Informations- und IT-Sicherheit im akkreditierten Unternehmen

Grundlagen und Anforderungen

September 2024

METRAS

TENIM

TEN Information Management GmbH
Altlaufstraße 40 | D - 85635 Höhenkirchen
Tel: +49-8102-7278934-0 | info@ten-im.com

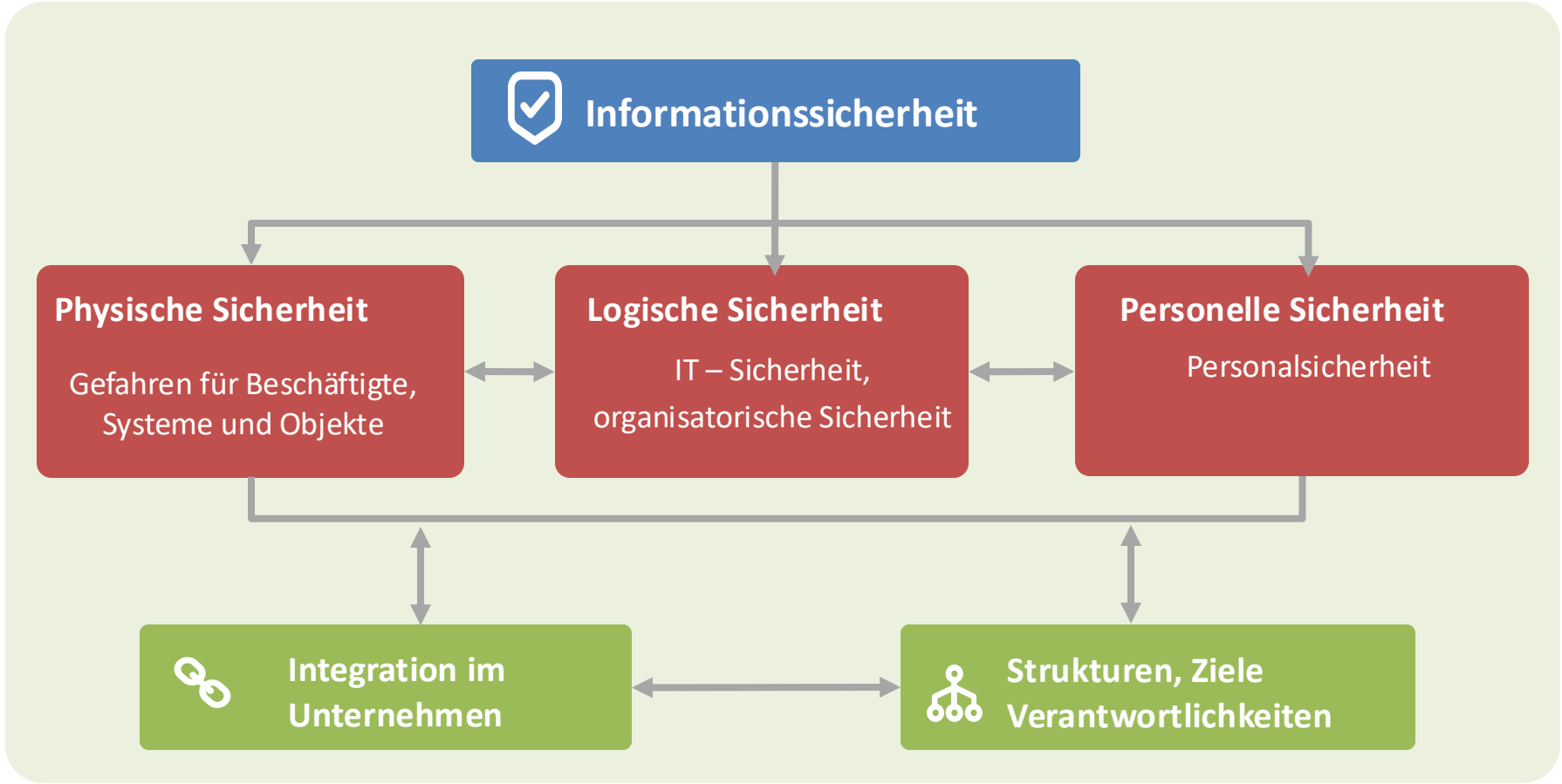
Vorstellung

- Thomas Neeff, Dipl. Wirtsch.-Inf.
  - CISA – Certified Information Systems Auditor (ISACA)
  - CISSP – Certified Information Systems Security Professional (ISC2)
  - CCSP – Certified Cloud Security Professional (ISC2)
  - ISO27000 Auditor (TÜV Süd)
  - ISO20000 Professional & Auditor (TÜV Süd)
  - ITIL 2011 Expert (EXIN)
  - ITIL 4 Managing Professional (AXELOS)
  - Trainer für Vulnerability Scanning & Penetration Testing
