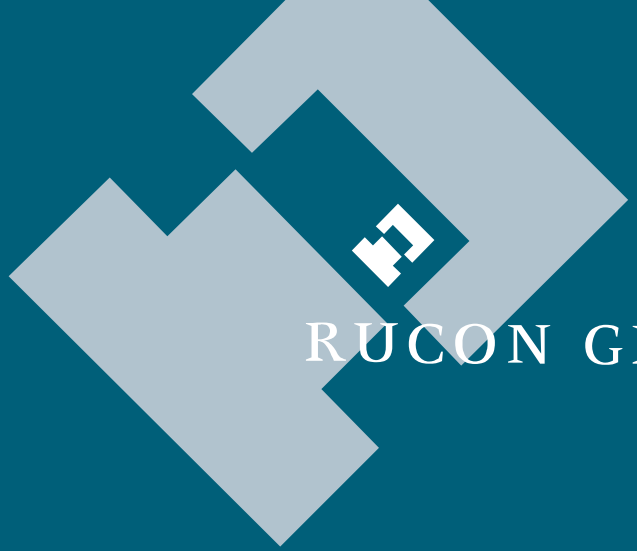
SEIEN SIE **SICHER.**

Blog: www.rucon-group.com/blog

Newsletter: www.rucon-group.com/newsletter

Twitter: @Uwe_Ruehl



RUCON GRUPPE

Uwe Rühl

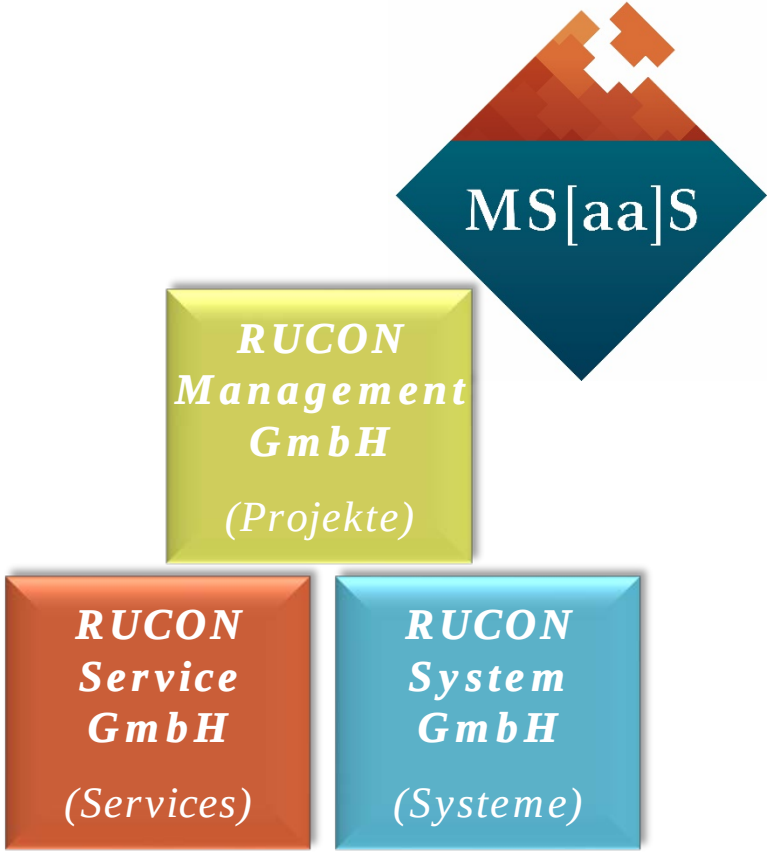
Zertifizierung von Cloud Information Security?

ISO/IEC 27017 und ISO/IEC 27018 - was geht und was geht nicht.

