Cloud dienstverlening en Informatiebeveiliging

ISACA Round Table Assen - Maart 2017

ORDINA

ICT. MAAR DAN VOOR MENSEN

Even voorstellen

- Irmin Houwerzijl.
- Werkzaam bij Ordina.
- Ordina haar dienstverlening betreft o.a. traditionele hosting en Cloud dienstverlening.
- 20+ ervaring met beheer dienstverlening.

Vraag

- Wie maakt gebruik van Cloud?
- Waarvoor?
- Welke partij?

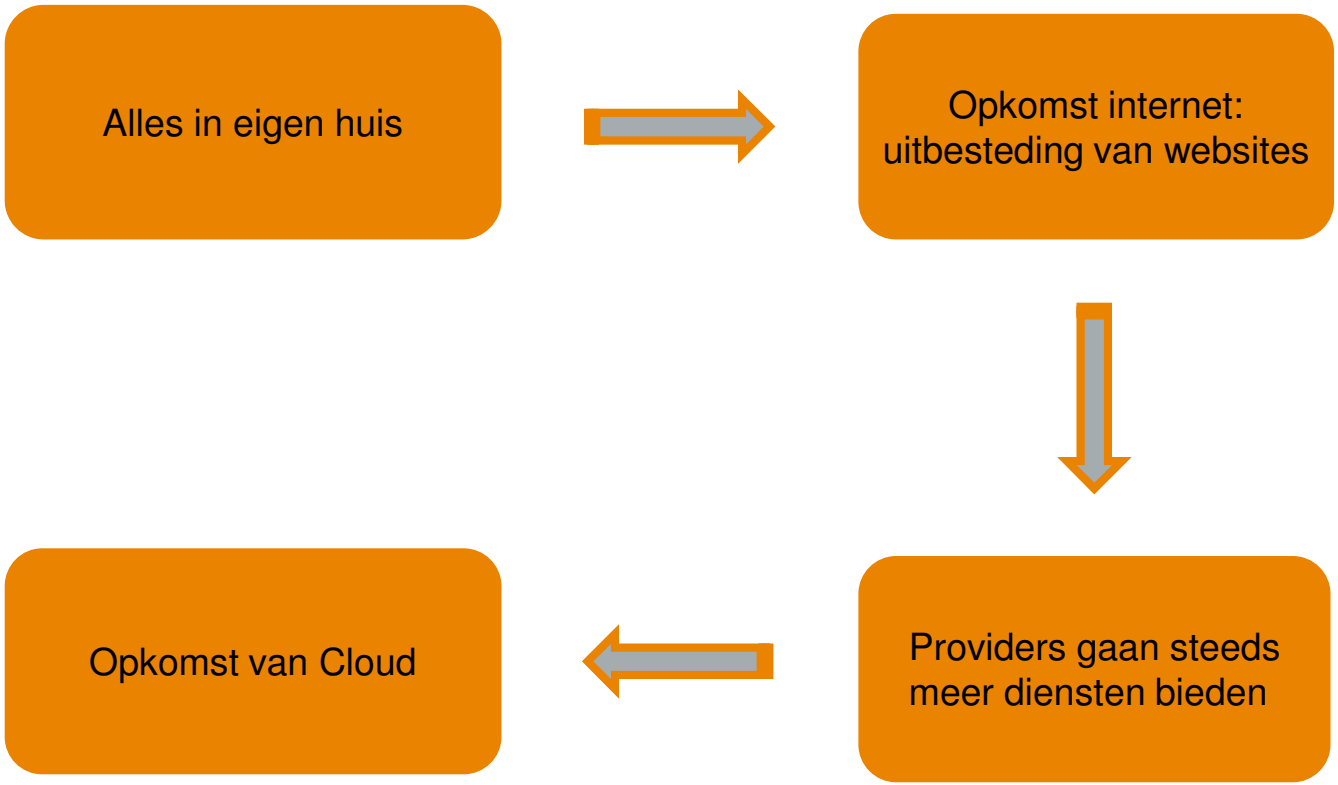
Agenda voor vanavond

- Begrip krijgen wat Cloud dienstverlening is:
  - Verschil traditioneel vs. Cloud
  - Cloud terminologie
  - Praktijk: Self Service module
- Specifieke risico's voor Cloud i.r.t. hosting.
- Informatiebronnen.
- Certificeringen in de markt.
- Aanpak.

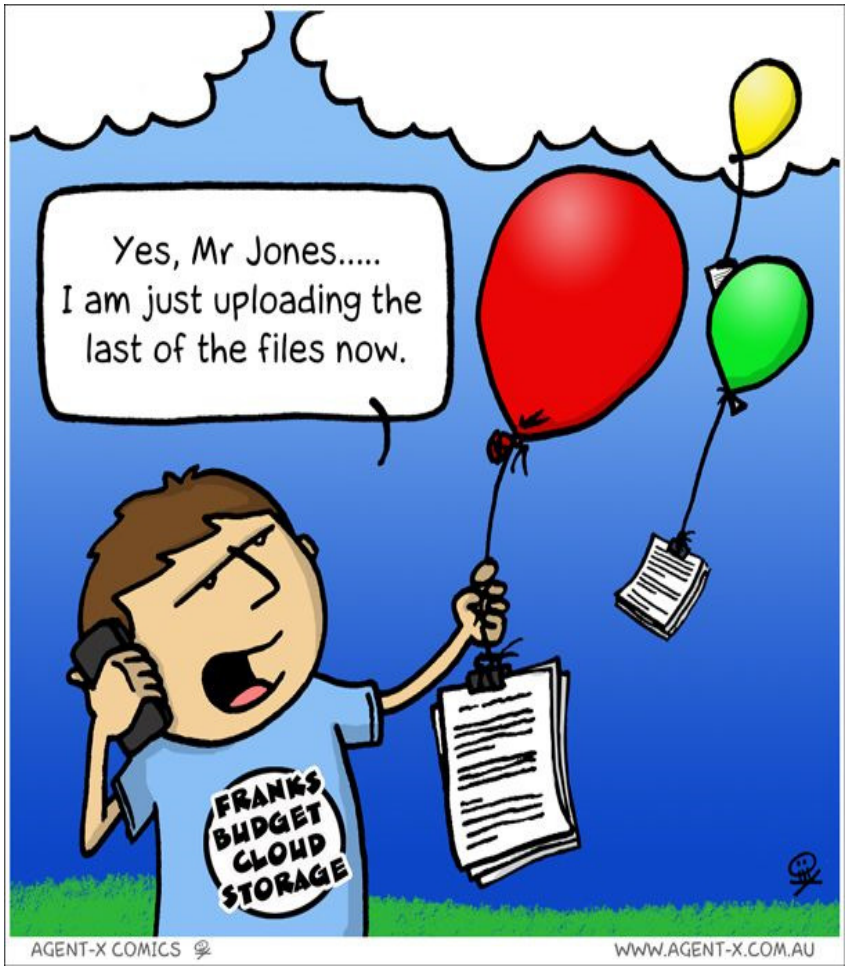
Vragen tussendoor?

