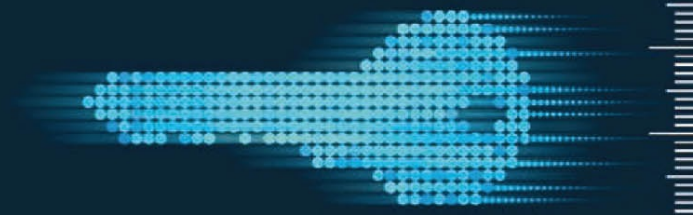
Frank Simon · Jürgen Grossmann
Christian Alexander Graf · Jürgen Mottok · Martin A. Schneider

Basiswissen Sicherheitstests

Aus- und Weiterbildung zum
ISTQB® Advanced Level Specialist
Certified Security Tester



dpunkt.verlag

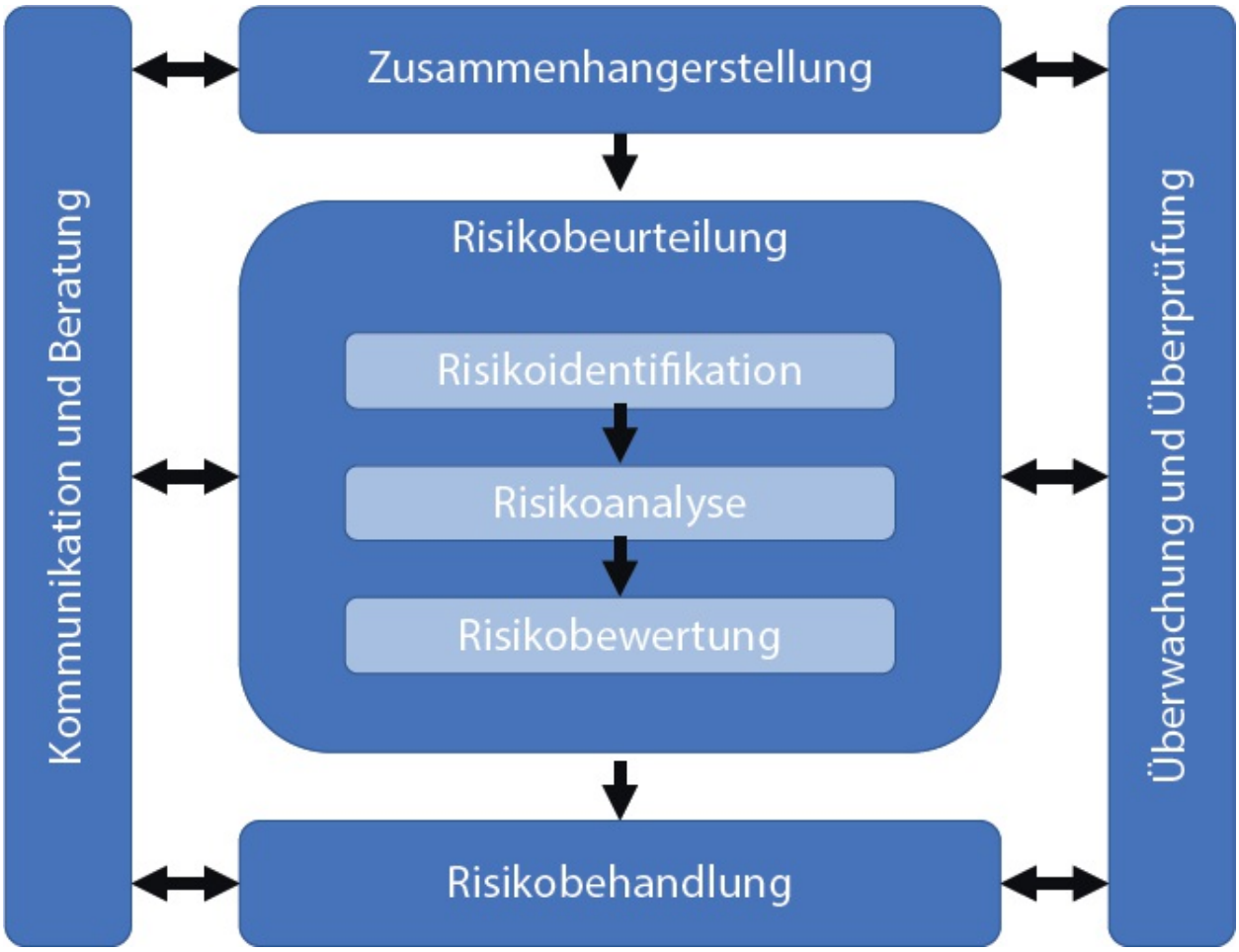


Abb. 1–1 *Schematische Darstellung der ISO 31000*

Sie ist dabei hinreichend generisch, um auch in tagtäglichen Situationen risikobasiert vorzugehen. Dies soll anhand eines Szenarios verdeutlicht werden.

Die ISO 31000 beschreibt einen eingängigen, universell einsetzbaren Risikomanagementprozess.

Beispiel: Risikomanagement

Beispiel: Risikomanagement

Das folgende Beispiel ist bewusst dem Nicht-IT-Bereich entnommen und soll den universellen Charakter des Risikomanagements aufzeigen. Im konkreten Beispiel geht es um die Abschätzung, ob man abends ein Bier trinken sollte, wenn man anschließend noch mit dem Auto selbst nach Hause fahren muss.

Eine allgemeingültige Sicht auf eine solche Risikoanalyse ist in Abschnitt 1.1.3 weiter unten beschrieben. Das konkrete Beispiel wird im Folgenden entlang des beschriebenen Risikomanagementprozesses betrachtet:

1. **Zusammenhangerstellung**
   Auch wenn die schädliche Wirkung der Zutat Bier außer Frage steht, gibt es weitere Parameter aus einem konkreten Kontext, die für die Folgeabschätzung relevant sind: Handelt es sich beim potenziellen Trinker um eine Schwangere, muss anschließend noch Auto gefahren werden, gibt es gruppendynamische Effekte und Einflüsse usw.

2. **Risikoidentifikation**