- Zertifizierter Datenschutzbeauftragter (GDD.Cert)

Über TEN IM: Leistungsportfolio

- Informationssicherheitsmanagement auf der Grundlage der internationalen Norm ISO27001:
  - ISMS-Einführung / Beratung / Coaching / Auditierung
  - Individuelle Projektunterstützung zu Themen der Informationssicherheit
- Schwachstellen-Scans und Penetrationstests, Phishing-Kampagnen
- Awareness Kampagnen und Mitarbeiter-Schulungen
- Watchdog by TEN IM, eine Managed SIEM Lösung für mittelständische Unternehmen

Bausteine der Informationssicherheit



Informationssicherheit

Informationssicherheit

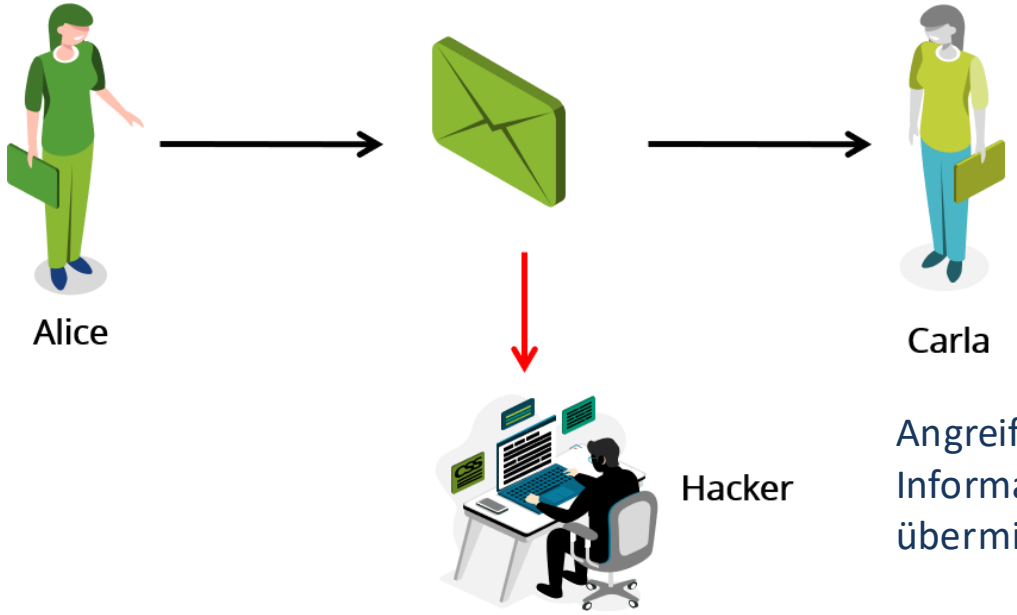
Sicherstellung der Vertraulichkeit, Integrität und Verfügbarkeit von Informationen.