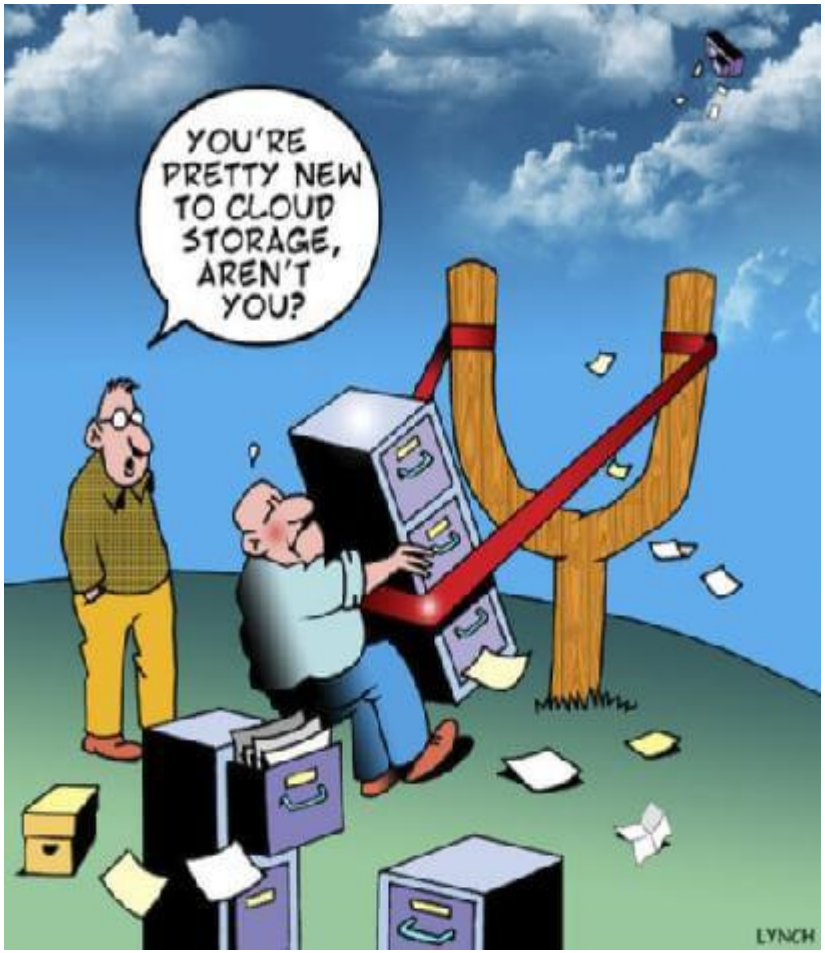
Zeer welkom!!!

Geschiedenis

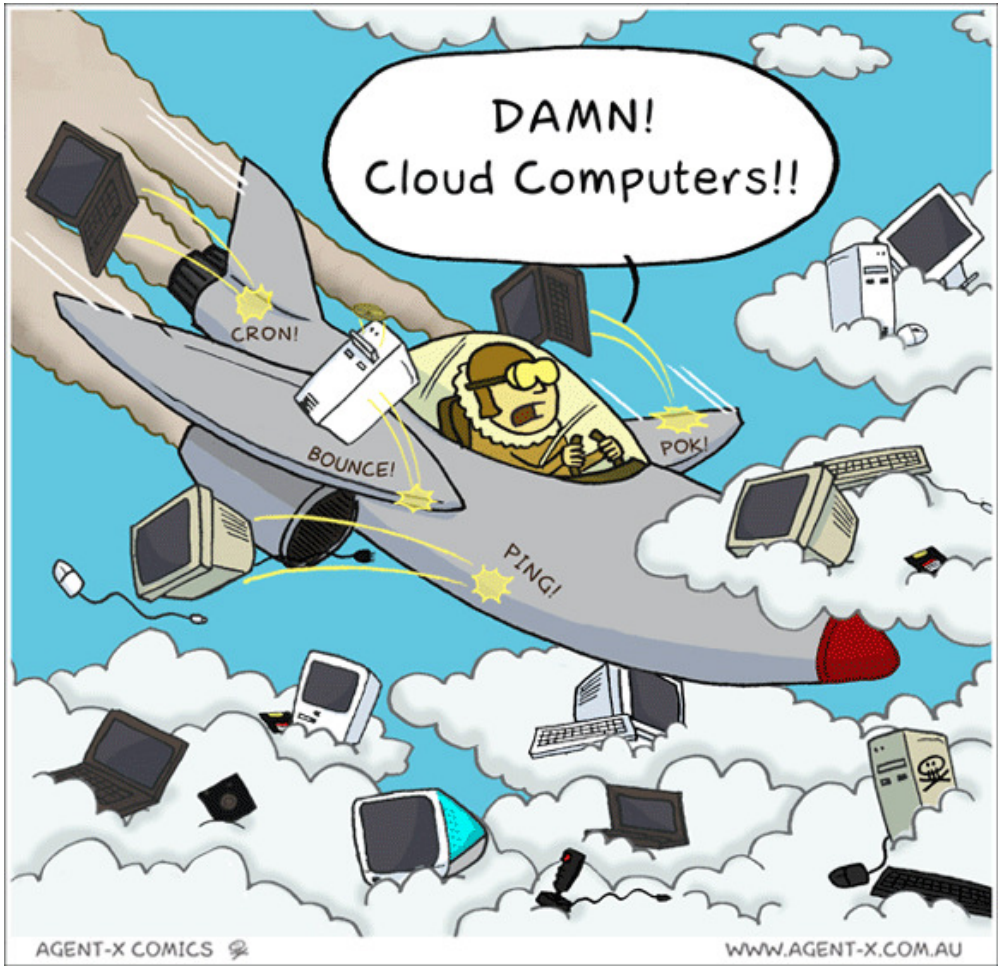


Hoe ziet dat er uit, Cloud ???





Of zo ???


DAMN!
Cloud Computers!!
CRON!
BOUNCE!
POK!
PING!
AGENT-X COMICS
WWW.AGENT-X.COM.AU


ACCORDING TO THIS, THE PLANET EARTH WAS ONCE POPULATED BY HUMANS, THEN IN 2012...
...THEY ALL MOVED TO THE CLOUD.

