carmasec

security. done. right.

#suw2019


# Cloud-Security, Risikomanagement und Maßnahmen zum Schutz von Daten

Carsten Marmulla

startupweek:ruhr, Camp Essen, 25.09.2019

carmasec

*„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*

# Einführung

carmasec

Über welche Sicherheit reden wir eigentlich?

- Funktionale vs. nicht-funktionale Sicherheit

  (Safety vs. Security)

- Datenschutz vs. Datensicherheit

# Terminologie

carmasec

Governance
Risk Management
Compliance

| | | |
|---|---|---|
| Informations-Sicherheit | Datenschutz | IT-Security |
| Schutz von geschäftskritischen Daten | Schutz von personenbezogenen Daten | Schutz von Applikationen, Systemen und Netzen |

# Status Quo

carmasec

| | Typ 1: „Skript-Kid“ | Typ 2: „Hacktivist“ | Typ 3: „Cybercrime“ | Typ 4: „Nachrichtendienste“ |
|---|---|---|---|---|
| **Beispiele** | • Verunstalten von Internetseiten<br>• Meldungen von Schwachstellen in Webseiten an die Presse<br>• ... | • DDoS gegen Banken, die Wikileaks Konten gesperrt hatten<br>• Anonymous-Angriffe gegen Unternehmen<br>• ... | • APTs<br>• Phishing-E-Mails<br>• DDoS auf Online-shops/Onlinewetten<br>• SPAM<br>• ... | • Stuxnet (Iranisches Atomprogramm)<br>• Red October (Regierungen im Ostblock)<br>• ... |
| **Aufwand Prävention/ Abwehr** | Niedrig bis mittel | Mittel | Hoch | Sehr Hoch |
| **Wirksamkeit** | Hoch | Hoch bis mittel | Hoch bis mittel | Mittel bis niedrig |

