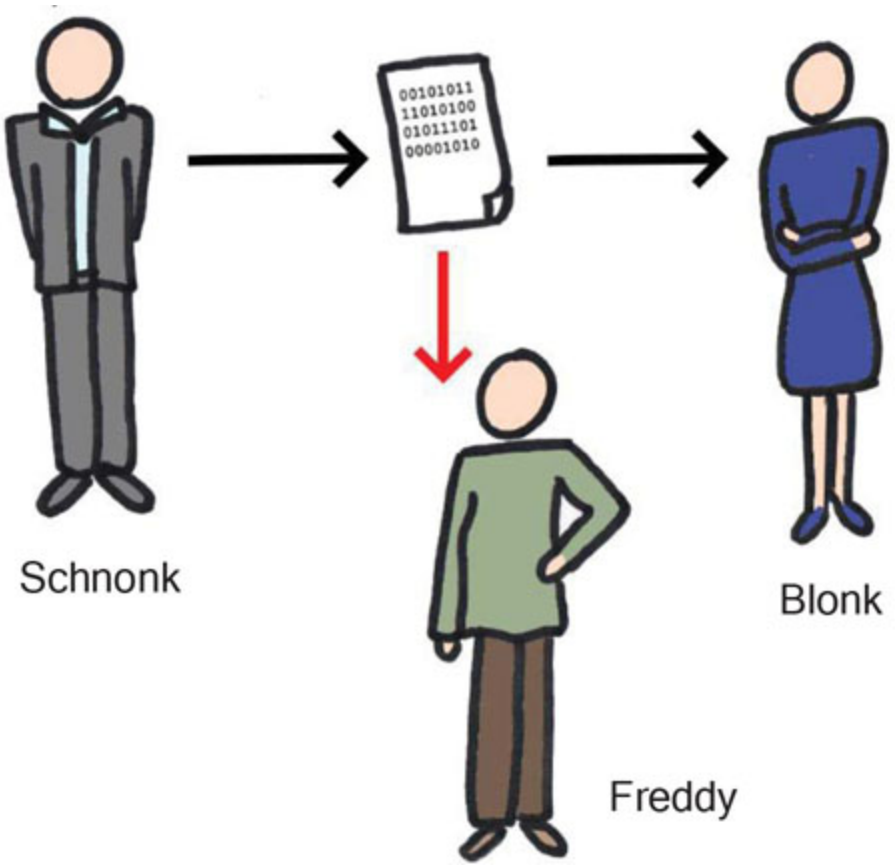


Abbildung 2: Vertraulichkeit

## 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 Schnonk abgefangen und vor der Weiterleitung manipuliert.

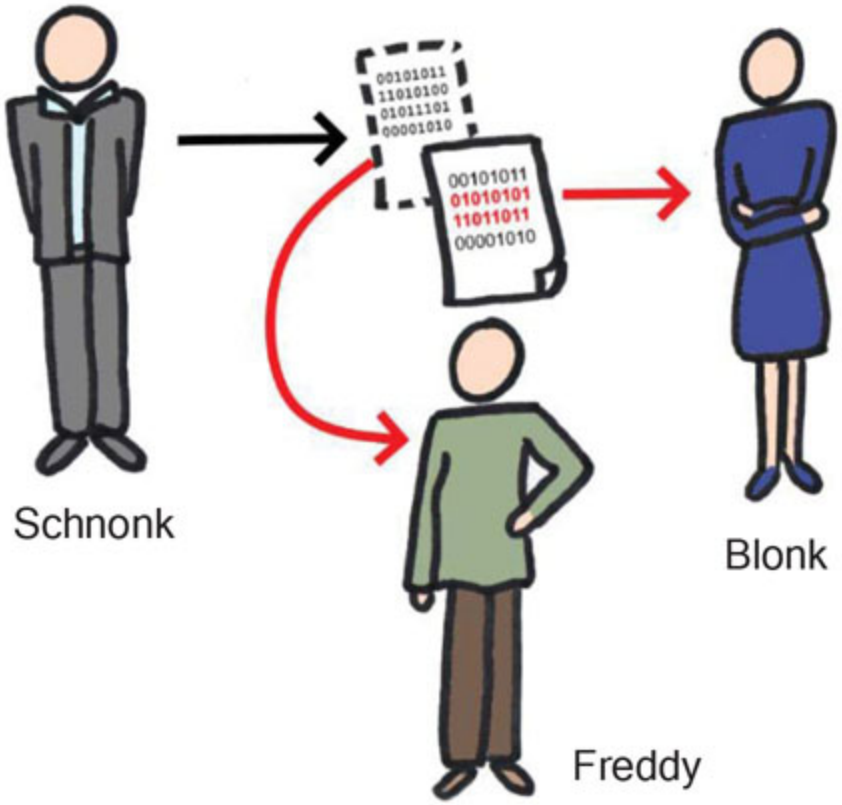


Abbildung 3: Integrität

## 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, Schnonk ist berechtigt, auf Dokumente im Tresor permanent zuzugreifen.

