
# Entwicklung eines Managementsystems für Informationssicherheit in 5 Phasen

*„There are only two types of companies:*
*those, that have been hacked,*
*and those, who don’t know,*
*they have been hacked.“*

—

*John T. Chambers*

# Überblick

carmasec

- Phase 1: Begriffsklärung und Leitlinie
- Phase 2: Analyse der betroffenen Geschäftsbereiche
- Phase 3: Risikoidentifizierung und -bewertung
- Phase 4: Maßnahmendefinition und -umsetzung
- Phase 5: Steuerung und Überwachung der Maßnahmen
- Ausblick: carmasec Cyber Security Reifegradmodell

# Phase 1: Begriffsklärung

*Ein **Managementsystem für Informationssicherheit (ISMS)***

*ist die Aufstellung von Verfahren und Regeln innerhalb einer Organisation,*

*die dazu dienen, die Informationssicherheit dauerhaft zu definieren,*

*zu steuern, zu kontrollieren, aufrechtzuerhalten und fortlaufend zu verbessern.*

Für eine ausführlichere Einführung in das Thema ISMS empfehlen wir einen Video-Vortrag von Senior Trusted Advisor Carsten Marmulla.
**Zum Video:** Managementsysteme für Informationssicherheit (ISMS) für KMU.

# Phase 1: Leitlinie

carmasec

**Die Umsetzung eines ISMS ist eine strategische Entscheidung, die eine Geschäftsführung bewusst trifft.**

- Erstellen Sie daher als erstes eine Leitlinie zur systematischen Umsetzung von Cybersicherheit.
- Dokumentieren Sie diese als Selbstverpflichtung.
- Kommunizieren Sie die Leitlinie an Ihre Mitarbeiter.

# Phase 1: Begriffsklärung

carmasec

## Aufbau eines ISMS (systematisch)

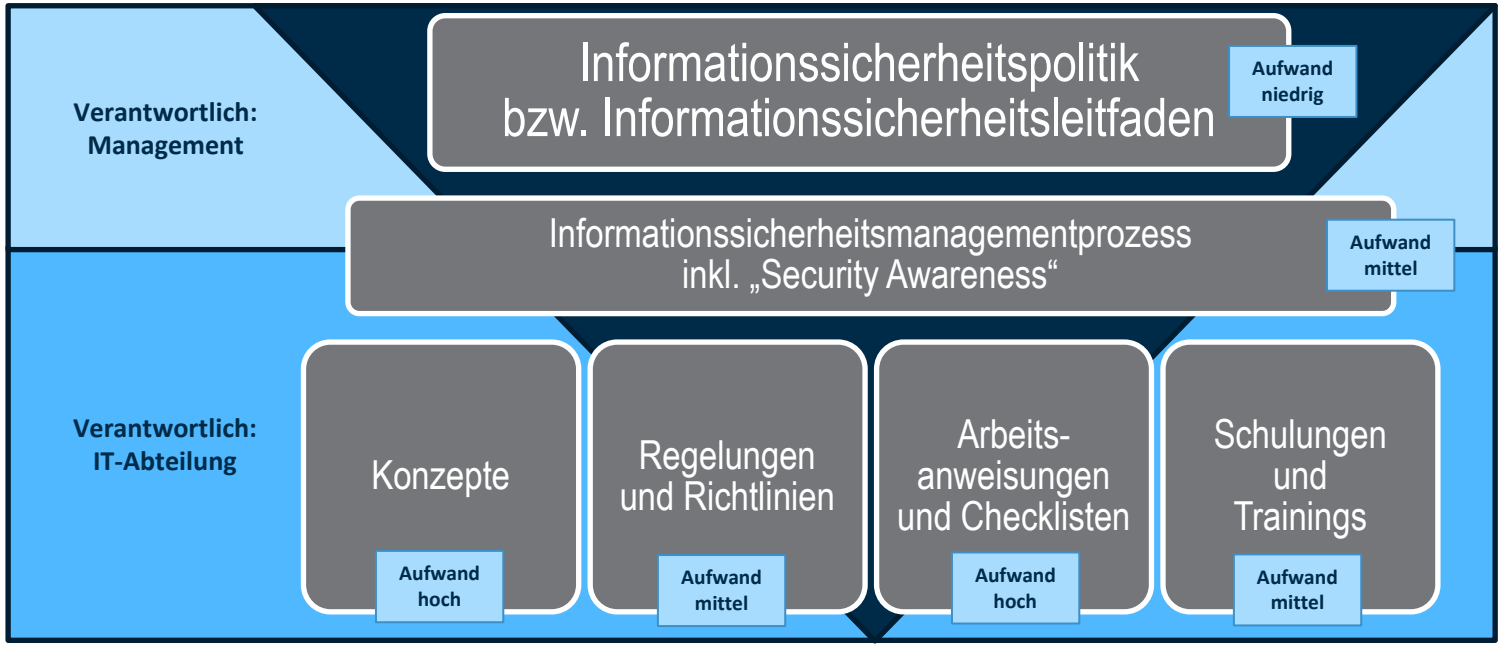
**Ebene 1 – Regulatorischer Rahmen/Informationssicherheitspolitik:**
Diese Ebene umfasst gesetzliche Vorgaben, Rahmenrichtlinien von Kunden oder Dienstleistern, branchenübliche Vorschriften etc.