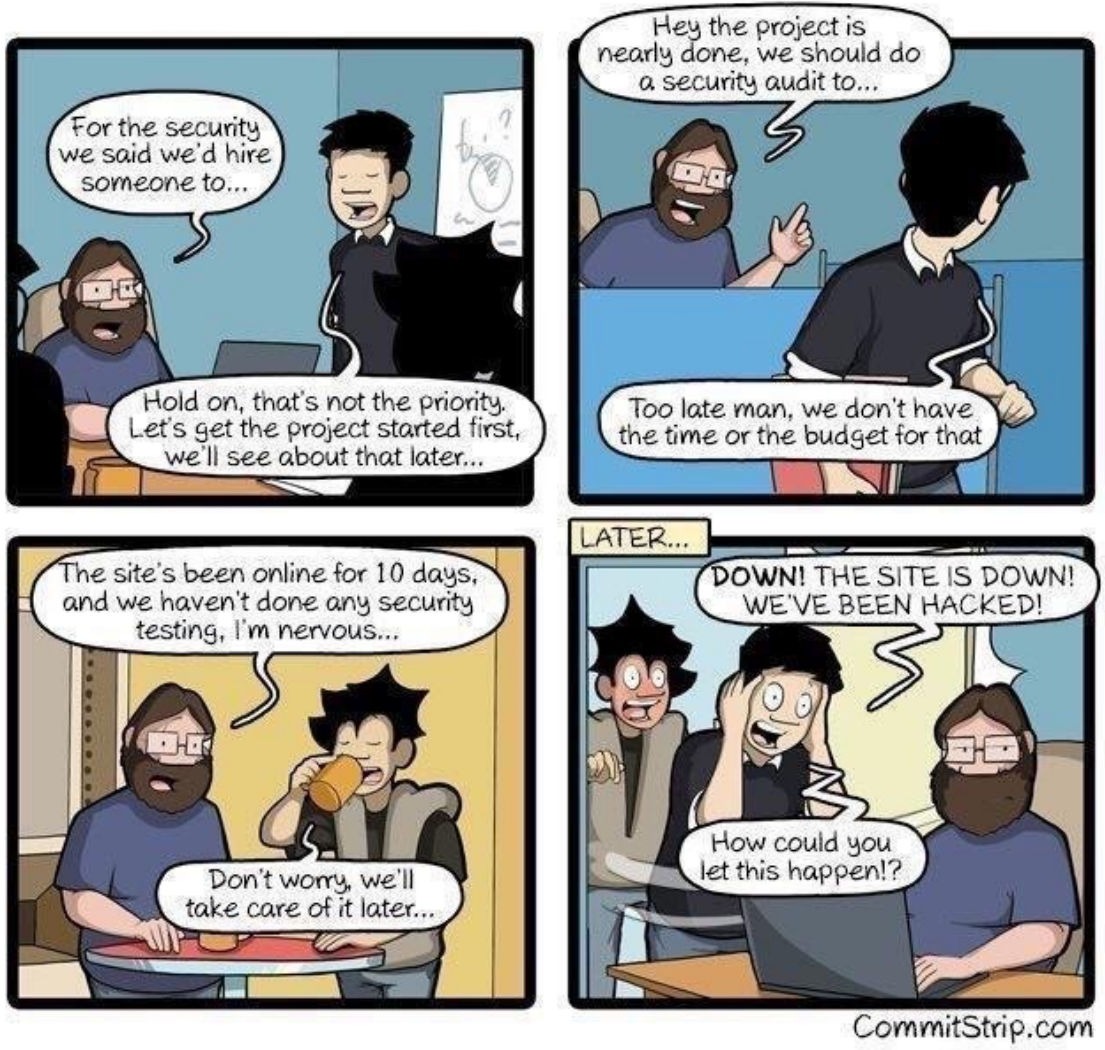
**Primärer Fokus**

**Sekundärer Fokus**

# Status Quo

carmasec

# INNOVATION


For the security we said we'd hire someone to...
Hold on, that's not the priority. Let's get the project started first, we'll see about that later...
Hey the project is nearly done, we should do a security audit to...
Too late man, we don't have the time or the budget for that
The site's been online for 10 days, and we haven't done any security testing, I'm nervous...
Don't worry, we'll take care of it later...
LATER...
DOWN! THE SITE IS DOWN! WE'VE BEEN HACKED!
How could you let this happen!?
CommitStrip.com