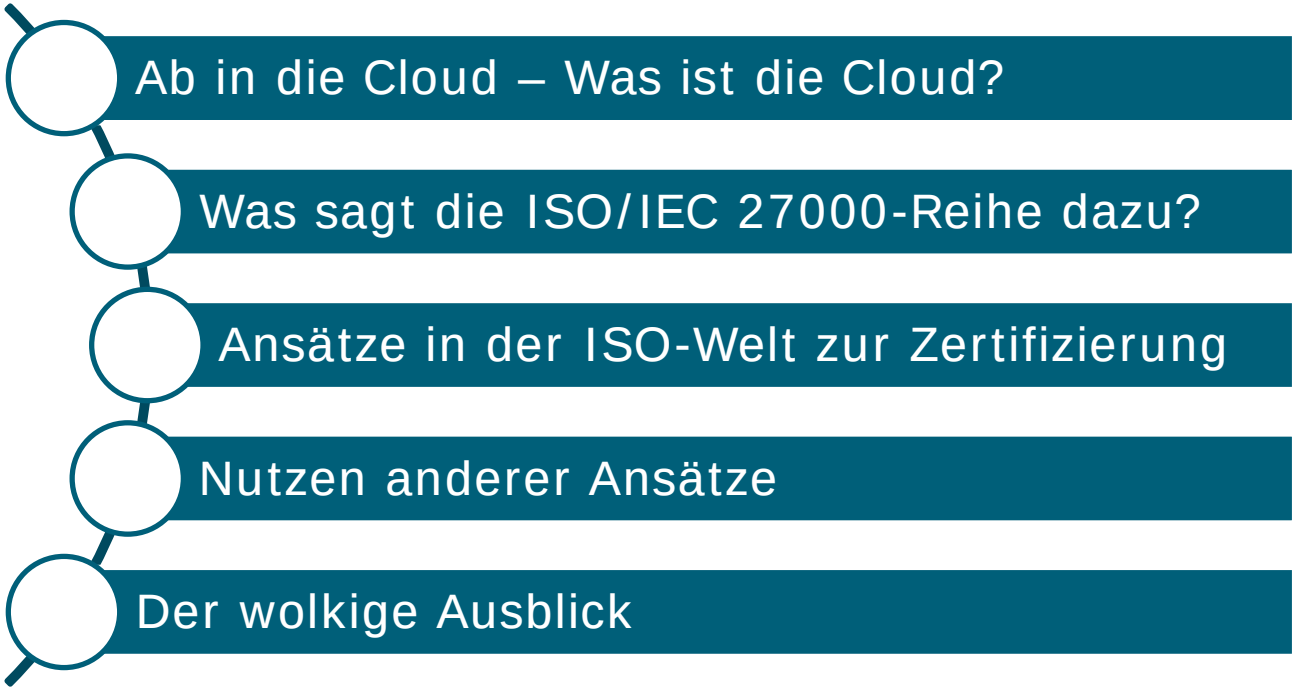
Die RUCON Gruppe

Schwerpunkt: Organizational Resilience

- Informationssicherheitsmanagement (ISMS)
- Business Continuity Management (BCMS)
- Risikomanagement
- Krisenmanagement
- Integrierte Managementsysteme



Agenda

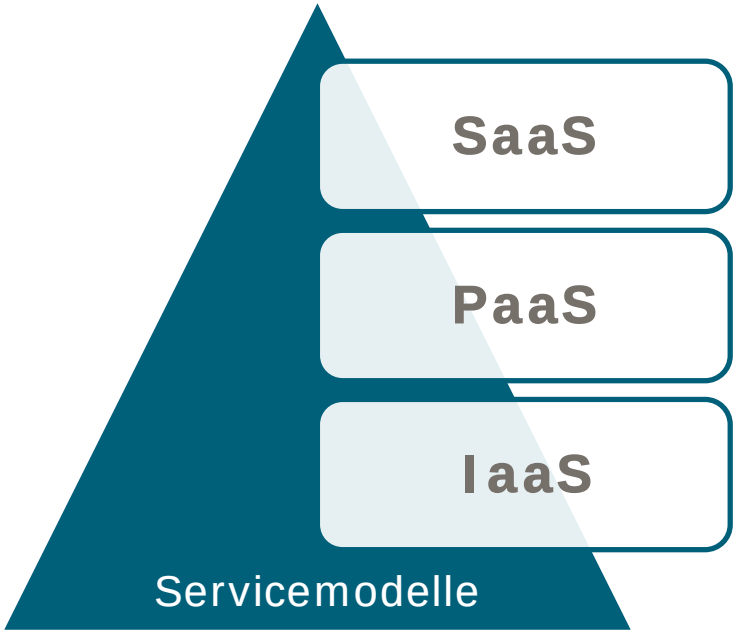

Ab in die Cloud – Was ist die Cloud?
Was sagt die ISO/IEC 27000-Reihe dazu?
Ansätze in der ISO-Welt zur Zertifizierung
Nutzen anderer Ansätze
Der wolkige Ausblick