**Ebene 2 – Managementprozess für Informationssicherheit:**
Welche kritischen Werte , die es zu sichern gilt, gibt es in Ihrem Unternehmen? Wie gehen Sie mit ihnen um? Dies müssen nicht zwingend IT-getriebene Werte und Prozesse sein. Eine handschriftliche Auftragsliste gilt es ebenso zu erfassen und zu sichern.

**Ebene 3 – operative Ebene:**
Die erfassten Werte und Prozesse werden in operativen Modulen konkretisiert, erforderliche Maßnahmen zur Sicherung werden abgeleitet.

# Phase 1: Begriffsklärung

## Aufbau eines ISMS (Schema)



# Phase 2: Analyse der betroffenen Geschäftsbereiche

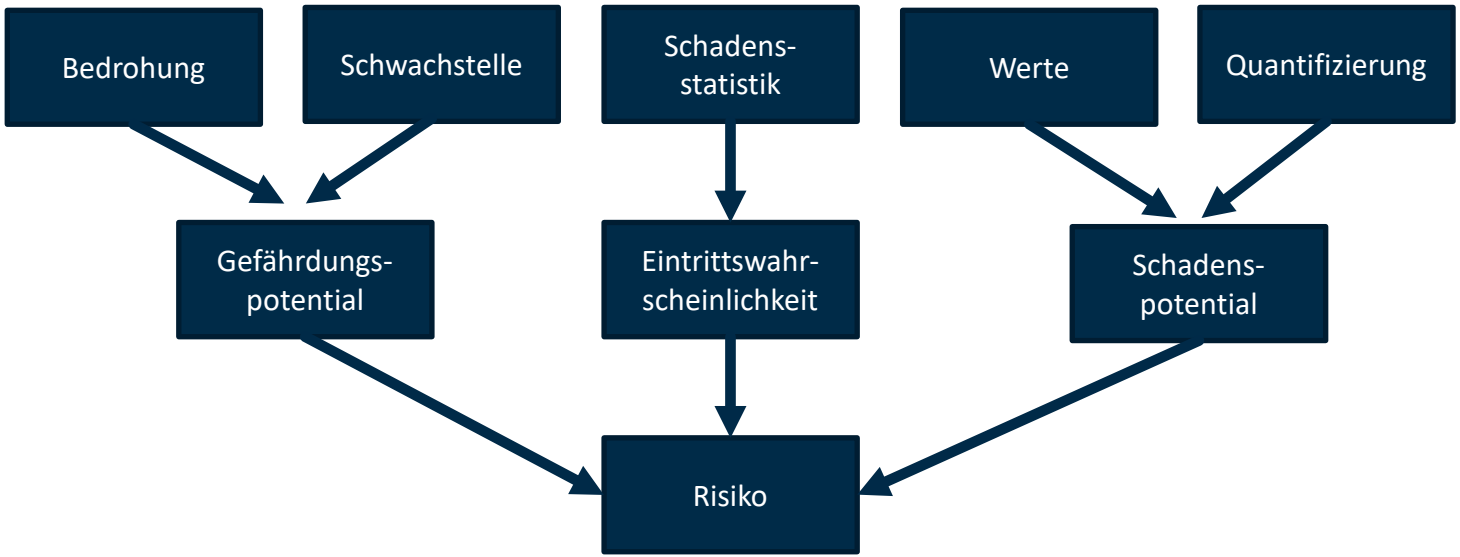
carmasec

**Sichten Sie Ihre Geschäftsbereiche und Prozesse und bewerten Sie: An welchen Stellen ist die systematische Organisation von Maßnahmen der IT-Sicherheit relevant?**