Informationssicherheit ist das Ergebnis eines systematischen Ansatzes, der aus folgenden Elementen besteht

- Grundsätze
- Planungsaktivitäten
- Verantwortung / Rechenschaftspflicht
- Prozesse und Verfahren
- Ressourcen

Vertraulichkeit (Confidentiality)

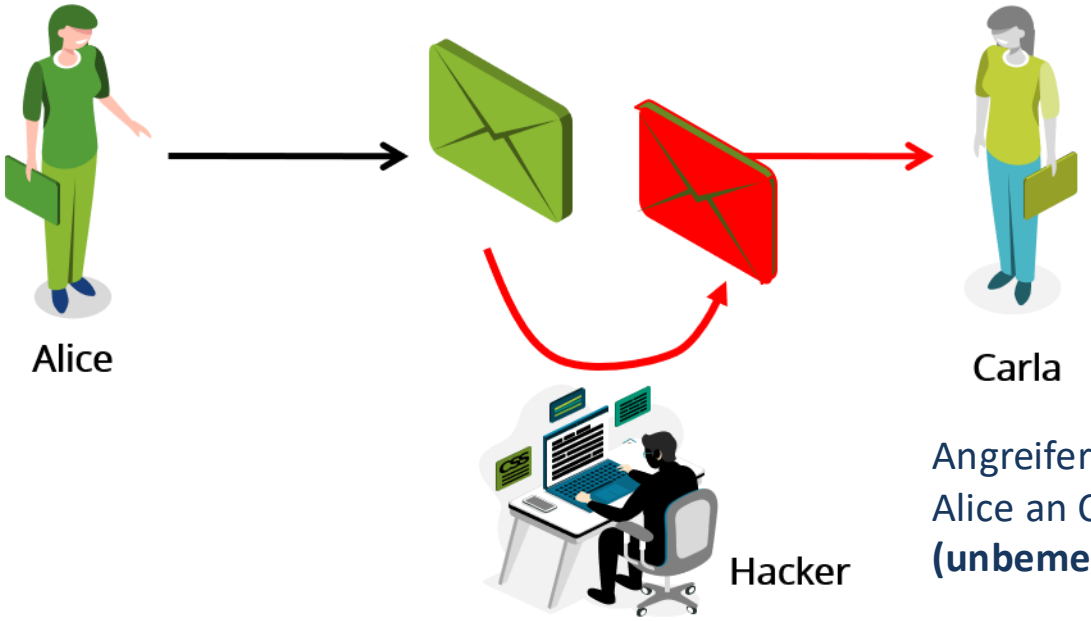
Schutz von Informationen vor unberechtigter Offenlegung. Informationen dürfen nur von zuvor autorisierten Benutzern gelesen und geändert werden.



Angreifer kann die vertraulichen Informationen, die Alice an Carla übermittelt, nicht einsehen.

Integrität (Integrity)