   In diesem Abschnitt werden für den konkreten Kontext (vgl. vorheriger Schritt) die einzelnen Risiken identifiziert. Die Abhängigkeit zum Kontext ist hier wichtig: Erzeugt eine Schwangere z.B. Risiken für sich und das ungeborene Kind, so gefährdet ein Mann ggf. nur sich (aber Achtung: Straßenverkehr).
3. **Risikoanalyse**
   In diesem Schritt werden die einzelnen Risiken detailliert analysiert: Wie groß ist der mögliche Schaden, welche Art ist der Schaden (monetär, gesundheitlich, reputationsbezogen usw.), wie wahrscheinlich ist er usw. Im konkreten Fall könnten medizinische Studien herangezogen werden, Verkehrsstatistiken oder auch soziologische Studien für den Fall, dass ein Nicht-Trinken zur Gruppenisolation führt.
4. **Risikobewertung**
   In diesem Schritt findet ein Abgleich der Ergebnisse der Risikoanalyse mit dem eigenen Risikoappetit statt: So können zwei Menschen in einem sehr ähnlichen Kontext trotz sehr ähnlicher Risikoanalysen immer noch völlig unterschiedliche Bewertungen erzeugen; äußern kann sich das im nächsten Schritt der Risikobehandlung als ein unbekümmertes Trinken oder ein entsetztes Ablehnen des Getränkeangebotes.
5. **Risikobehandlung**
   Dieser Schritt bedeutet die eingeleitete Aktivität auf Basis der Bewertung. Die ISO sieht hier vier verschiedene Arten vor:
   - Das Risiko akzeptieren, was in dem konkreten Beispiel zum Trinken des Bieres führen würde.
   - Das Risiko vermeiden, was zum Ablehnen des Getränkes führen würde.
   - Das Risiko vermindern, was durch eine Reduktion der Trinkmenge oder des Alkoholgehaltes (Radler) erreicht werden kann.
   - Das Risiko delegieren, was im Falle des Autofahrers bedeuten könnte, den Autoschlüssel seinem ebenfalls mittrinkenden Kollegen zu geben.