SEIEN SIE **SICHER.**

RUCON GRUPPE

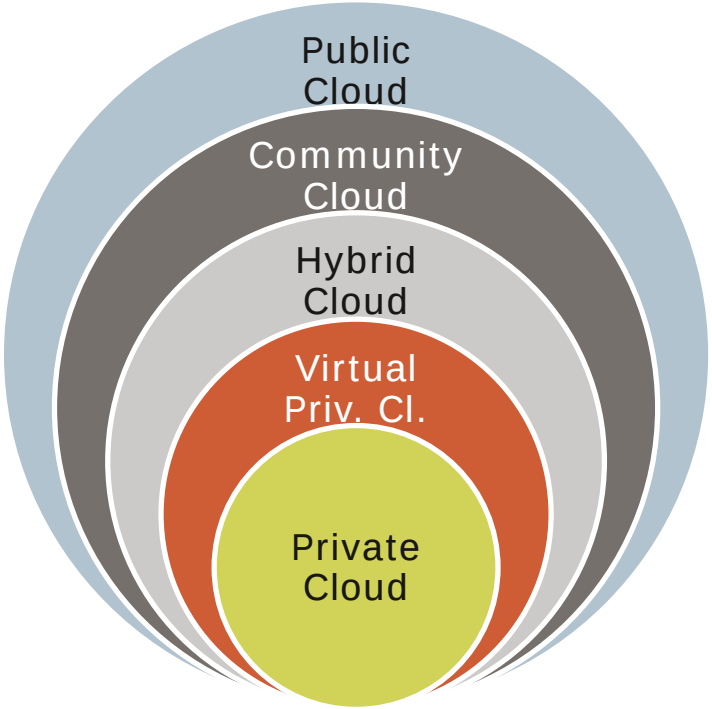
Ab in die Cloud – Was ist die Cloud?

Definition durch NIST



NIST – National Institute of Standards and Technology

Definition durch NIST - Liefermodelle



NIST – National Institute of Standards and Technology

Definition in ISO/IEC 27000

Definition in ISO/IEC 27018

3.7 Public Cloud Service Provider

Party which makes cloud service available according to the public cloud model.

RUCON GRUPPE

Was sagt die ISO/IEC 27000-Reihe dazu?

ISO/IEC 27001 & Cloud Computing

Noch einmal:

In der ISO/IEC 27000/1 gibt es keine Definition, was Cloud Computing bedeutet – Cloud wird nicht erwähnt!

Also:

- Halten wir uns am besten an NIST oder vergleichbare Definitionen!

Quelle: „Hartmann Schedel, „Weltchronik 1493“, Blatt C

ISO/IEC 27003

Empfehlungen auf 3 Ebenen...

Ebene	Aspekte	Abgrenzung (Beispiele)
Organizational Scope	▪ Geschäftsprozesse ▪ Unterstützungsprozesse ▪ Aktivitäten	▪ Verträge ▪ Aufbau- und Ablauforganisation ▪ OLA`s
ICT Scope	▪ Informationsverarbeitende Einrichtungen ▪ IT Systeme	▪ Netzzonen ▪ ISO-OSI-Modell
Physischer Scope	▪ Räume ▪ Racks	▪ Zutrittskontrollierbare Bereiche