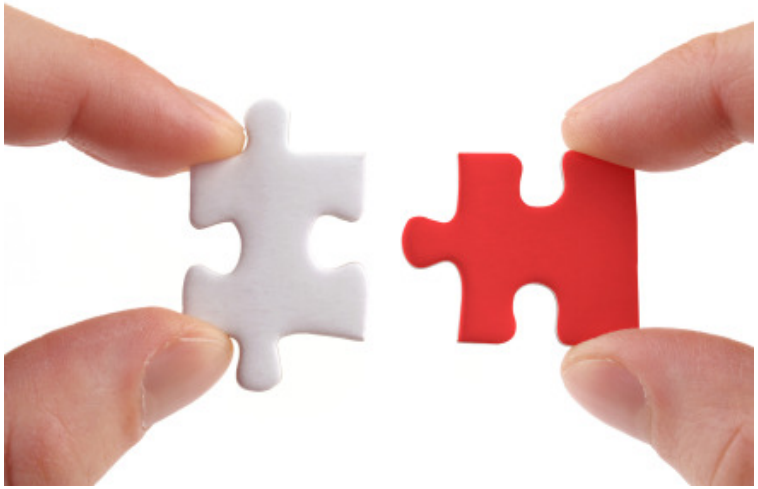
Cloud en traditionele hosting

De verschillen en overeenkomsten

ORDINA

Overeenkomsten traditionele hosting en Cloud

- Uitbesteding, gebruik maken van diensten van een andere partij.
- Afrekenmodellen per maand / minuut.
- Capex vs. Opex.
- Eigendom hardware bij de provider.



- Vaak ook uitbesteding applicatie-, database- en os beheer.

Specifieke kenmerken traditionele hosting

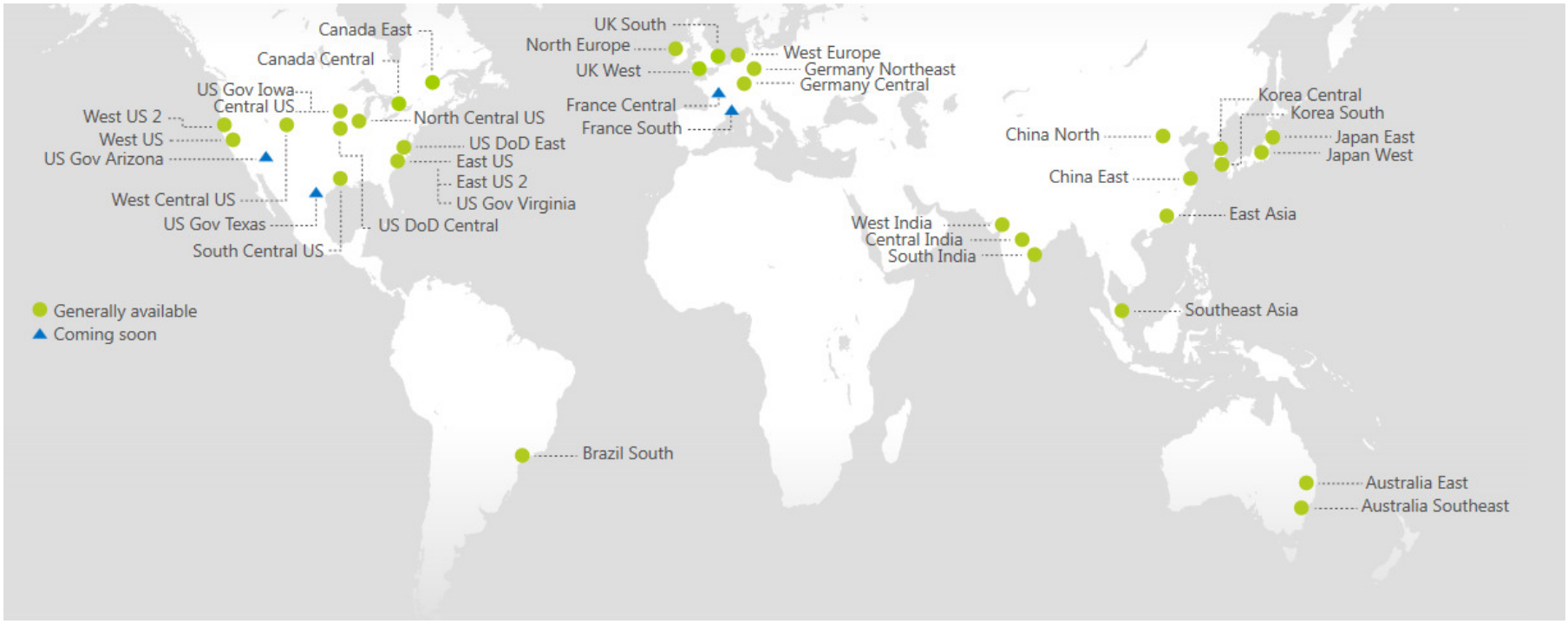
- Dienstverlening vanuit beperkt aantal datacentra relatief dicht bij elkaar b.v. in Nederland.
- Verschuiving van fysieke hardware naar virtualisatie.
- Hardware:
  - Hardware met intelligentie
  - Redundantie in de componenten
  - Relatief weinig componenten
- Beschikbaarheid: Mean Time Between Failure.

Specifieke Cloud kenmerken

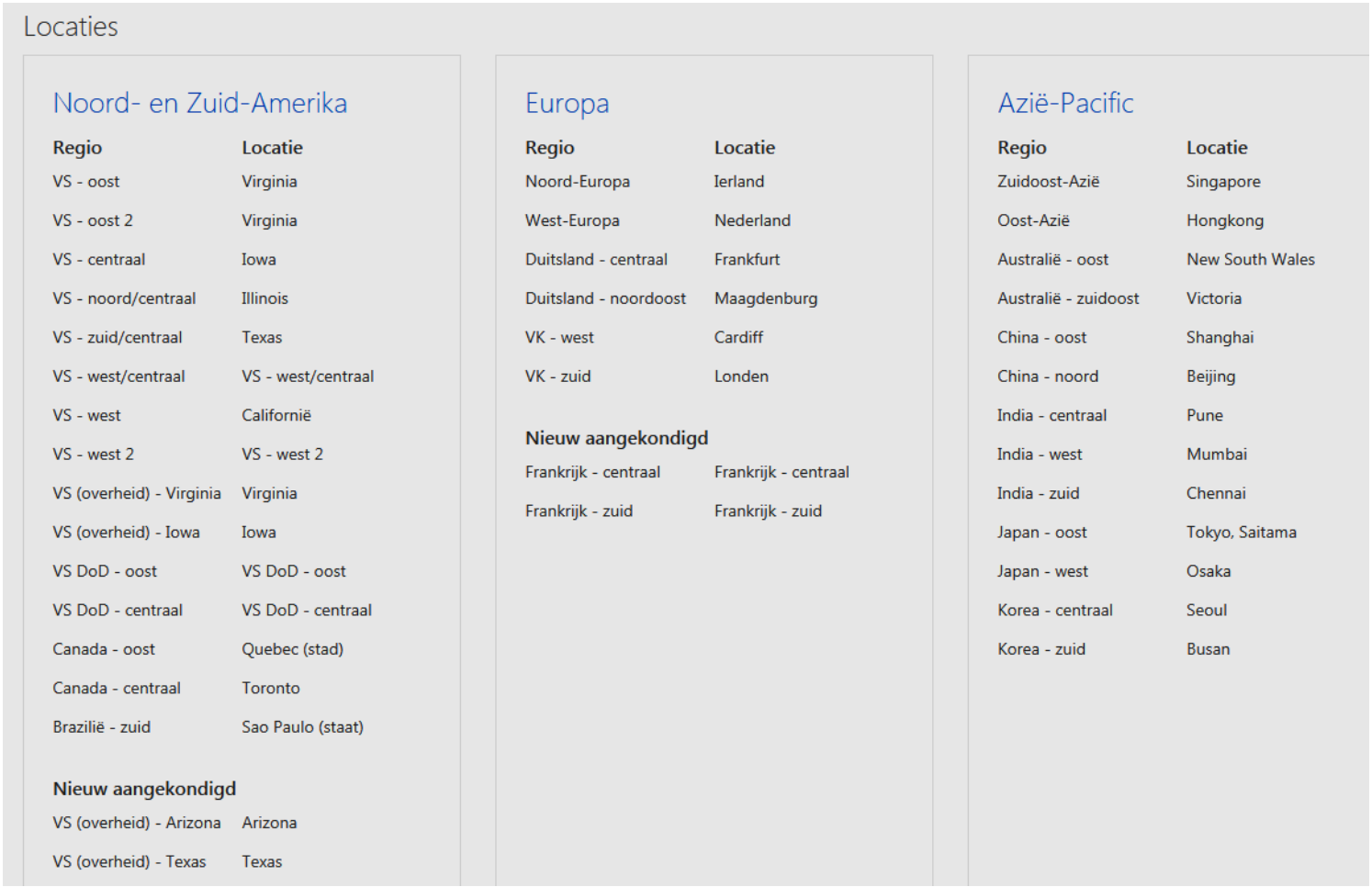
- Dienstverlening vanuit wereldwijde datacentra.
- Volledig gebruik van virtualisatie technologie.
- Hardware:
  - Eenvoudige hardware, geen intelligentie in hardware
  - Heel veel identieke componenten
  - Weinig tot geen redundantie in de componenten
- Self Service Portal.