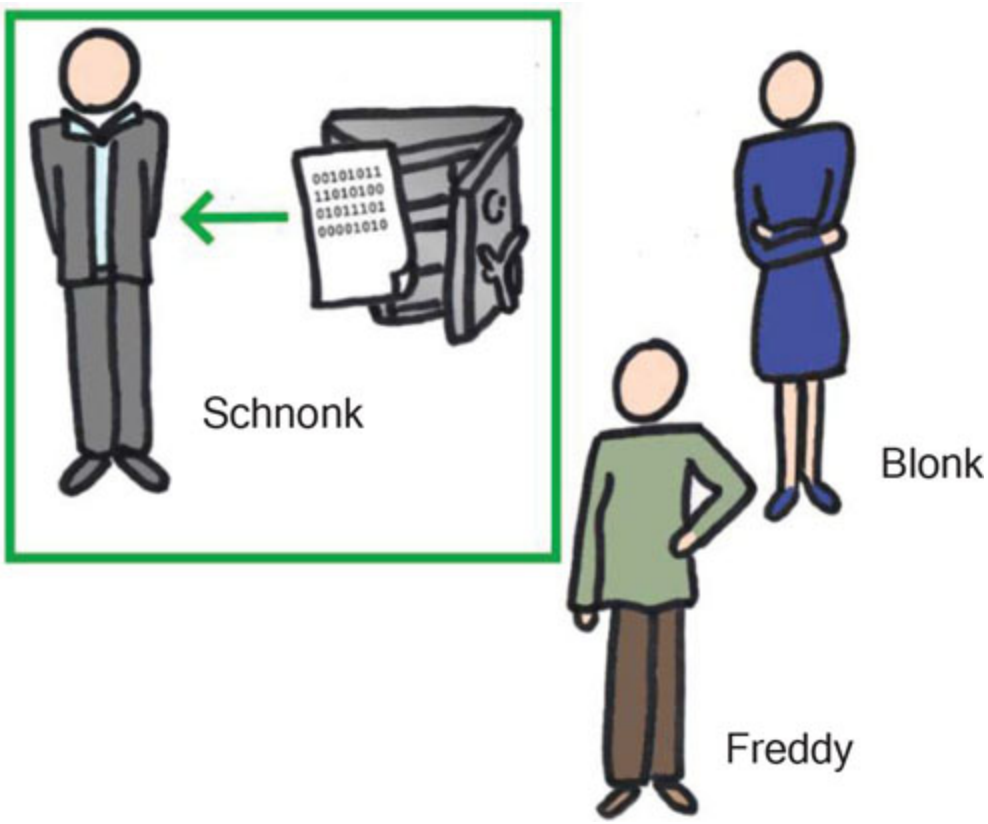


Abbildung 4: Verfügbarkeit

## 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.

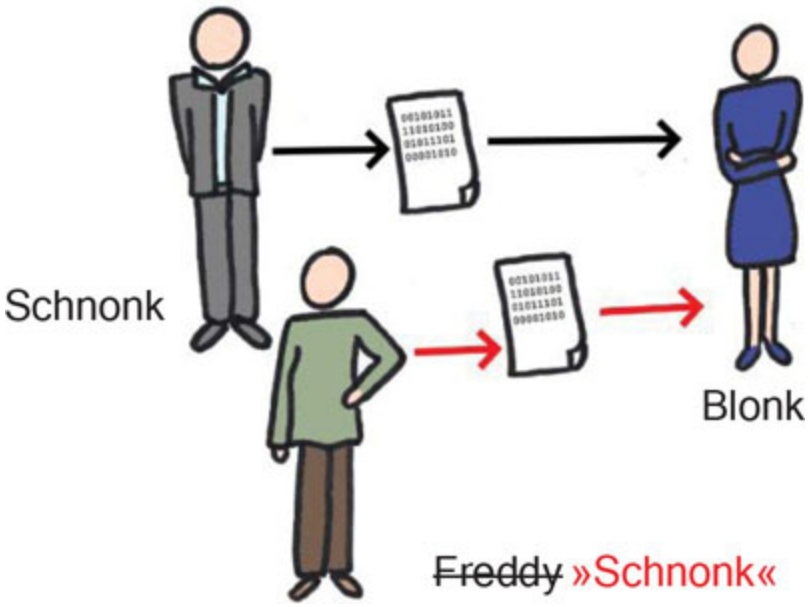


Abbildung 5: Authentizität