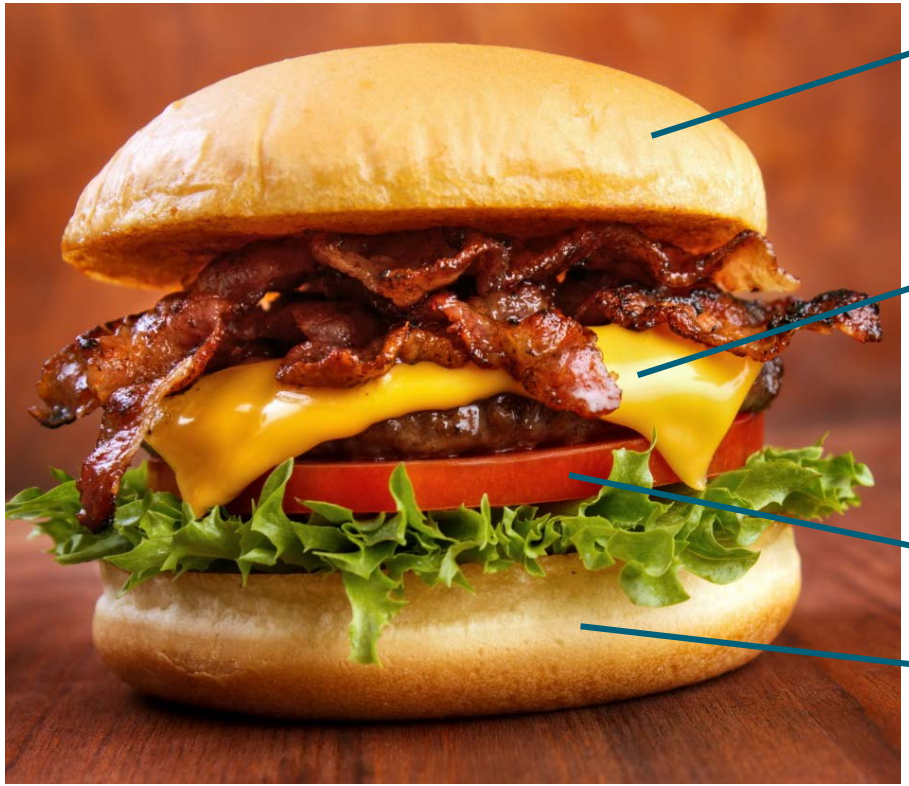
Herausforderung: „schneiden“ des Anwendungsbereichs

Burg

vs.

Burger

Quelle: „Hartmann Schedel, „Weltchronik 1493“, Blatt C und Fotolia



Primary Assets (ISO/IEC 27005)

- Informationen
- Business Processes

Information Processing Facilities (ISO/IEC 27000)

(alternativ: Information Systems oder Business Services)

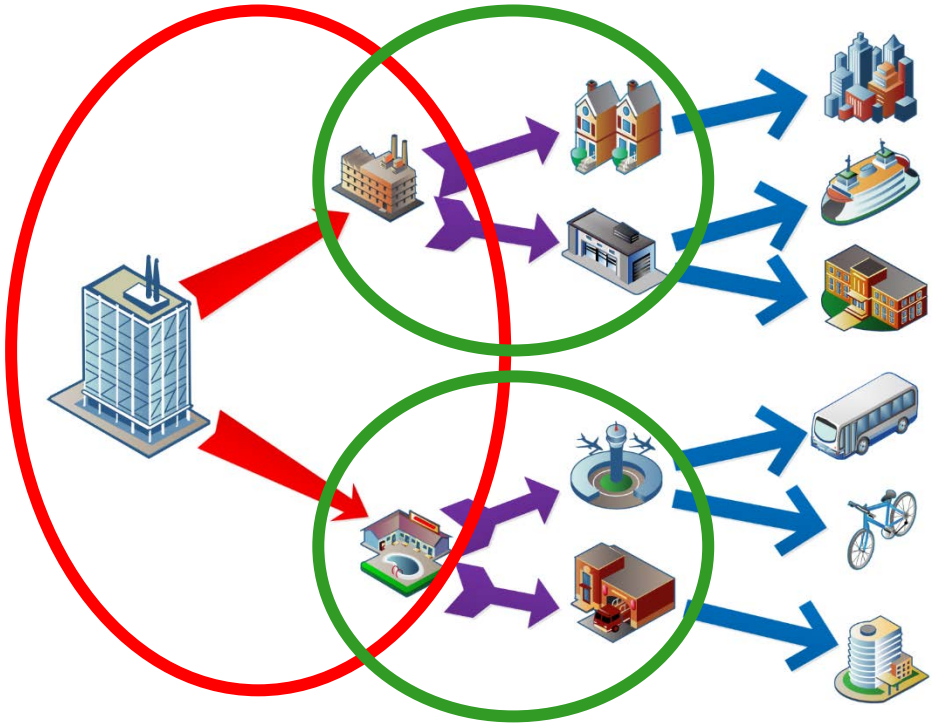
Technical Services (Hilfsebene)