Cloud provider markt volgens Gartner

Azure wereldwijde spreiding



Locaties



Locaties

Noord- en Zuid-Amerika

Regio	Locatie
VS - oost	Virginia
VS - oost 2	Virginia
VS - centraal	Iowa
VS - noord/centraal	Illinois
VS - zuid/centraal	Texas
VS - west/centraal	VS - west/centraal
VS - west	Californië
VS - west 2	VS - west 2
VS (overheid) - Virginia	Virginia
VS (overheid) - Iowa	Iowa
VS DoD - oost	VS DoD - oost
VS DoD - centraal	VS DoD - centraal
Canada - oost	Quebec (stad)
Canada - centraal	Toronto
Brazilië - zuid	Sao Paulo (staat)

Nieuw aangekondigd

VS (overheid) - Arizona	Arizona
VS (overheid) - Texas	Texas

Europa

Regio	Locatie
Noord-Europa	Ierland
West-Europa	Nederland
Duitsland - centraal	Frankfurt
Duitsland - noordoost	Maagdenburg
VK - west	Cardiff
VK - zuid	Londen

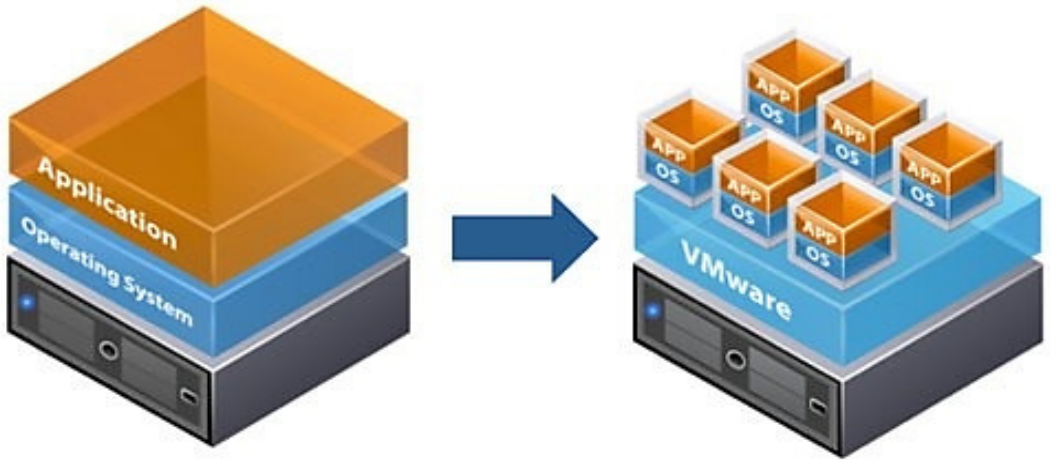
Nieuw aangekondigd

Frankrijk - centraal	Frankrijk - centraal
Frankrijk - zuid	Frankrijk - zuid

Azië-Pacific

Regio	Locatie
Zuidoost-Azië	Singapore
Oost-Azië	Hongkong
Australië - oost	New South Wales
Australië - zuidoost	Victoria
China - oost	Shanghai
China - noord	Beijing
India - centraal	Pune
India - west	Mumbai
India - zuid	Chennai
Japan - oost	Tokyo, Saitama
Japan - west	Osaka
Korea - centraal	Seoul
Korea - zuid	Busan