Auch wenn dieser Prozess wenig komplex ist und damit evtl. eine einfache Anwendbarkeit suggeriert, so soll bereits hier nicht unerwähnt bleiben, dass eine Risikoanalyse eine höchst anspruchsvolle Aufgabe ist. Häufig werden hier bekannte Risiken vergessen, oder es dominieren eigene Gewohnheiten (»ich trinke immer ein Bier vor dem Nach-Hause-Fahren«) und eigene Risikobereiche (»nachts fahre ich sehr ungern«), oder die Risiken basieren auf unreflektierten Expertenmeinungen. Es benötigt meist sehr viel Erfahrung, wirklich vollständige und objektive Risikoanalysen durchzuführen.

Der Sicherheitstest, bei dem geprüft wird, wie sicher ein IT-System ist, lässt sich entlang dieses Standards im Bereich der Risikoidentifikation und der Risikoanalyse verorten. Der Sicherheitstest hilft also, existierende Risiken weiter zu analysieren, und zeigt ggf. weitere auf.

Ohne Risiken bedarf es keiner Risikoanalyse.

1.1.1.2 Das Risiko im Detail

Um eine detaillierte Risikoanalyse durchführen zu können, muss der Begriff Risiko weiter präzisiert werden:

Definition: Risiko

Ein Risiko ist ein Faktor, der zu negativen Konsequenzen in der Zukunft führen könnte, gewöhnlich ausgedrückt durch das Schadensausmaß und die Eintrittswahrscheinlichkeit. [GTB Glossar 18]

Beide Faktoren werden in der Praxis häufig quantifiziert (s. hierzu u.a. weiter unten Abschnitt 1.3.2) und für die Risikokalkulation multipliziert. So kann ein Risiko, das mit einer 1 %igen Wahrscheinlichkeit einen Schaden von 1.000 Euro bedeuten kann, als identisch zu einem anderen Risiko angesehen werden, bei dem mit einer 10%igen Wahrscheinlichkeit ein Schaden von 100 Euro erzeugt werden kann. Das kalkulierte Risiko ist in beiden Fällen 10 Euro.

Beide Faktoren sind in der Praxis häufig nicht leicht und nachvollziehbar analysierbar:

- **Eintrittswahrscheinlichkeit**
  Häufig fehlen entsprechende Analysen, sie sind zueinander nicht konsistent oder lassen sich nur bedingt auf einen konkreten Kontext anwenden.
- **Schaden**
  Wie lassen sich Reputation, Marktdominanz oder auch gesundheitliche Schäden und Tod quantifizieren? Wie viel ist eine Beziehung »wert«, die z.B. aufgrund einer falsch zugestellten E-Mail zerbricht?

Um dennoch die Ermittlung von Eintrittswahrscheinlichkeit und Schaden durchführen zu können, existieren für den Bereich der IT-Sicherheit spezielle Risikomodelle (vgl. hierzu Abschnitt 1.3.2).

CIA der Security: Vertraulichkeit (Confidentiality=C), Integrität (Integrity=I) und Verfügbarkeit (Availability=A)

Informationssicherheitsrisiken sind nun solche Risiken, die die Sicherheit von Informationen eines Systems gefährden. Diese Definition ist eine Vereinfachung der Definition innerhalb der ISO 27001 [ISO 27001]:

Definition: Informationssicherheitsrisiko

»Als Informationssicherheitsrisiko wird das Potential bezeichnet, dass eine Bedrohung ausgenutzt werden kann und der Organisation so Schaden zugefügt wird.« [Klipper 15]

IT-Sicherheit ist folglich der Zustand, in dem Vertraulichkeit, Integrität und Verfügbarkeit von Informationen und Informationstechnik durch angemessene Maßnahmen geschützt sind (vgl. [BSI Glossar 13]).