Supporting Assets (ISO/IEC 27005)

- Hardware, Netzwerk, Software…

Quelle: Fotolia

Ausgelagerte Prozesse



Quelle: eigenes Bild

Muss direkt gesteuert werden

8.1

A.15.1.1

A.15.1.2

A.15.2.1

A.15.2.2

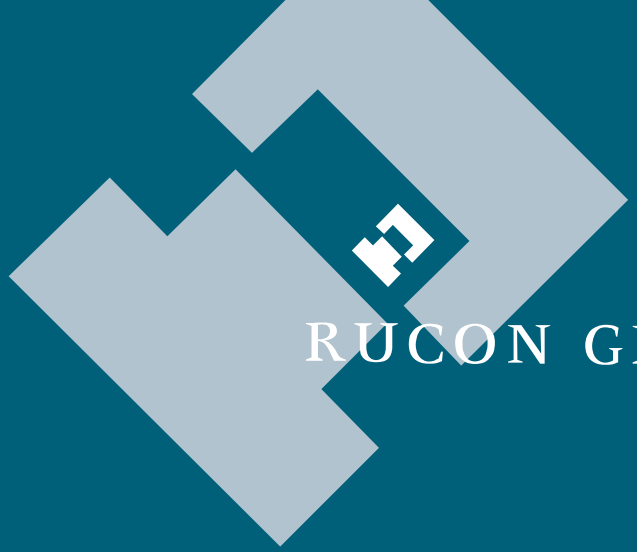
Muss den Auftraggebern durch Auftragnehmer nachgewiesen werden

A.15.1.3

Was heißt das nochmal konkret?

1. Kenne Deinen Anwendungsbereich, vor allem seine Grenzen! **Burg** vs. **Burger**!
2. Kenne die Abhängigkeiten zu externen Dienstleistungserbringern!
3. Erkenne Deine Geschäftsinformationen und bewerte deren Wertigkeit („Klassifizierung“)!
4. Behandle Beziehungen zu Dienstleistungserbringern abhängig der Risiken!

SEIEN SIE **SICHER.**



RUCON GRUPPE

Ansätze in der ISO-Welt zur Zertifizierung „Cloud“

INTERNATIONAL STANDARD

ISO/IEC 27017

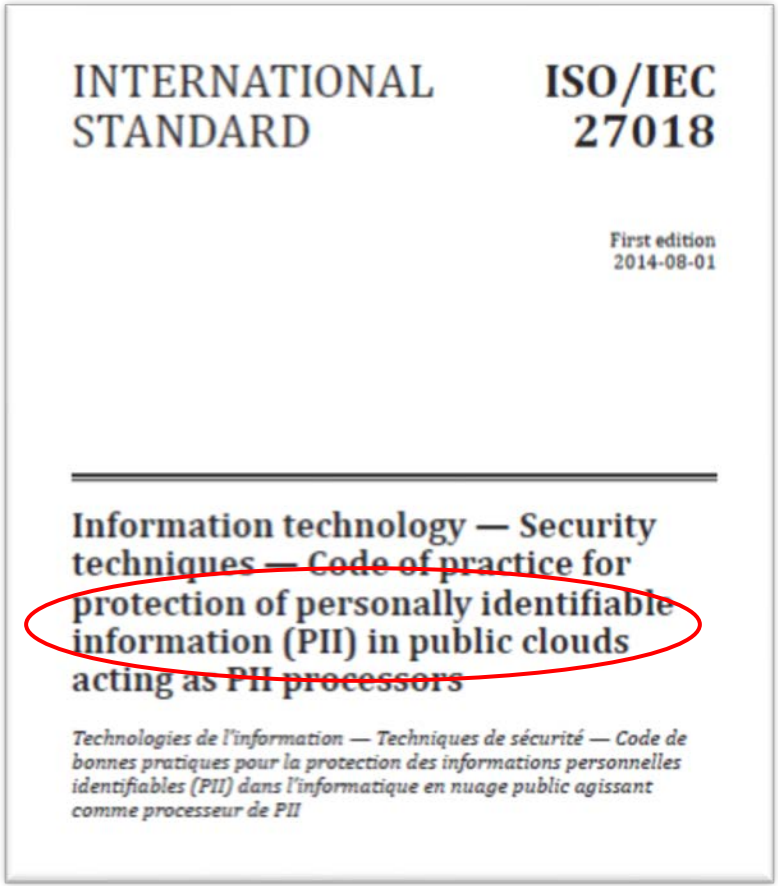
First edition
2015-12-15

Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services

Technologies de l'information — Techniques de sécurité — Code de pratique pour les contrôles de sécurité de l'information fondés sur l'ISO/IEC 27002 pour les services du nuage