- Sicherheitsstrategie, Sicherheitsrichtlinien
- Sicherheitsorganisation
- Personalmanagement
- Management von Informationswerten
- Zugriffskontrollen
- Kryptographie
- Physische Sicherheit
- Sicherer IT-Betrieb
- Kommunikationssicherheit
- Beschaffung / Entwicklung / Wartung von IT-Systemen
- Vertrags- / Dienstleistermanagement
- Management von Informationssicherheitsvorfällen (Incident Management)
- Management der Geschäftskontinuität

# Phase 3: Risikobewertung

**Unterziehen Sie die vorab identifizierten Geschäftsbereiche einer Risikobewertung anhand der unten stehenden Grafik. Unterscheiden Sie hohes/mittleres/geringes Risiko.**



# Phase 4: Maßnahmendefinition und -umsetzung

carmasec

## Definieren Sie anhand der in Phase 3 entwickelten Risikomatrix eine geeignete Maßnahmenstrategie für Ihre Geschäftsbereiche. (1/2)

- **Risikovermeidung:**
  Ein identifiziertes Risiko wird durch eine technische und/oder organisatorische Maßnahme vollständig vermieden, so dass kein Restrisiko nach Durchführung der Maßnahme verbleibt.
  (Beispiele: Abschaltung einer Applikation, Datenlöschung)

- **Risikominderung:**
  Ein identifiziertes Risiko wird beispielsweise durch eine technische und/oder organisatorische Maßnahme gemindert und auf ein definiertes akzeptables Niveau reduziert. Es verbleibt ein Restrisiko unterhalb der zuvor definierten Risikotoleranzgrenze.
  (Beispiele: Einsatz von Firewalls, Implementierung von Verschlüsselungslösungen, Verschärfung von Zugriffskontrollen)

# Phase 4: Maßnahmendefinition und -umsetzung

carmasec

## Definieren Sie anhand der in Phase 3 entwickelten Risikomatrix eine geeignete Maßnahmenstrategie für Ihre Geschäftsbereiche. (2/2)

- **Risikoverlagerung:**
  Das identifizierte Risiko wird an einen Dritten übergeben.
  (Beispiele: Abschluss einer Risikoversicherung, Übergabe der Applikationsverantwortung im Rahmen von „Managed Services“ oder Gewerken)

- **Risikoakzeptanz:**
  Das identifizierte Risiko liegt unterhalb der zuvor definierten Risikotoleranzgrenze.
  (Beispiele: Ausnahmegenehmigung, dokumentierte Risikoübernahme durch die Fachseite)

# Phase 4: Maßnahmendefinition und -umsetzung

carmasec

## Nutzen Sie für die Definition die Maßnahmenkataloge zertifizierter Frameworks.

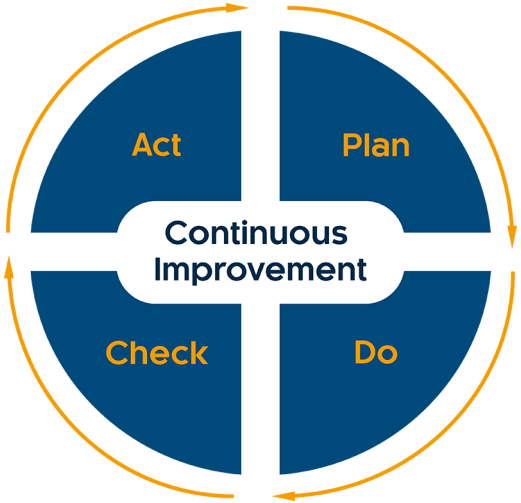
| | ISO/IEC 27001 | BSI IT-Grundschutz | VdS 10000 (ehem. 3473) | ISIS12 |
|---|---|---|---|---|
| Primäre Zielgruppe | Mittelgroße bis große Organisationen | Öffentliche Einrichtungen, Behörden | Mittelgroße Organisationen | Kleine bis mittelgroße Organisationen |
| Umsetzungsaufwand | Hoch | Sehr hoch | Mittel bis niedrig | Mittel bis niedrig |
| Renommée | International anerkannt | National anerkannt | National anerkannt | Regional anerkannt |
| Risikobasierter Ansatz | Ja (ISO 27005) | Teilweise | Teilweise | Teilweise (ab Version 2.x) |