carmasec

# Cloud-Security

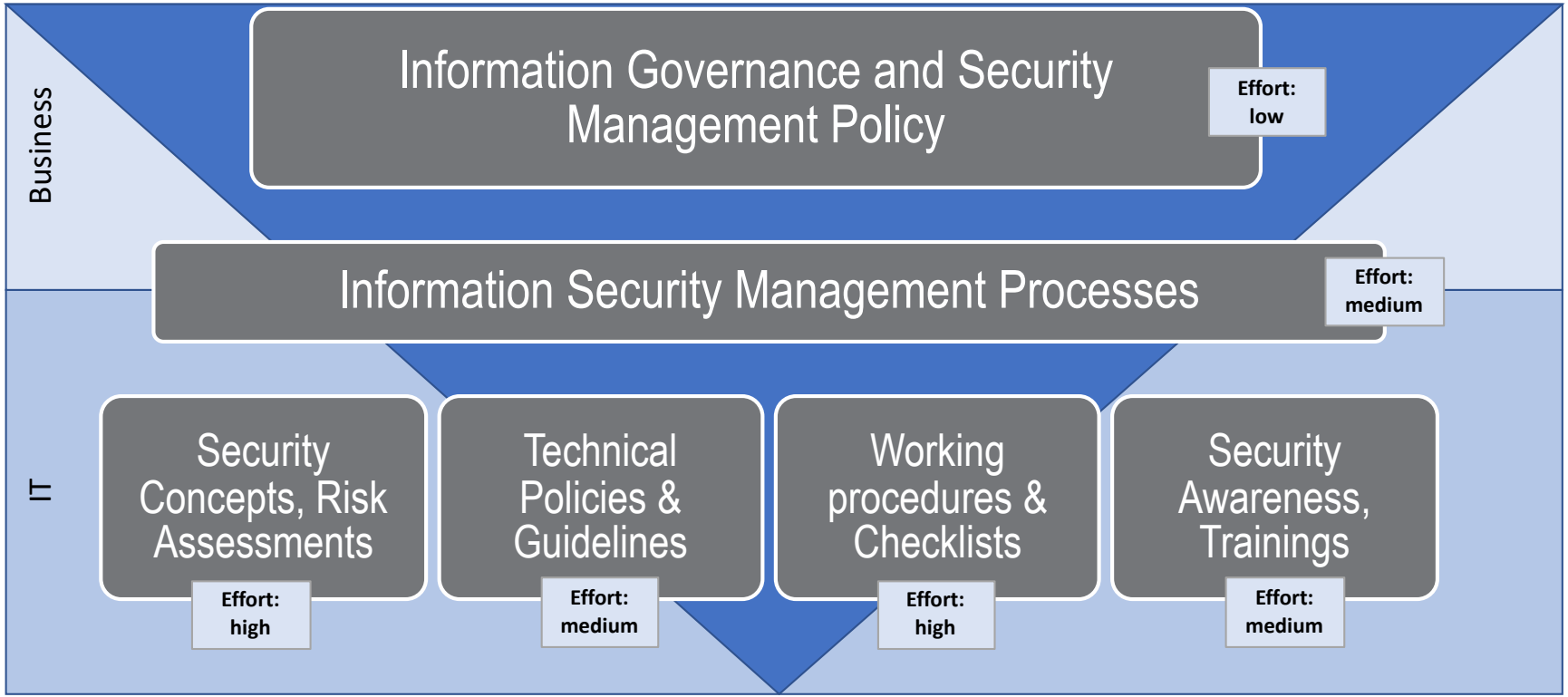
carmasec


# Cloud-Security

carmasec

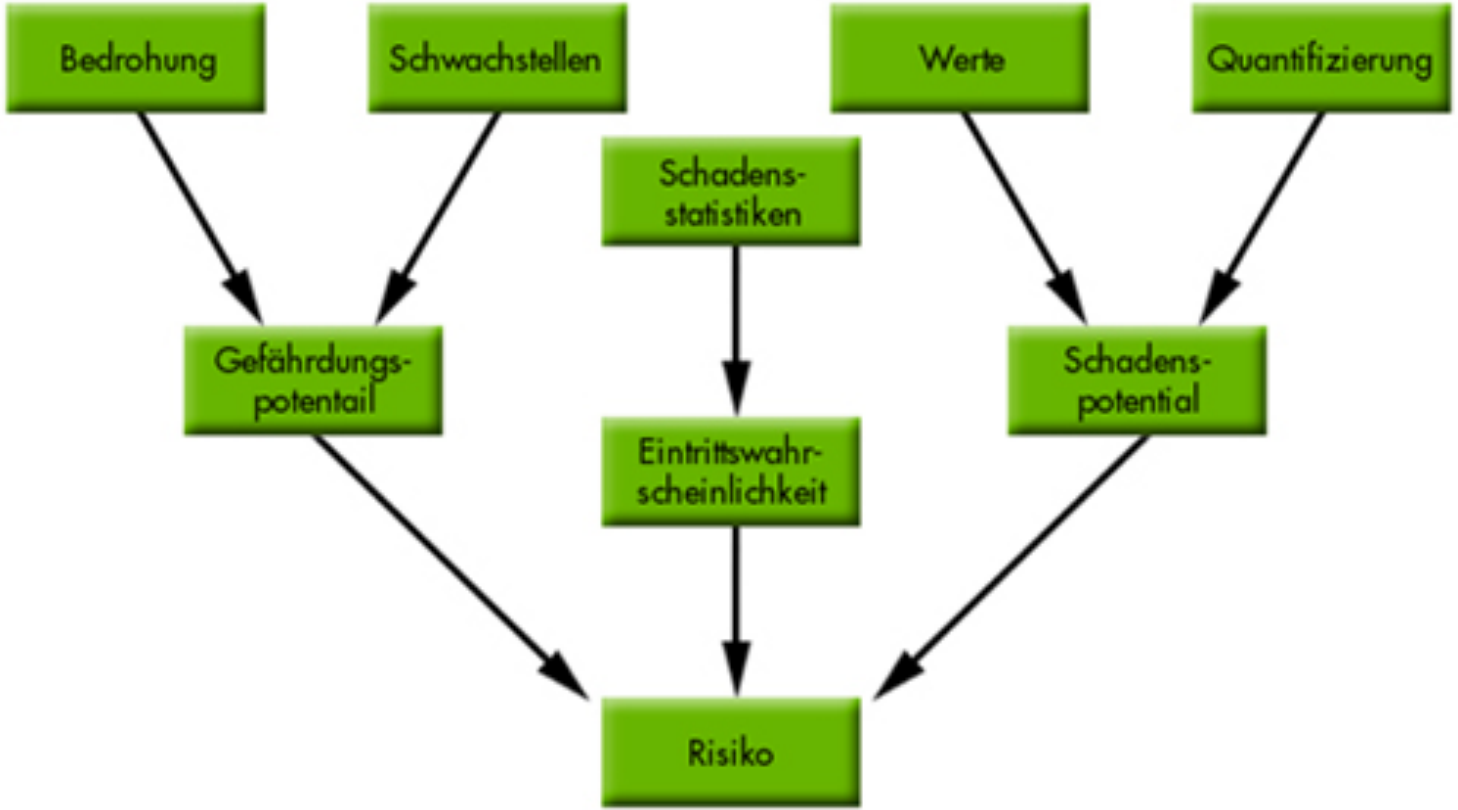