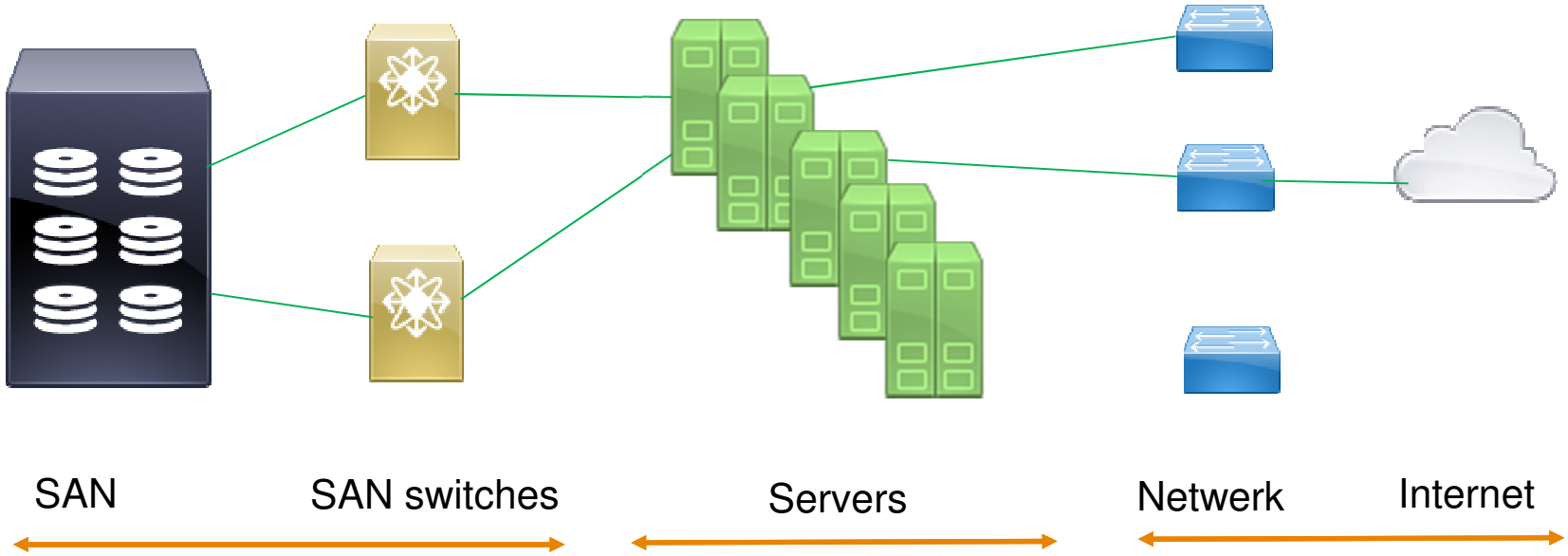
Toelichting virtualisatie



Traditional Architecture

Virtual Architecture

Traditionele hosting architectuur



Storage Array, in het echt..

Gebruik van Raid technologie

Cloud server

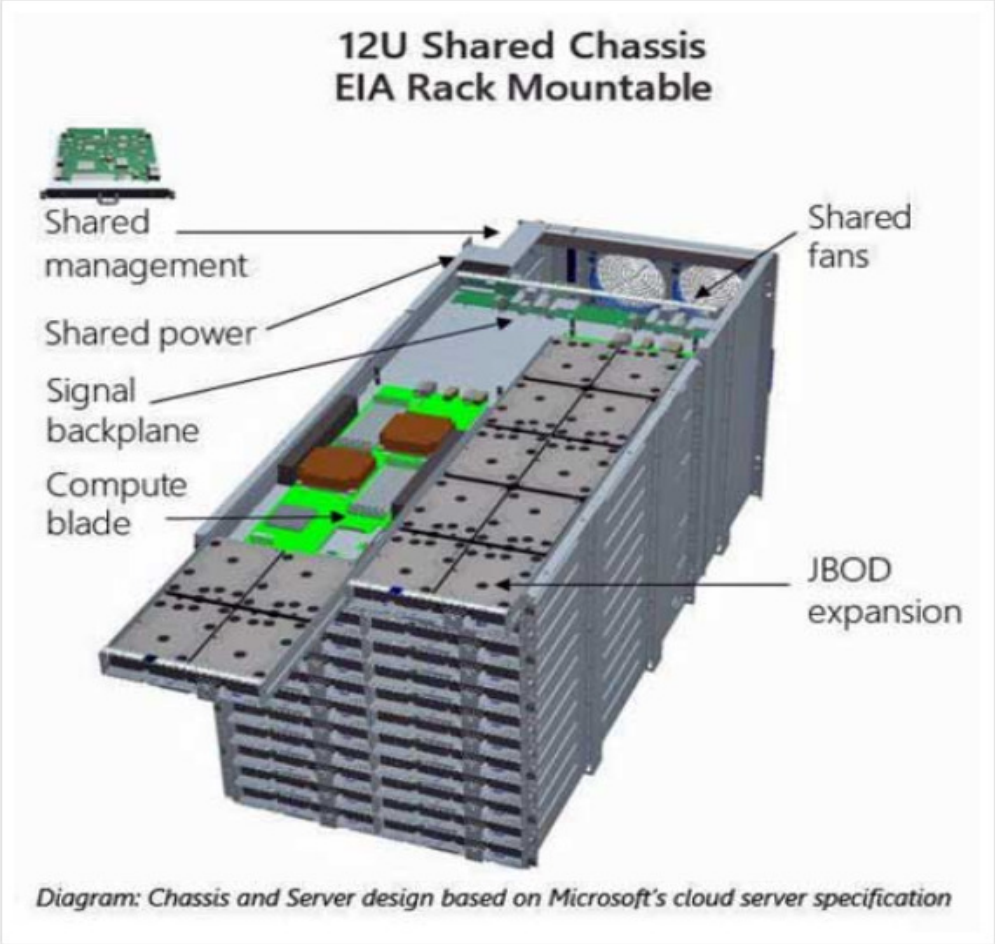


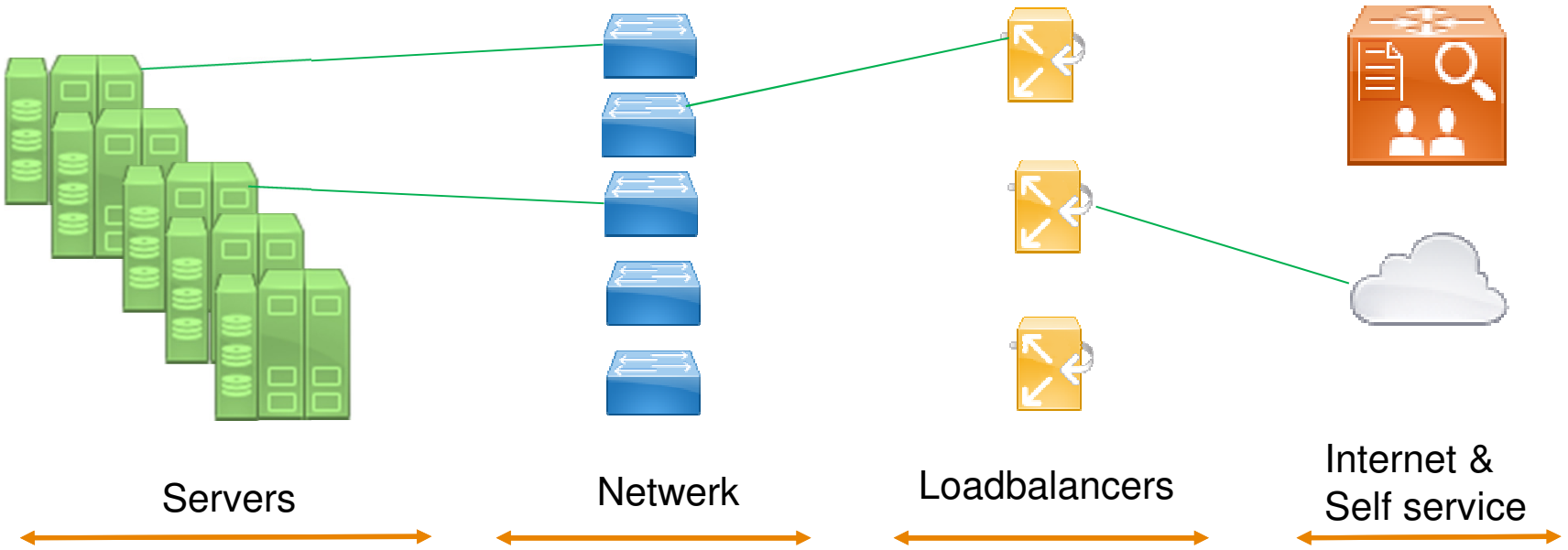
Diagram: Chassis and Server design based on Microsoft's cloud server specification

- Chassis: 96 servers
- 4 chassis per rack
- 384 servers in een rack

Traditioneel:
48 of 24 servers in een rack

Kijkje in het Cloud datacentrum

Cloud architectuur



Beschikbaarheid in de Cloud gaat niet vanzelf

- Fault domain: hardware, zoals disk, CPU (rack) etc, niet redundant.
- Update domain: Fysieke systemen en de virtualisatie laag worden in dit domein in eenmaal voorzien van patches.
- Voor virtual machines wordt 99,95% beschikbaarheid gegeven mits je twee machines hebt voor dezelfde taak.
- Availability set: Twee machines met een identieke taak zullen op Azure altijd in een ander fault- en update domain terecht komen.