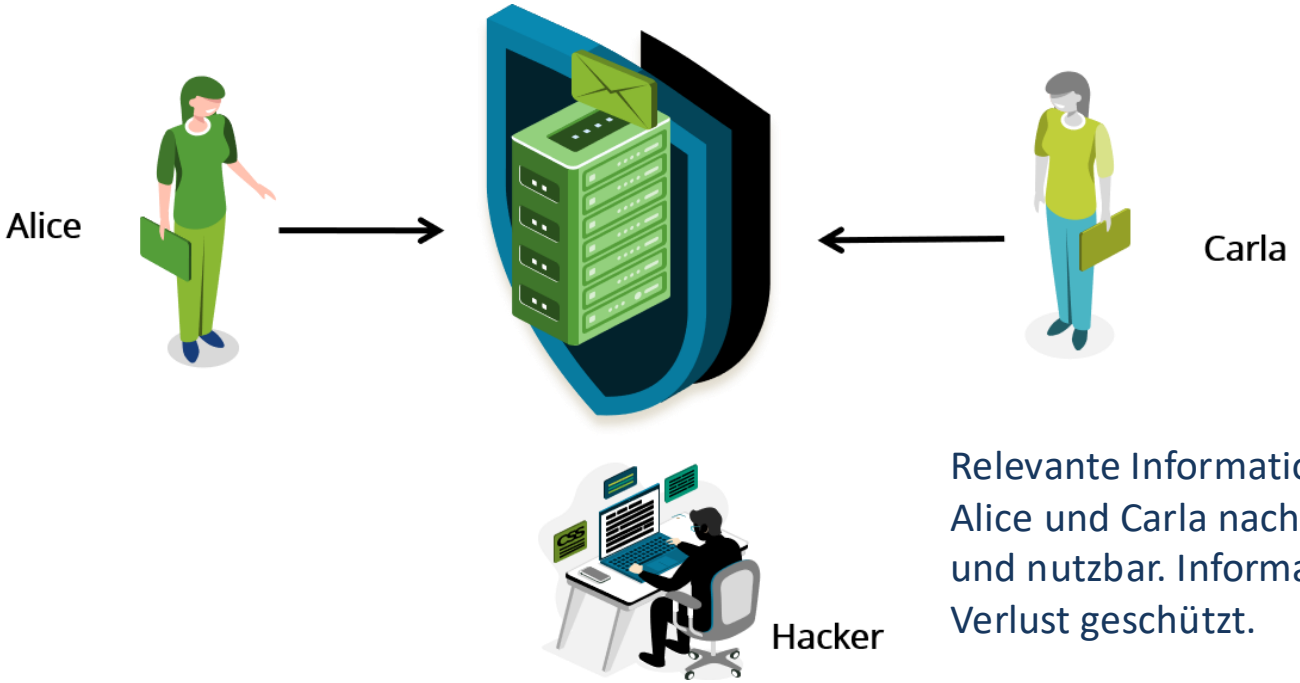
Schutz von Informationen vor nicht erlaubten und unbemerkten Modifikationen, Einfügungen, Löschungen, Umordnung, Duplikaten oder Wiedereinspielung.



Angreifer kann die Informationen, die Alice an Carla