- Adressiert die Nutzung und Bereitstellung von „Cloud Services“
- Sie nutzt den selben Aufbau wie ISO/IEC 27001 Annex A
- Es werden zusätzliche Empfehlungen zur ISO/IEC 27002 gegeben

Quelle: International Organization for Standardization, Genf.



INTERNATIONAL STANDARD

ISO/IEC 27018

First edition
2014-08-01

Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors

Technologies de l'information — Techniques de sécurité — Code de bonnes pratiques pour la protection des informations personnelles identifiables (PII) dans l'informatique en nuage public agissant comme processeur de PII

- Selbe Struktur wie ISO/IEC 27001 Annex A
- Adressat: Cloud Service Provider
- Hat „nur“ Schutz von PII im Fokus
- Baut auf ISO/IEC 29100-Prinzipien auf
- Spricht direkt den PII Processor an
- Es werden zusätzliche Controls definiert

Quelle: International Organization for Standardization, Genf.

DEUTSCHE NORM November 2016

DIN ISO/IEC 27009

DIN

ICS 03.100.70; 03.120.20; 35.030

Informationstechnik –
IT-Sicherheitsverfahren –
Sektorspezifische Anwendung der ISO/IEC 27001 – Anforderungen
(ISO/IEC 27009:2016)

Information technology –
Security techniques –
Sector-specific application of ISO/IEC 27001 – Requirements
(ISO/IEC 27009:2016)

Technologies de l'information –
Techniques de sécurité –
Application de l'ISO/IEC 27001 à un secteur spécifique – Exigences
(ISO/IEC 27009:2016)

- Sektorspezifische Anwendung der ISO/IEC 27001
- ISO/IEC 27017 folgt diesen Ansatz