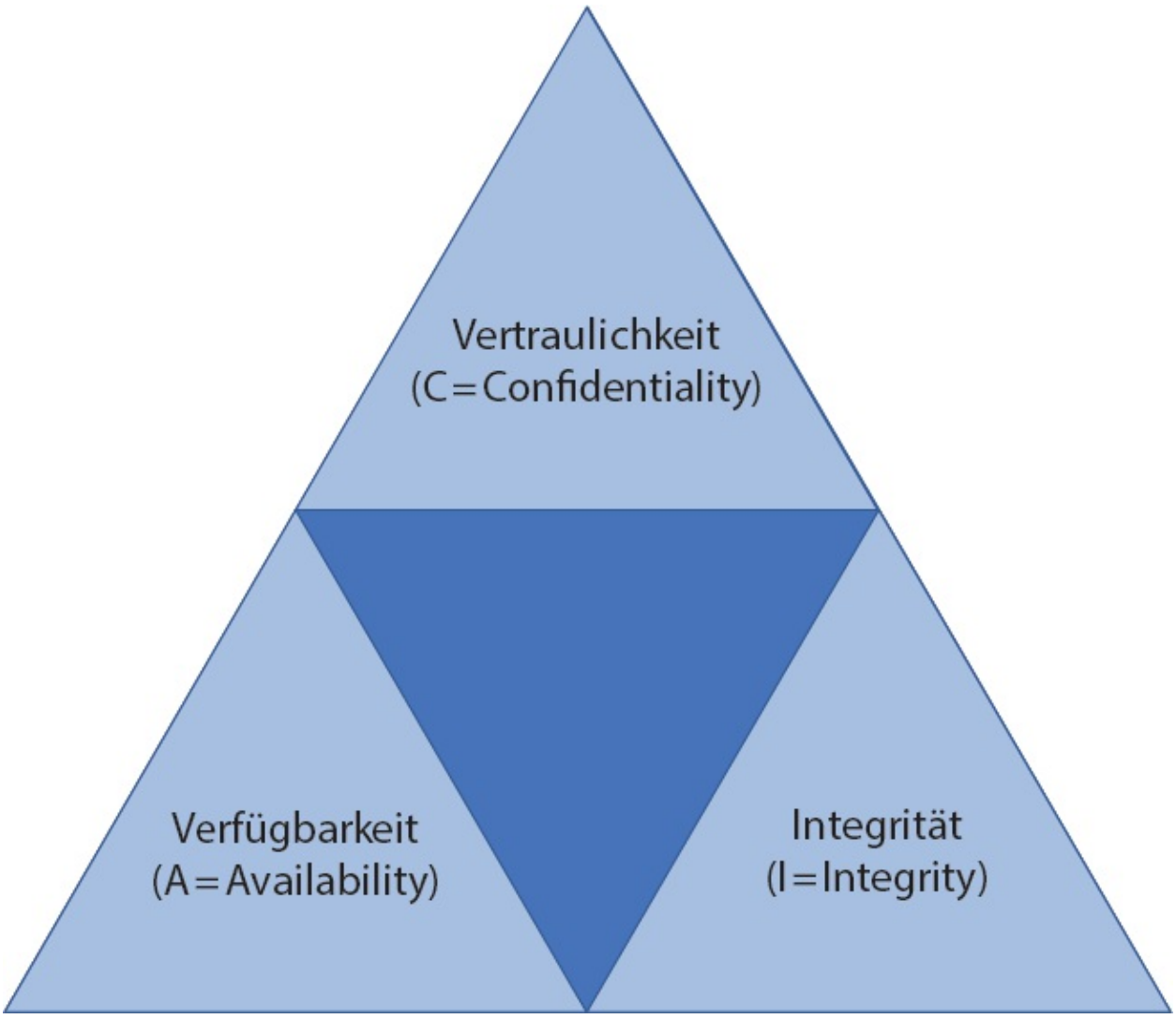


Abb. 1–2 *CIA-Dreieck der Sicherheit*

Der Verlust der IT-Sicherheit bedeutet folglich den Verlust von Vertraulichkeit, Integrität oder Verfügbarkeit von Informationen oder Informationssystemen. Die Risiken hängen ganz wesentlich von den potenziellen schädlichen Auswirkungen auf betriebliche Vorgänge (z.B. Ziele, Funktionen, Image oder Reputation), betriebliche Assets, Individuen, andere Unternehmen sowie ein gesamtes Land ab [NIST SP 800-30 02]. Der Schaden wird dabei wiederum stark vom Kontext des Systems bestimmt:

Schadenshöhen hängen vom Kontext ab.