übermittelt, nicht **(unbemerkt)** manipulieren.

Verfügbarkeit (Availability)

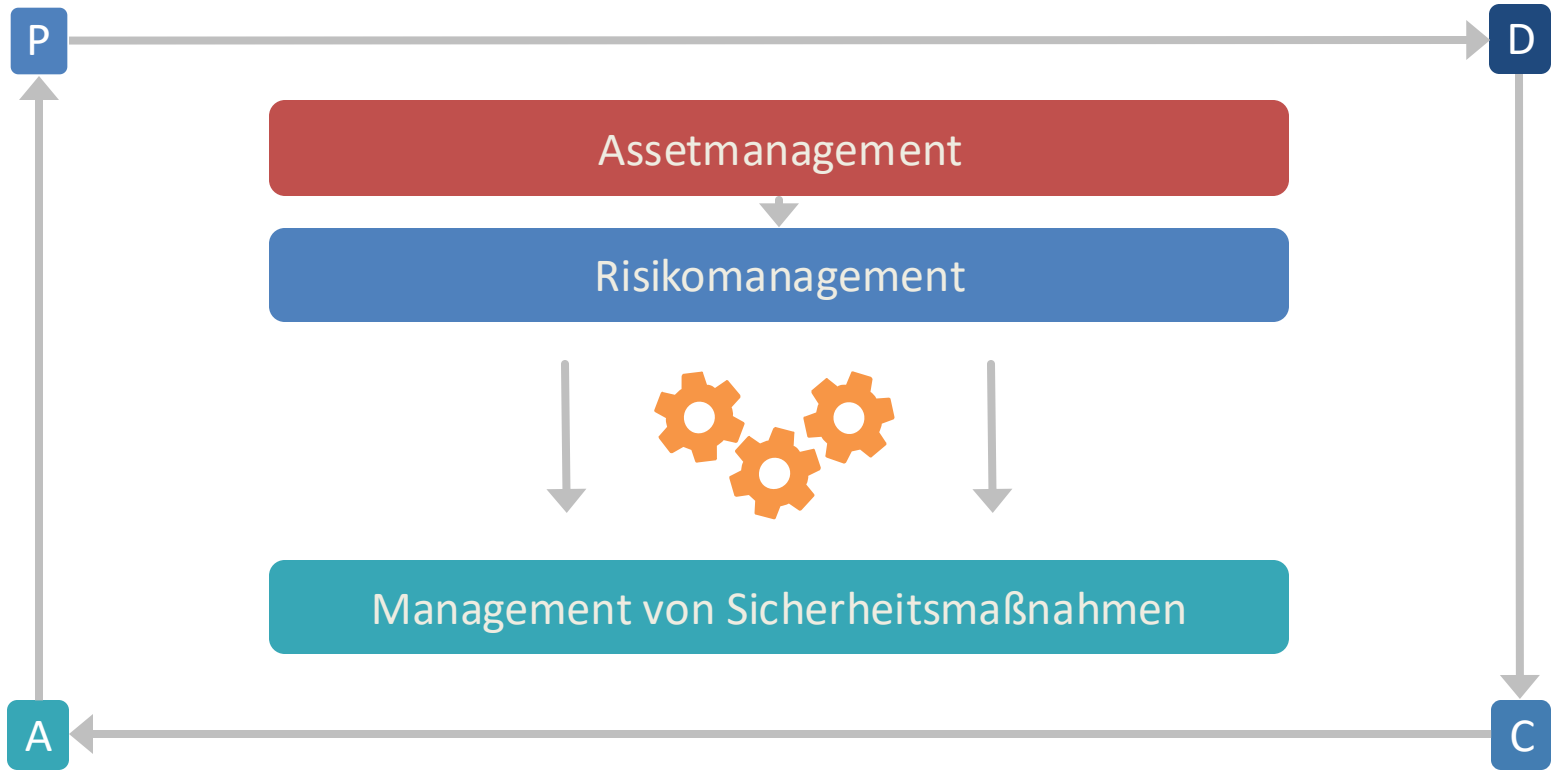
Die Verfügbarkeit von Informationen, Dienstleistungen oder IT-Systemen ist vorhanden, wenn diese wie festgelegt genutzt werden können.