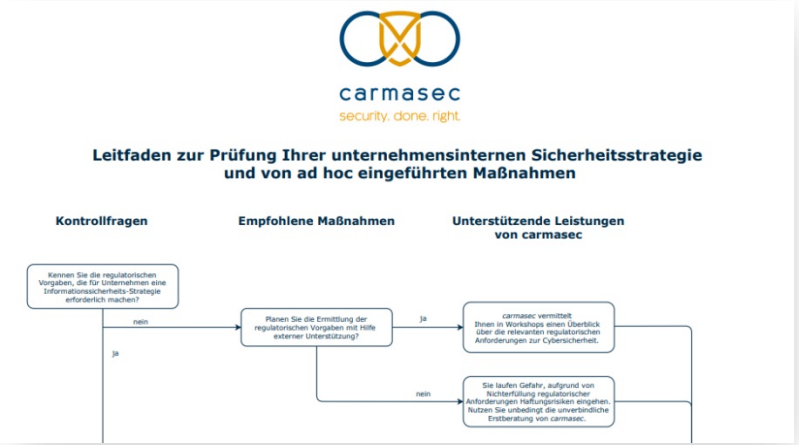
**Weiterführende Quellen:**

Bundesamt für Sicherheit in der Informationstechnik: ISO/IEC 27001-Zertifizierung
Bundesamt für Sicherheit in der Informationstechnik: BSI IT-Grundschutz
VdS Verband der Sachversicherer: VdS 10000 – Informationsverarbeitung für den Mittelstand
IT-Sicherheitscluster e.V.: ISIS12 – Informationssicherheit für KMO

# Phase 5: Steuerung und Überwachung der Maßnahmen

**Evaluieren und optimieren Sie Ihre Maßnahmen regelmäßig (einmal jährlich). Nutzen Sie dafür beispielsweise das Modell des PDCA-Zyklus oder unseren Leitfaden zur Integration für Maßnahmen in Ihr ISMS für einen kontinuierlichen Verbesserungsprozess.**





carmasec
security. done. right.

**Leitfaden zur Prüfung Ihrer unternehmensinternen Sicherheitsstrategie und von ad hoc eingeführten Maßnahmen**

| Kontrollfragen | Empfohlene Maßnahmen | Unterstützende Leistungen von carmasec |
|---|---|---|
| Kennen Sie die regulatorischen Vorgaben, die für Unternehmen eine Informationssicherheits-Strategie erforderlich machen? | | |
| nein | Planen Sie die Ermittlung der regulatorischen Vorgaben mit Hilfe externer Unterstützung? | ja |
| | | carmasec vermittelt Ihnen in Workshops einen Überblick über die relevanten regulatorischen Anforderungen zur Cybersicherheit. |
| ja | | |
| | nein | Sie laufen Gefahr, aufgrund von Nichterfüllung regulatorischer Anforderungen Haftungsrisiken einzugehen. Nutzen Sie unbedingt die unverbindliche Erstberatung von carmasec. |

Den vollständigen Leitfaden können Sie auf der Website von carmasec herunterladen.

# Ausblick: carmasec Cyber Security Reifegradmodell

**Erhöhen Sie die Wirksamkeit Ihrer Cybersicherheits-Maßnahmen mit Hilfe des carmasec Cyber Security Reifegradmodells (CS2RM), das für die Anforderungen deutscher Unternehmen entwickelt wurde.**


Unsere Leseempfehlung: Whitepaper **Reifegradmodelle für die Cybersicherheit Ihres Unternehmens**


Melden Sie sich für unseren Newsletter an: www.carmasec.com/newsletter

Hauptsitz:
**carmasec GmbH & Co. KG**
Ruhrallee 185
45136 Essen
Germany

Niederlassung:
**carmasec GmbH & Co. KG**
Im Mediapark 5
50670 Köln
Germany

Telefon: +49 (0) 201 426 385 900
Fax: +49 (0) 201 426 385 909
Web: www.carmasec.com
Email: contact@carmasec.com