# Informationssicherheitsmanagement

carmasec



# Was ist ein Risiko?

carmasec



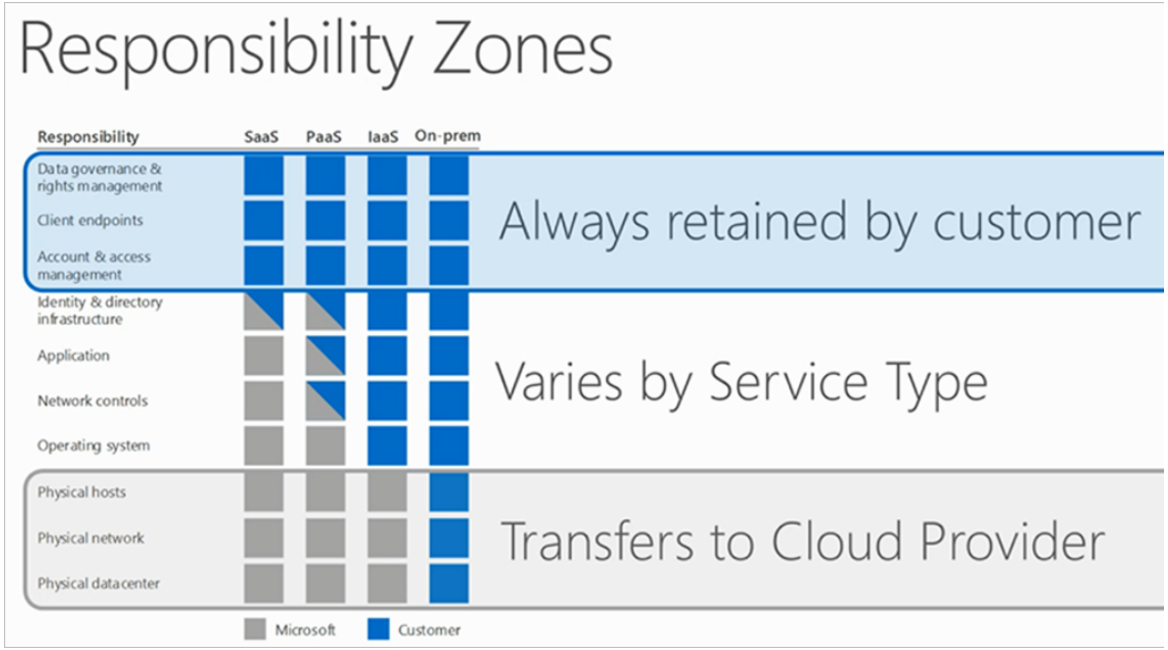
# Risikomanagement (gemäß ISO 27005)