- Ist die Vertraulichkeit eines einfachen, öffentlichen Webservers verletzt, so ist der Schaden gering, da die Informationen per se für jeden gedacht waren. Bei einem internen Schadenssystem einer Versicherung ist ein solcher Verlust dagegen verheerend.
- Ist die Verfügbarkeit eines öffentlichen Warenbestellsystems nicht mehr gewährleistet, so beginnt direkt nach der ersten Sekunde der Nichtverfügbarkeit der

Schaden durch Umsatzausfall zu wachsen. Die Nichtverfügbarkeit eines Druckers kann dabei bei Ausfällen von einigen Sekunden meist ignoriert werden.

- Ist die Integrität eines Wahrsageportals nicht gewährleistet, so kann dies – je nach Grad der Integritätsverletzung und der subjektiven Einstellung zu Wahrsagungen – durchaus vernachlässigt werden. Die Nichtintegrität von Systemen im medizinischen Bereich kann dagegen tödliche Folgen haben.

Im Rahmen einer Sicherheitsrisikobeurteilung, bestehend aus den drei Schritten der ISO 31000 – Risikoidentifikation, Risikoanalyse und Risikobewertung –, kann ein Unternehmen systematisch ermitteln, welche Bereiche und Assets einem Risiko ausgesetzt sind und welchen Schweregrad die einzelnen Risiken haben. Für Sicherheitstester kann eine Sicherheitsrisikobewertung eine ergiebige Informationsquelle sein, auf deren Grundlage sich Sicherheitstests planen und konzipieren lassen. Idealerweise fokussieren Sicherheitstests dabei die besonders großen Risiken. Je größer ein Risiko, desto tiefer die Sicherheitstesttiefe. Die Sicherheitsrisikobewertung hilft also bei der Priorisierung von Sicherheitstests.

Ergebnisse der Sicherheitstests fließen dabei in eine verbesserte Sicherheitsrisikobewertung wieder ein. Sicherheitstests liefern also weitere wichtige Informationen, die für die Bewertung relevant sind.

Einen guten Überblick über die verschiedenen Möglichkeiten, wie Sicherheitsrisikobewertung und Sicherheitstesten sich im Rahmen einer umfassenden Sicherheitsbewertung ergänzen, erlauben die Norm ETSI 203-251 [ETSI 203-251 15] sowie ein technischer Bericht der ETSI mit einigen konkreten Fallbeispielen [ETSI TR 101 582 14].

1.1.1.3 Grenzen der Risikobewertung

Risikobewertung als eine fortwährende Aufgabe

Jede Risikobewertung (ob sicherheitsbezogen oder nicht) ist nur eine Momentaufnahme der berücksichtigten Parameter und fußt auf limitierten Informationen.

Beispiel: Geänderte Parameter einer Risikobewertung

Beispiel: Geänderte Parameter einer Risikobewertung

- **Geänderte Gesetze**
  Die Neufassung der Datenschutz-Grundverordnung kann dazu führen, dass eine Vielzahl von Risikobewertungen ungültig geworden ist.
- **Neue Nutzungsszenarien**
  Der zunehmende Einzug von meist unverschlüsselten Messenger-Diensten in kommerzielle Prozesse führt zu einer Neubewertung der Risiken.
- **Neue Marktanforderungen**
  Die zunehmende Sensibilisierung der Gesellschaft für Datenmissbrauch und die mit einem Sicherheitsvorfall aktuell verbundene negative Presse kann zu neuen Risikobewertungen führen.