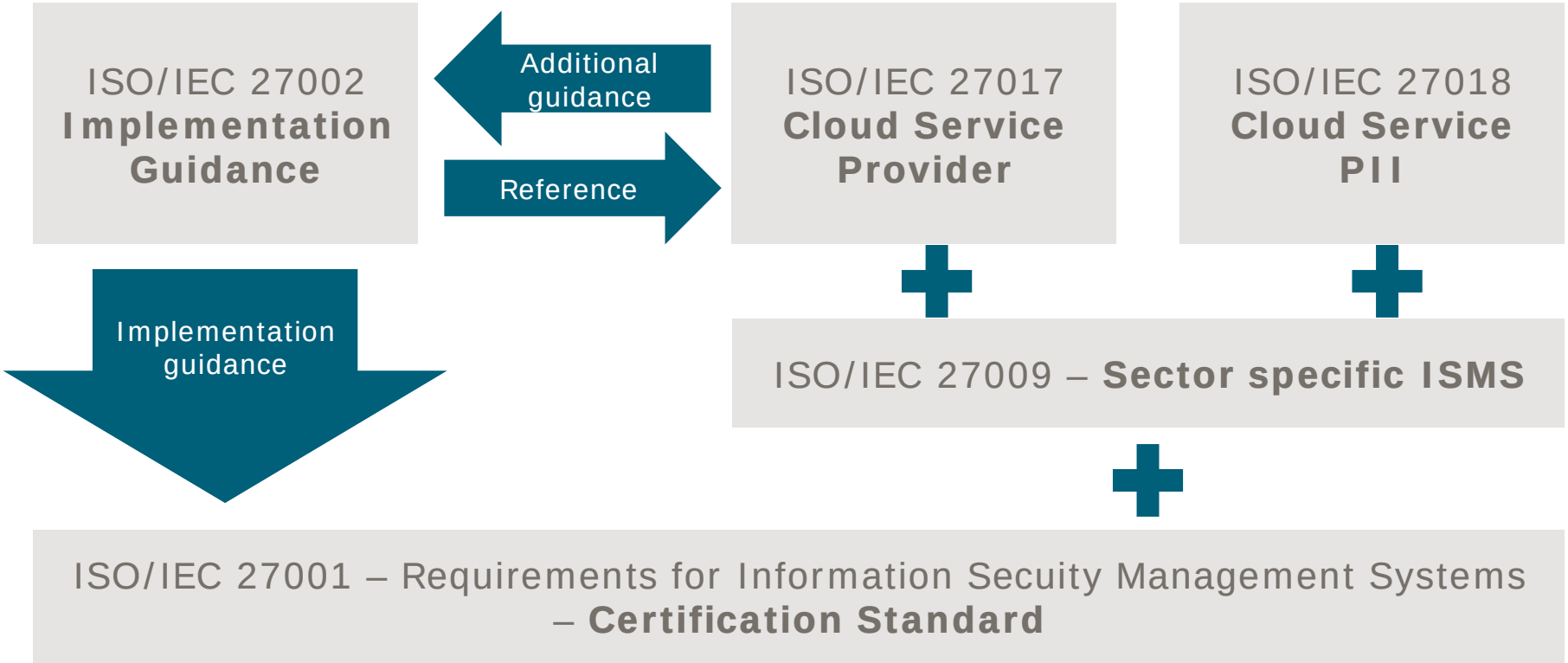
Die Herausforderung

Steigendes Interesse an Zertifizierungen für Cloud-Services

ABER: ISO/IEC 27001 ist eine generelle Basis für ISMSe

- Zertifizierungsstellen können z.B. Cloud Service ISMS Zertifizierungen auf Basis ISO/IEC 27001 und ISO/IEC 27017 & 27018 anbieten

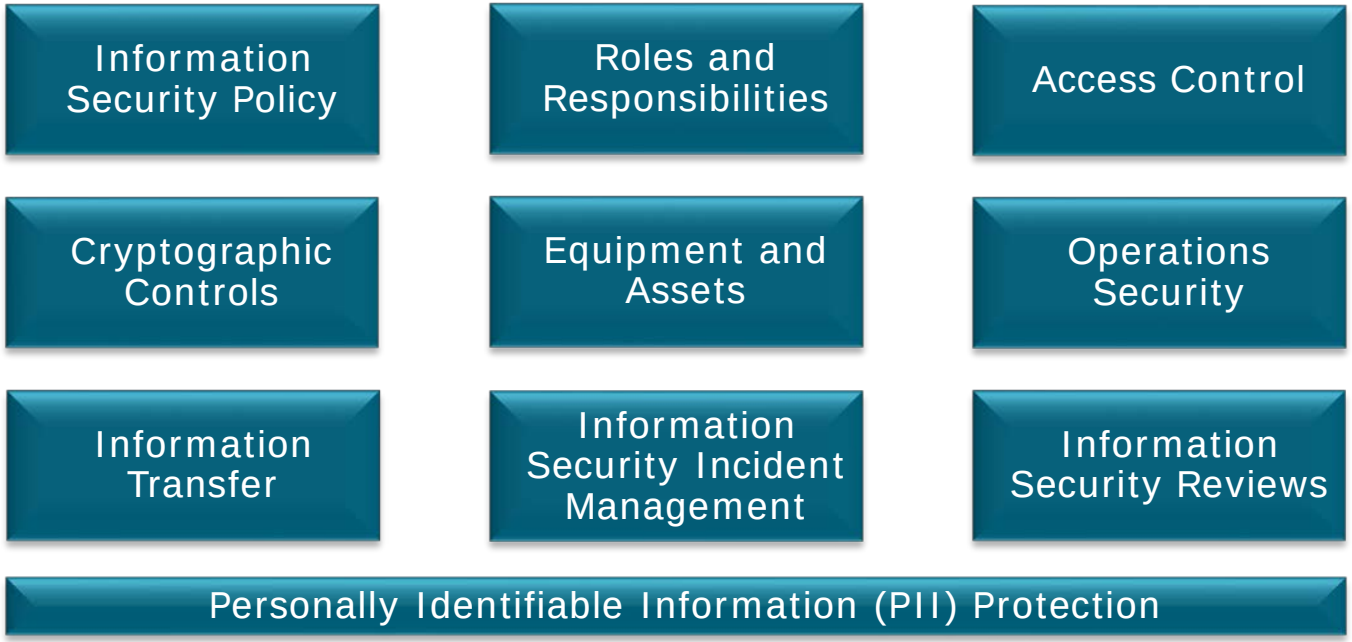
- Momentan sehen wir vor allem non-accredited Zertifizierungen!