Self Service

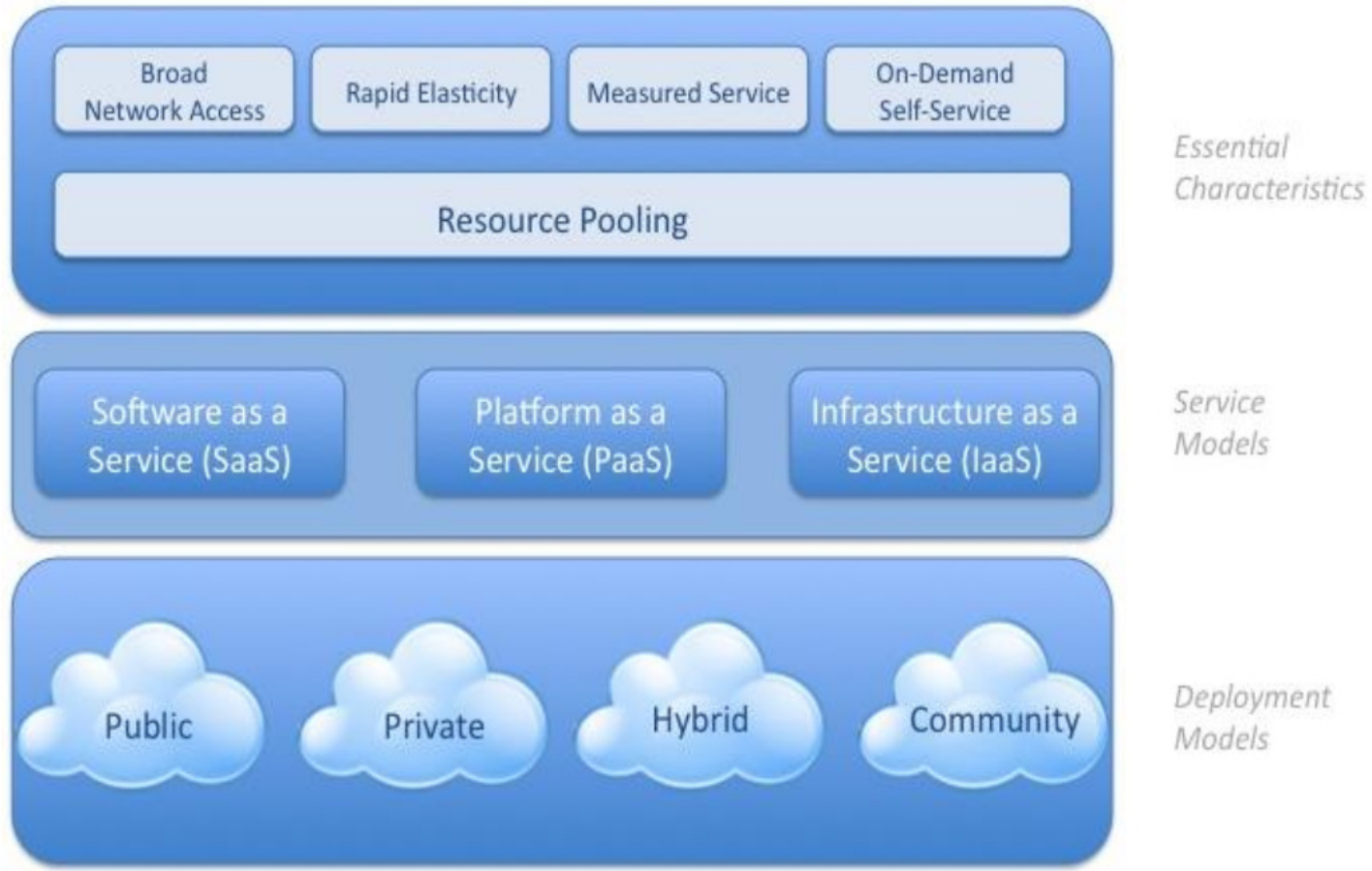
- Self Service Portal: Maar.. realiseer je de kracht van deze portal: positief als negatief.
- API
- Praktijkvoorbeeld: Laten we eens kijken bij de Azure Self Service Portal.