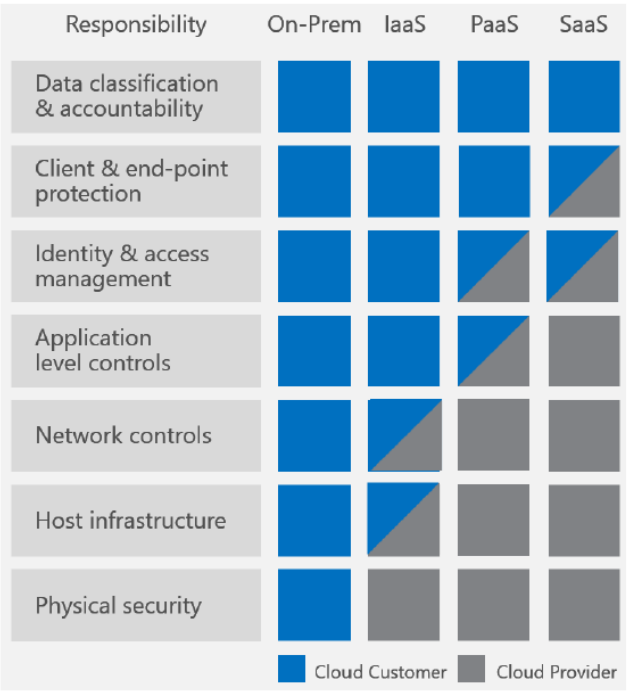
- **Risikovermeidung:**
  Ein identifiziertes Risiko wird durch eine technische und/oder organisatorische Maßnahme vollständig vermieden, so dass kein Restrisiko nach Durchführung der Maßnahme verbleibt.
  (Beispiele: Abschaltung einer Applikation, Datenlöschung)
- **Risikominderung:**
  Ein identifiziertes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

# Shared Responsibility Model

carmasec

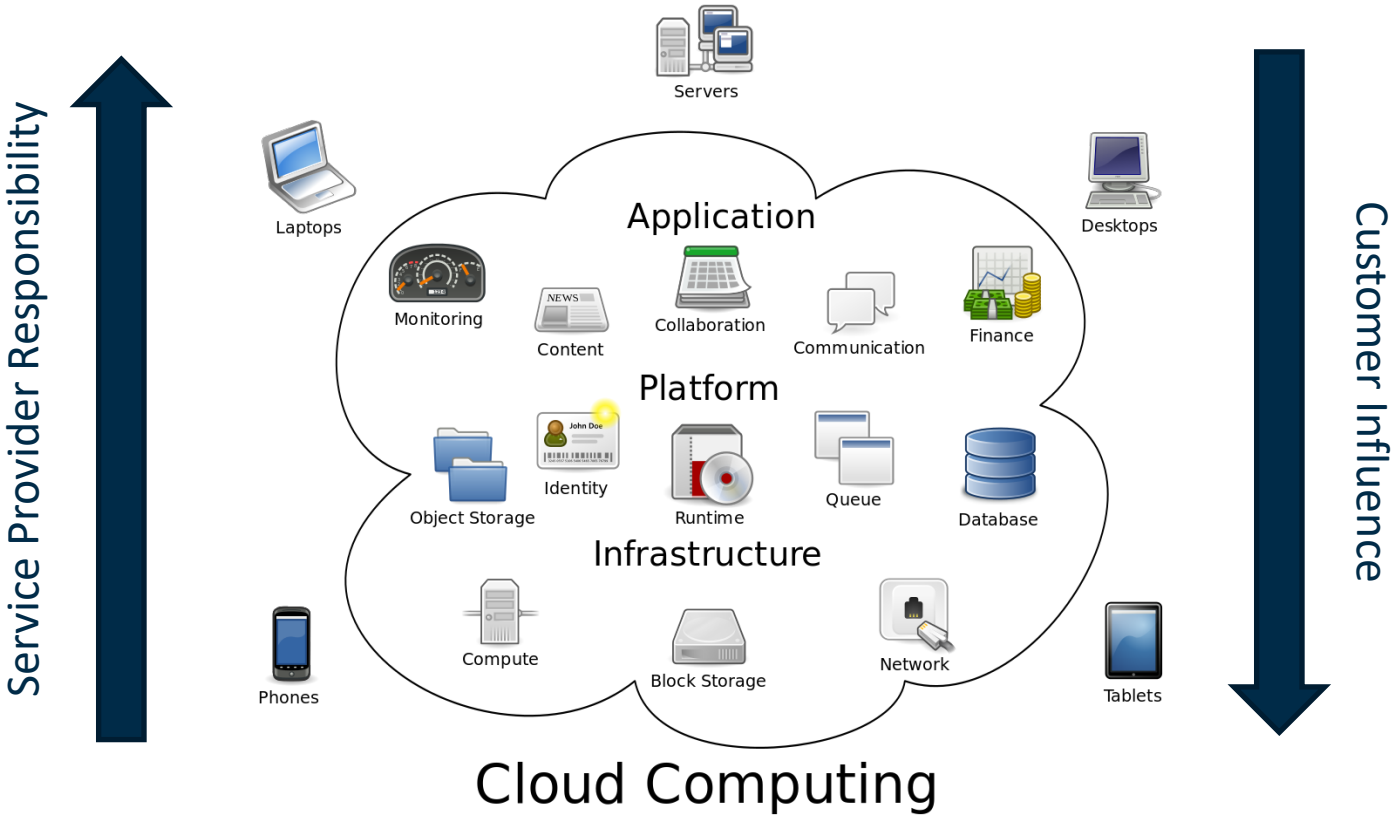
## Verantwortlichkeiten zwischen Kunde & Cloud-Dienstleister (hier: Microsoft)