## 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, Schnonk besitzt die Verantwortung für ein Dokument. Wenn in diesem Dokument Fehler entdeckt werden, muss dies Person sich darum kümmern.

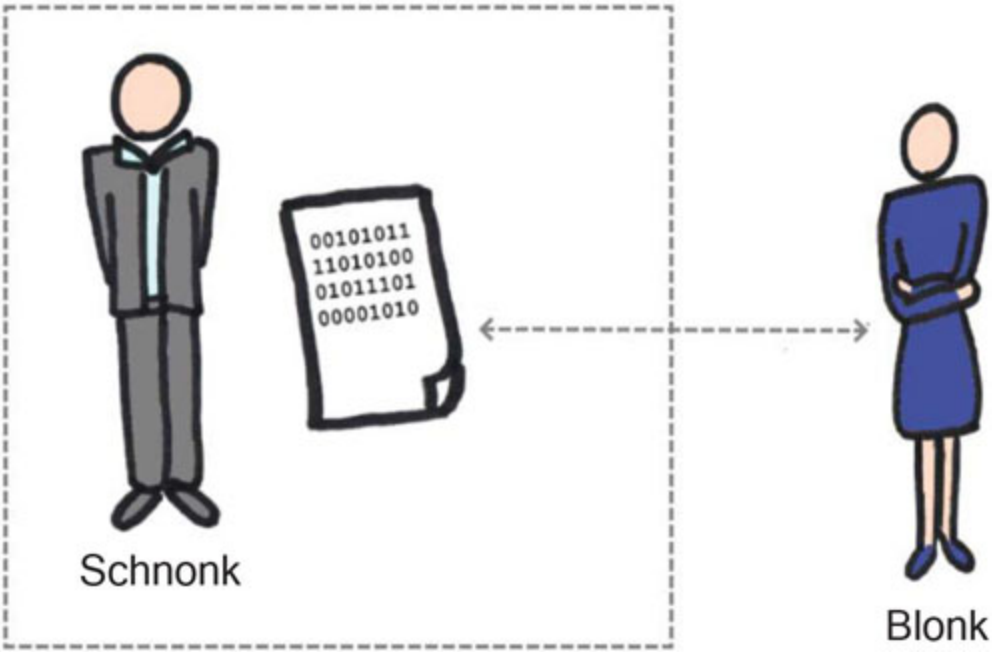


Abbildung 6: Verantwortlichkeit