Cloud en terminologie

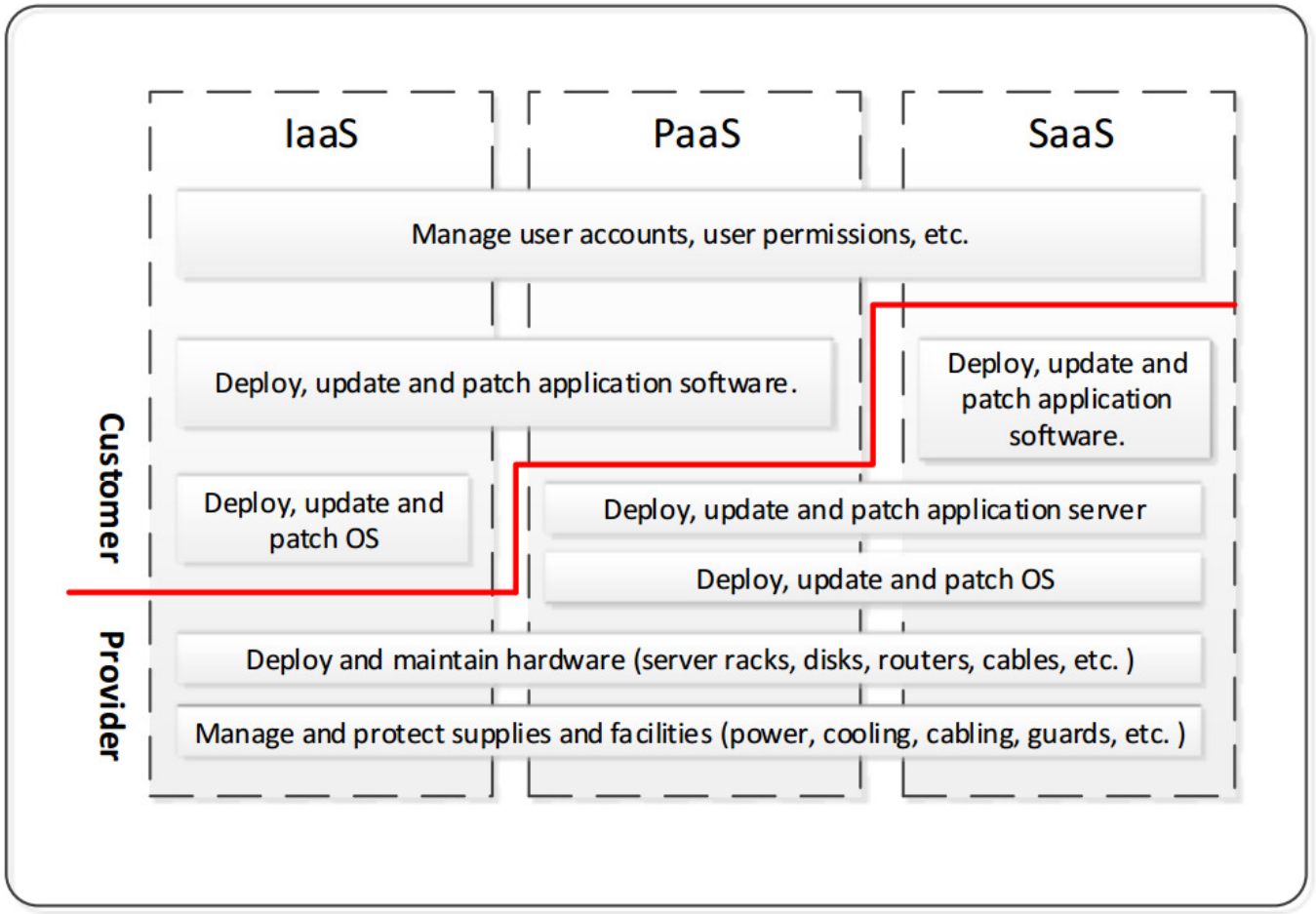
Cloud kent weer nieuwe woorden!

ORDINA

Cloud terminologie

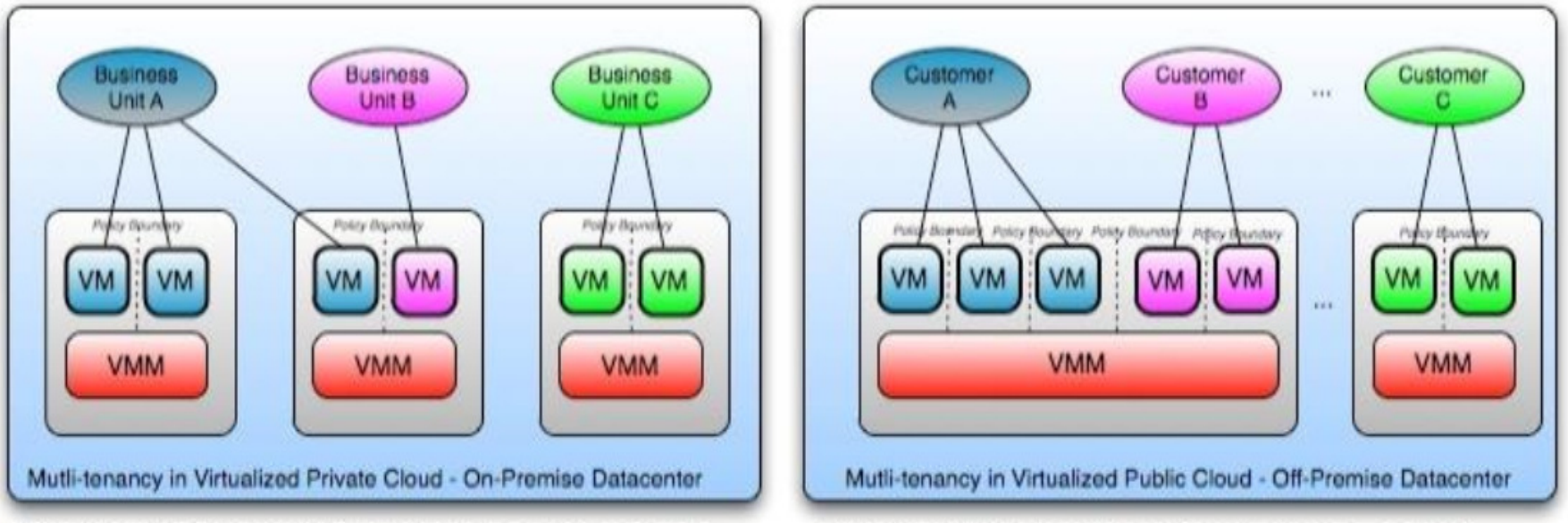


Cloud Service modellen en verantwoordelijkheden



Cloud deployment modellen

- Public
- Private
- Community b.v. Rijkscloud, Azure Government Cloud
- Hybrid



Hoe groot is de stap naar Cloud?

- Geen uitbesteding: Grote stap voor een organisatie.
- Vanaf traditionele hosting naar Cloud, mijn inziens geen hele grote stap.
- Maar… wel nieuwe risico's.
- Wie……

Risico’s

Specifiek voor de Cloud

ORDINA

Interactief – risico's specifiek voor Cloud

- Risico 1:
- Risico 2:
- Risico 3:
- Risico 4:
- Risico 5:

Risico's van Cloud computing volgens Enisa

Network and information security risks
R1: Software security vulnerabilities
R2: Network attacks
R3: Social engineering attacks
R4: Management GUI and API compromise
R5: Device theft/loss
R6: Physical hazards
R7: Overloads
R8: Unexpected costs
R9: Vendor lock-in
R10: Administrative or legal outages
R11: Foreign jurisdiction issues

Risico's van Cloud computing volgens Irmin

Network and information security risks
R1: Software security vulnerabilities
R2: Network attacks
R3: Social engineering attacks
R4: Management GUI and API compromise
R5: Device theft/loss
R6: Physical hazards
R7: Overloads
R8: Unexpected costs
R9: Vendor lock-in
R10: Administrative or legal outages
R11: Foreign jurisdiction issues

Welke maatregelen kun je nemen?

- Netwerk aanvallen:
  - Alleen de hoogst nodigde poorten open
  - Zelf testen of laten testen op reguliere basis
  - Gebruik IPS, Cloud bied standaard mogelijkheden

- Self Service Portal / Api aanvallen:
  - Kun je niet beïnvloeden, volledig afhankelijk van je provider
  - Hoe schermt je provider dit af?
  - Wat voor testen voeren ze uit?
  - Hoe beheersen ze hun code?
  - Etc.