# Shared Responsibility Model

carmasec



# Fazit & Tipps

carmasec

1. **Cyber-Sicherheit-Awareness:**
    - Thematisches Bewusstsein (und Verständnis) über Informationssicherheit
2. **Risikomanagement:**
    - Definition des individuellen Risikoprofils (Risikoanalyse)
    - Etablierung eines Managementsystems für Informationssicherheit und Datenschutz
    - Berücksichtigung von technologie-spezifischen Risiken (bspw. Cloud)
3. Definition und Umsetzung von geeigneten **technischen und organisatorischen Maßnahmen** („TOMs“)
4. **DAS WICHTIGSTE: KEINE ZEIT VERLIEREN UND HEUTE STARTEN**

# Checkliste / Themenüberblick

carmasec

- Anforderungsmanagement, Auswahlprozess
- Servicemanagement, Cloud-Betrieb
- Datenmigration, Dienstleisterabhängigkeit
- Verantwortung, Berechtigungen


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

carmasec Ltd. & Co. KG
Ruhrallee 185
45136 Essen
Germany

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

# Steckbrief Referent

***Carsten Marmulla***

*Managing Partner &*
*Senior Trusted Advisor*

**Skills und Themenschwerpunkte**:

- 20 Jahre IT-Branchenerfahrung (Projekt-management- und IT-Beratungserfahrung)
- Zertifizierungen: Certified Information Security Manager (CISM), ITIL v3, ISO 27001 Auditor (ISMS), COBIT-Practitioner, PRINCE2-Practitioner, ...
- Informationssicherheitsmanagement (ISO 27001, BSI IT-Grundschutz)
- IT-Servicemanagement gemäß ITIL v3
- IT-Sicherheit & Datenschutz
- IT-GRC: IT-Governance, IT-Risikomanagement, IT-Compliance

**Projekterfahrungen (Auszug):**

- Aufbau und Optimierung von IT-Servicemanagementprozessen
- Erstellung von Sicherheitskonzepten; Schutzbedarfsfeststellungen; Organisatorische Reifegradermittlung; Durchführung von Schwachstellen-/ Risiko- und Business Impact Analysen (BIA); Identifizierung und Steuerung der Maßnahmen
- Definition von Prozessen für Informations-, IT-Sicherheit sowie Datenschutz, Erstellung von Informationssicherheitsrichtlinien, Festlegung, Einführung und Kontrolle der Sicherheitspolitik und Sicherheitsstrategie
- Konzeption, Aufbau und Einführung von Managementsystemen für Informationssicherheit gemäß ISO 27001 und Zertifizierungsvorbereitung; Konzeption und Implementierung von Kennzahlensystemen (KPI)
- Optimierung der IT-Wertschöpfung im Rahmen der IT-Governance (COBIT); Überprüfung der Einhaltung der IT-Compliance und der Datenschutzanforderungen