ISO/IEC 27002
Implementation Guidance
Additional guidance
Reference
ISO/IEC 27017
Cloud Service Provider
ISO/IEC 27018
Cloud Service PII
Implementation guidance
ISO/IEC 27009 – Sector specific ISMS
ISO/IEC 27001 – Requirements for Information Secuity Management Systems – Certification Standard

Fazit

- Es werden spezifische Zertifizierungen möglich, aber immer auf Basis eines ISMS nach ISO/IEC 27001
- Sektorspezifische Normen konkretisieren, interpretieren, ergänzen ISO/IEC 27001, insbesondere Anhang A
- Derzeit Akkreditierungsprojekt in Japan für ISO/IEC 27017

Kernthemen ISO/IEC 27017 und ISO/IEC 27018



Unternehmensbefragung

Im Rahmen einer Masterarbeit

Informationssicherheit in Lieferantenbeziehungen
Supplier Management aus Sicht der ISO/IEC 27001:2013

- Einfache Zufallsstichproben von Unternehmen D-A-CH
- Schriftliche Befragung über Online-Fragebogen
- 167 Rückläufer
- 82 % der Rückmeldungen aus Deutschland
- Jeweils 9 % aus Österreich und der Schweiz

Hypothesen

- Informationsklassifizierung wird nur vereinzelt angewendet
- Unzureichende Kenntnis über rechtliche, behördliche und vertragliche Informationssicherheit vorhanden
- Konkrete Maßnahmen werden in der Minderheit vereinbart
- Überwachung erfolgt meist reaktiv
- Ein Kriterienkatalog für Maßnahmen wird für sinnvoll gehalten
- Eine Zertifizierung von Dienstleistern wird als hilfreich empfunden

RUCON GRUPPE

Nutzen anderer Ansätze

ISO/IEC 27001:2013 – 6.1.3 b *Note*

Organizations can design controls as required, or identify them from any source.

Was könnten solche *Quellen* sein?

- BSI Anforderungskatalog Cloud Computing (C5)
- Trusted Cloud Datenschutzprofil
- CSA Cloud Security Alliance
- Und viele mehr…

Anwendung in ISO/IEC 27001 Kontext

RUCON GRUPPE

Der wolkige Ausblick

Alles kann, nichts muss...

- Information Security sollte weder Enabler noch Bremser sein, sondern „Prozessbegleiter“.
- Wir kommen faktisch um „Cloud Services“ nicht mehr herum.
- Informationsklassifizierung spielt eine wesentliche Rolle als Basis für risikoorientierte Maßnahmen.
- Zertifizierung von „Cloud Services“ ist möglich und kann ein Element in der Dienstleistersteuerung sein.

Ein Bild aus der angewandten Praxis...

57. Ionic security, Inc., Atlanta, Georgia, United States of America (ISO/IEC 27018:2014) [certificate nr. 2016-007]
58. Google Inc., San Francisco, California, United States of America (ISO/IEC 27001:2013) [certificate nr. 2016-006]
59. Google Inc., San Francisco, California, United States of America (ISO/IEC 27018:2014) [certificate nr. 2016-005]
60. Google Inc., San Francisco, California, United States of America (ISO/IEC 27017:2015) [certificate nr. 2016-004]
61. AFAS Software B.V., Leusden, The Netherlands (ISO/IEC 27001:2013) [certificate nr. 2016-003]

Quelle: http://www.ey.com/gl/en/services/specialty-services/certifypoint/certifypoint---certificate-register

CLOUD Act

Clarifying Lawful Overseas Use of Data Act:
legale, aber doch unerwünschte, Zugriffe auf Informationen und deren Auswertung

SEIEN SIE SICHER.

Blog: www.rucon-group.com/blog

Newsletter: rucon-group.com/newsletter

Twitter: @Uwe_Ruehl

ISO/IEC 27017 und ISO/IEC 27018 – wertvolle Ergänzung eines bestehenden ISMS!

Danke für Ihre Aufmerksamkeit!