Relevante Informationen sind für Alice und Carla nachhaltig zugreifbar und nutzbar. Informationen sind vor Verlust geschützt.

Managementsystem für Informationssicherheit (ISMS)

Systematischer Ansatz zur Gewährleistung und Aufrechterhaltung von Vertraulichkeit, Integrität und Verfügbarkeit mit angemessenen Ressourcen.



Identifikation schützenswerter Assets

Wert (engl. „Asset“)

Jede Art von (schützenswertem) Wert des Unternehmens / der Organisation.

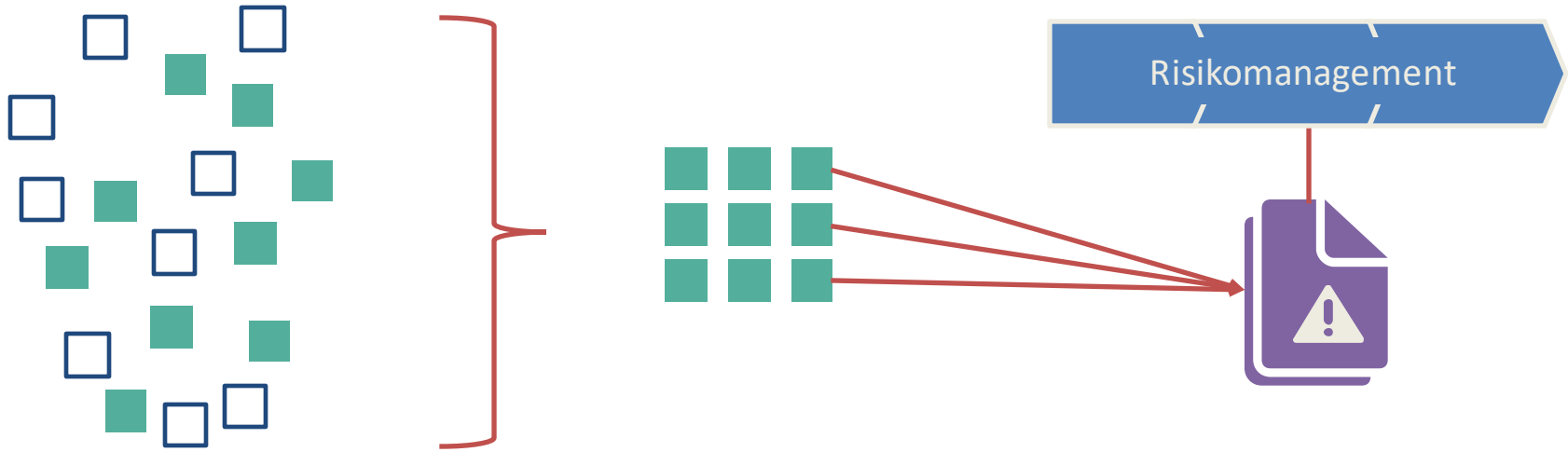
Mögliche Arten von Werten:

- Informationen
- Dokumente
- Software und Hardware (z. B. Laptops)
- Dienstleistungen
- Menschen mit ihren Qualifikationen, Fähigkeiten und Erfahrungen
- immaterielle Werte wie Ruf und Ansehen

Asset Management

Ziel

- Erfassung und Inventarisierung der Assets des akkreditierten Unternehmens
- Input für das Risikomanagement



Alle Assets
der Organisation

Schützenswerte Assets
(z.B. Asset-Datenbank)

Bezug zwischen
Risiken und Assets

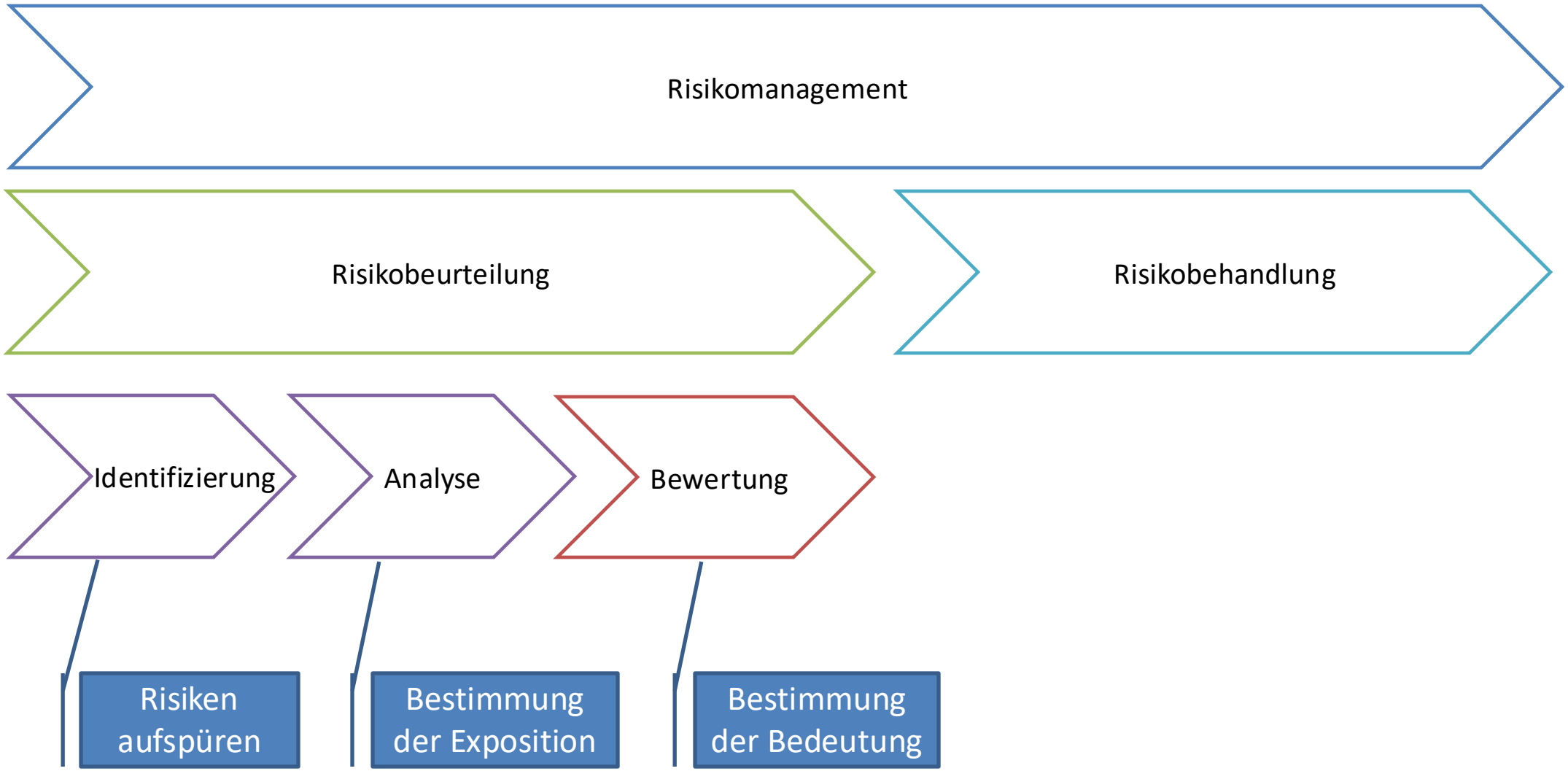
Schutzbedarfe von Assets

- Vertraulichkeit
- Integrität
- Verfügbarkeit

Der Schutzbedarf eines Assets bezüglich eines dieser Grundwerte orientiert sich an dem Ausmaß des bei Verletzungen jeweils drohenden Schadens.

- Weitere Schutzziele:
  - Authentizität
  - Zurechenbarkeit
  - Nicht-Abstreitbarkeit
  - Zuverlässigkeit

Überblick über den Risikomanagementprozess



Risikobehandlungsmöglichkeiten

- Akzeptieren: Der Risikoeigner (Management) akzeptiert das Risiko
- Verringern: Es werden Maßnahmen zur Verringerung des Risikos ergriffen (z. B. mit Hilfe der in Anhang A aufgeführten Maßnahmen).
- Vermeiden: die Aktivität, die das Risiko auslöst, wird eingestellt
- Transferieren: eine andere Partei, z. B. eine Versicherungsgesellschaft, übernimmt das Risiko

Maßnahmen zur Informationssicherheit

- Gründe für die Umsetzung von Maßnahmen:
  - Spezifische(s) Risik(o)/en besteht(en)
  - Gute/übliche Praxis ("jeder macht das")
  - Rechtliche/vertragliche Anforderungen
  - ... und andere
- Erwägen Sie die proaktive Umsetzung von Maßnahmen

Praxisbeispiel: Datensicherungskonzept umsetzen

- Asset: Labormanagementsystem und seine Daten
- Risiko: Datenverlust durch Fehlfunktion, äußere oder innere Einflüsse

- Maßnahme: Backup & Restore-Konzept einführen:
  - Festlegen von maximal tolerierbaren Datenverlusten und Wiederherstellungszeiten
  - Regelmäßige Datensicherung etablieren (Sicherungsziele nicht vergessen!)
  - Wiederherstellung regelmäßig testen und üben (!)

Praxisbeispiel: Rollen-basierter Zugang zu LMS etablieren

- Asset: Labormanagementsystem und seine Daten
- Risiko: unberechtigte Modifikation von Daten

- Maßnahme: Rollenbasiertes Zugangskonzept einführen:
  - Definition von Rollen und Berechtigungen
  - Identifikation, wer welcher Rolle zugeordnet wird
  - Zuordnung durchführen
  - Regelmäßige Überprüfung etablieren

TEN Information Management GmbH
Altlaufstraße 40 | D - 85635 Höhenkirchen
Tel: +49-8102-7278934-0 | info@ten-im.com

Vielen Dank für Ihre Aufmerksamkeit!