**Referenzkunden (Auszug)**:

- Deutsche Post AG
- Postbank Systems AG
- Vodafone Group Services GmbH
- Deutsche Telekom AG
- Vodafone D2 GmbH
- DeTeAccounting GmbH
- Fresenius Netcare GmbH
- TÜV Rheinland AG
- OXEA GmbH
- Grünenthal GmbH
- ProActiv Service GmbH (Talanx)
- Hochtief Concessions GmbH

# Leistungsangebot

carmasec

**Information Security Management**
Wegweisende Konzepte auf Basis langjähriger Expertise und Best-Practise.

**Security Automation**
Automatisierte Lösungen für das Security Management in agilen Entwicklungsprozessen und im Incident Response.

**Data Privacy Protection**
Evaluation relevanter Datenschutzvorgaben und Sicherstellung der Compliance (z.B. BDSG und DSGVO).

**Governance, Risk, Compliance**
Beratung des Managements im GRC Kontext auf Basis der spezifischen Anforderungen.

**Agile Security**
Integration des agilen Software Development Lifecycle in das vorhandene Security Management (Secure SDLC).

**Cyber Resilience**
Schutz vor Cyber Attacken und Steigerung der Widerstandskraft gegen Angriffe auf die Informationssicherheit.

**Business Continuity**
Aufrechterhaltung und Wiederherstellung des Geschäftsbetriebs nach Security Incidents.

**DevSecOps**
Transformation zu DevSecOps durch geräuschlose Integration von Security Controls in die DevOps und CI/CD Pipeline.

**Security Research**
Evaluation aktueller Security Entwicklungen und neuartiger Angriffsszenarien sowie Ableitung von Abwehrstrategien.

# Checkliste Cloud Computing & Compliance

carmasec

- Anforderungsmanagement, Auswahlprozess:
  - Definieren Sie Ihre IT-Anforderungen so detailliert wie möglich und prüfen daraufhin die für Sie verfügbaren Cloud-Services
  - Wählen Sie für Ihre Anforderungen das passende Service- und Deliverymodell aus  (Services: IaaS, PaaS, SaaS; Delivery: Public, Private, Hybrid Cloud)
  - Definieren Sie Ihre IT-Service-Managementprozesse für die Cloud-Nutzung: wie bearbeiten Sie Störungen oder Leistungsanpassungen; welche Servicelevel stellt Ihnen der Cloud-Serviceanbieter zur Verfügung

# Checkliste Cloud Computing & Compliance

carmasec

- Servicemanagement, Cloud-Betrieb:
  - Definieren Sie Ihre Schutzziele: welche Daten sind kritisch, welche Daten enthalten einen Personenbezug, welche Daten müssen dauerhaft verfügbar sein, welche Daten müssen vor unbeabsichtigten Veränderungen geschützt werden - beachten Sie hierbei insbesondere auch rechtliche Vorgaben zum Datenschutz und zur Revisionssicherheit
  - Definieren Sie Ihr Notfallmanagement, welche Maßnahmen ergreifen Sie und/oder Ihr Cloud-Serviceanbieter im Störungsfall oder bei Sicherheitsvorfällen (IT-Angriffen); definieren Sie entsprechende Gegenmaßnahmen; beachten Sie etwaige Fristvorgaben zur Meldung von Sicherheits- und Datenschutzverstößen

# Checkliste Cloud Computing & Compliance

carmasec

- Servicemanagement, Cloud-Betrieb (Fortsetzung):
  - Verwenden Sie für alle Komponenten, die in Ihrer operativen Verantwortung liegen, sichere und gehärtete Konfigurationseinstellungen; vermeiden Sie die Verwendung von durch Dritte vorkonfigurierte Komponenten
  - Definieren Sie den Umgang mit sicherheitsrelevanten Aktualisierungen für alle Komponenten, die in Ihrer operativen Verantwortung verbleiben, dokumentieren Sie diesen Prozess und setzen diesen um

# Checkliste Cloud Computing & Compliance

carmasec

- Datenmigrationen, Dienstleisterabhängigkeit:
  - Planen und kalkulieren Sie Ihre Datenmigration in Cloud-Services und ggf. auch den Rückweg - es entstehen schnell große Datenmengen, die auch in modernen Breitbandnetzen entsprechende Übertragungskapazitäten erfordern; prüfen Sie alternative Konzepte zur Migration
  - Berücksichtigen Sie die Gefahr einer unüberwindbaren Abhängigkeit zu Ihrem Cloud-Serviceanbieter, dem so genannten „Vendor Lock-in“; prüfen Sie bereits frühzeitig Alternativen oder Multi-Cloud-Konzepte und bedenken Sie Hybrid-Lösungen; verringern Sie wo Immer möglich die Abhängigkeiten zu Ihrem Dienstleister; machen Sie sich Gedanken über Datenexporte und Migrationen von Cloud-Diensten zu anderen Dienstleistern

# Checkliste Cloud Computing & Compliance

carmasec

- Verantwortung, Berechtigungen und Risikomanagement:
  - Setzen Sie sich ausführlich mit dem Modell der geteilten Verantwortlichkeit („Shared Responsibility Model“) der Cloud-Serviceanbieter auseinander; beachten Sie die für das jeweilige Servicemodell für Sie geltende Definition für welche Ebenen Ihr Cloud-Serviceanbieter operative Verantwortung übernimmt; bedenken Sie, dass die rechtliche Gesamtverantwortung und die Haftung stets beim Auftraggeber verbleibt
  - Definieren Sie, wer auf welche Daten zugreifen darf und erstellen Sie ein rollenbasiertes Berechtigungskonzept, welches sowohl rechtliche Anforderungen als auch Ihre Geschäftsprozesse berücksichtigt; definieren Sie Prozesse zur Vergabe und zum Entzug von Datenzugriffsberechtigungen

# Checkliste Cloud Computing & Compliance

carmasec

- Verantwortung, Berechtigungen und Risikomanagement (Fortsetzung):
  - Bewerten Sie insbesondere Cloud-spezifische Bedrohungen und Risiken durch vorhandene Modellierungshilfen; definieren Sie Ihren Risikoappetit und planen Sie entsprechende Strategien zur Risikobehandlung

# Checkliste Cloud Computing & Compliance

carmasec

- Datenverschlüsselung:
  - Verschlüsseln Sie durchgängig den Transport von Daten außerhalb und innerhalb Ihrer Infrastruktur mit anerkannten und sicheren Verfahren nach dem Stand der Technik
  - Verschlüsseln Sie geschäftskritische und/oder personenbezogene Daten bei der Datenhaltung wo dies notwendig oder sinnvoll ist; Basis hierfür sind sowohl rechtliche Anforderungen als auch Ihre individuelle Definition des Risikoappetits
  - Pseudonymisieren oder anonymisieren Sie personenbezogene Daten, sofern dies durch Regularien erforderlich ist
  - Konzipieren Sie die Schlüsselverwaltung und definieren Sie den Zugriff auf Schlüsselmaterial

# Checkliste Cloud Computing & Compliance

carmasec

- Audit und Kontrolle:
  - Führen Sie regelmäßige Sicherheitsüberprüfungen durch
  - Kontrollieren Sie den ordnungsgemäßen Umgang mit Ihren Daten bei Ihrem Dienstleister; prüfen Sie entsprechende Auditberichte und Zertifizierungen oder nutzen Sie Ihr Audit-Recht
  - Last but not least: dokumentieren Sie alle oben genannten Schritte individuell für Ihr Unternehmen, um eine transparente Nachvollziehbarkeit und regelmäßige Prüfung zu ermöglichen