Vervolg maatregelen

- Overbezetting, te weinig resources:
  - Ben je afhankelijk wederom van je Provider
  - Hoe voorkomen ze dergelijke bottlenecks?
- Vendor lock-in:
  - Strategie hoe je de Provider weer kunt verlaten
  - Hebben ze b.v. de mogelijkheid om disks met jou data aan te leveren?
  - Gebruiken ze standaard technologie of een exotische oplossing?
  - Hele grote partij vs. kleinere lokale Cloud leverancier
- Problemen met buitenlandse wetgeving:
  - Let goed op waar je de resources afneemt. Dit heb je volledig zelf in de hand

Informatiebronnen

Voor Cloud leveranciers selectie

ORDINA

Informatiebronnen

- Enisa
  - Tweetal uitgebreide risico analyses
- Cloud Security Alliance (CSA)
  - Initiator van framework voor Cloud Security
- Uitgebreide informatiebronnen voor:
  - Klanten
  - Auditors
  - Maar ook Cloud provider

Enisa

- Eu Organisatie promoot o.a. Cloud dienstverlening.

- Tweetal documenten:
  - Cloud computing security risk assessment – 2009
  - Cloud Security Guide for SME - 2015

- Deze documenten geven uitgebreid informatie:
  - Risico's
  - Kansen
  - Vragen die een onderneming kan stellen aan Cloud providers
  - Fictieve cases

Opzet cloud security guide

Security questions	Related opportunities	Related risks
SQ1: Organizational security, governance and risk management	O4, O5, O6, O11	R6
SQ2. Responsibilities and liabilities	O5, O10	R6
SQ3. Contingencies and backups	O1, O4, O5, O8	R5, R6, R7
SQ4. Legal and administrative issues	-	R10
SQ5. Human resources security	O4	R6
SQ6. Access Control	O4, O9	R6
SQ7. Software security	O6, O7	R1, R4
SQ8. User, management and application programming interfaces	O6, O7, O9	R3, R4, R5
SQ9. Monitoring and logging	O7	R4
SQ10. Interoperability and portability	O3	R6, R9
SQ11. Scaling, sizing and costs	O2	R7, R8
SQ12. Compliance with national/international legislation	-	R11

Cloud Security Alliance

Cloud Control Matrix

CCMv3.0.1 CLOUD CONTROLS MATRIX VERSION 3.0.1

Control Domain	CCM V3.0 Control ID	Updated Control Specification	Cloud Service Delivery Model Applicability			Supplier Relationship	
			SaaS	PaaS	IaaS	Service Provider	Tenant / Consumer
Application & Interface Security Application Security	AIS-01	Applications and programming interfaces (APIs) shall be designed, developed, deployed, and tested in accordance with leading industry standards (e.g., OWASP for web applications) and adhere to applicable legal, statutory, or regulatory compliance obligations.	X	X	X	X	
Application & Interface Security Customer Access Requirements	AIS-02	Prior to granting customers access to data, assets, and information systems, identified security, contractual, and regulatory requirements for customer access shall be addressed.	X	X	X	X	X

Domeinen Cloud Control Matrix

- Beveiliging van applicatie en interfaces.
- Audits.
- Business continuïteit.
- Wijzigingsbeheer.
- Beveiliging van data en Informatie life cycle management.
- Datacentra beveiliging (fysieke beveiliging).
- Encryptie.
- Governance en risk.
- Personeel.
- Identity en access management.
- Beveiliging van Infrastructuur en virtualisatie.
- Portability (vendor lock-in).
- Beveiliging van mobiele apparatuur.
- Security incident management.
- Supply Chain management.
- Management van kwetsbaarheden.

Consensus Assessments Initiative

CAIQv3.0.1 CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v3.0.1							
Control Domain	**Control ID**	**Question ID**	**Control Specification**	**Consensus Assessment Questions**	**Consensus Assessment Answers**		
					Yes	**No**	**Not Applicable**
Application & Interface Security *Application Security*	AIS-01	AIS-01.1	Applications and programming interfaces (APIs) shall be designed, developed, deployed, and tested in accordance with leading industry standards (e.g., OWASP for web applications) and adhere to applicable legal, statutory, or regulatory compliance obligations.	Do you use industry standards (Build Security in Maturity Model [BSIMM] benchmarks, Open Group ACS Trusted Technology Provider Framework, NIST, etc.) to build in security for your Systems/Software Development Lifecycle (SDLC)?			
		AIS-01.2		Do you use an automated source code analysis tool to detect security defects in code prior to production?			
		AIS-01.3		Do you use manual source-code analysis to detect security defects in code prior to production?			
		AIS-01.4		Do you verify that all of your software suppliers adhere to industry standards for Systems/Software Development Lifecycle (SDLC) security?			
		AIS-01.5		(SaaS only) Do you review your applications for security vulnerabilities and address any issues prior to deployment to production?			

Certificeringen

Welke zien we in de praktijk?

ORDINA

Certificeringen

- CSA was een voorloper met de Cloud certificering STAR.
- In Nederland zien we vooral vraag naar:
  - ISO27001
  - ISAE 3402 type 2
- En mogelijk raken deze in opkomst:
  - ISO27017
  - ISO27018
- Vraag: Wat zien jullie in de praktijk?

ISO27001

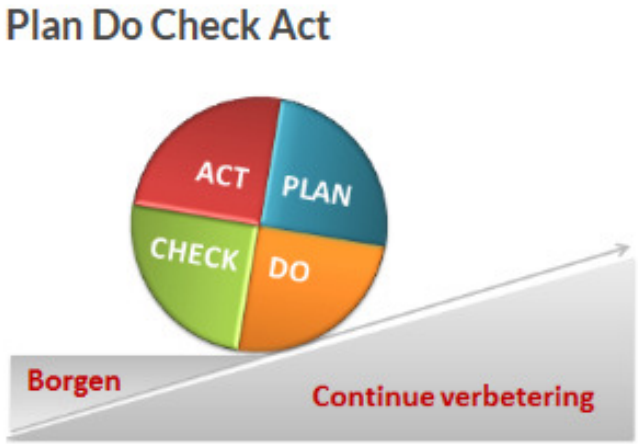
- Standaard norm voor informatiebeveiliging in Nederland.
  - BIR voor overheid
  - NEN7510 voor zorg
- Audit door een geaccrediteerde partij.
- ISMS.
- Begint een commodity te worden.
- Verschuiving naar ISAE 3402 zien wij in de markt.

ISMS

- Managementsysteem, continue proces.

- Input:
  - Resultaten van controles
  - Security incidenten
  - Audits

- Output:
  - Verbeteringen, aanpassingen
  - Nieuwe maatregelen



ISAE 3402

- Geen certificering maar een Assurance rapportage.

- Type 1 en 2.
- Beheers doelstelling, risico's en maatregelen: Effectiviteit van de maatregelen

- Hoe gaat een dergelijke audit in de praktijk?

ISO27017 en 27018

- Extra certificering boven op het ISO27001 certificaat.
- Extra maatregelen, uitbreiding op ISO27002.
- ISO27017: Cloud security (i.s.m. CSA)
  - Realisatie scheiding van virtuele omgevingen.
  - Hardenen van virtuele systemen.
  - Verantwoordelijkheden van beheerders Cloud omgeving.
- ISO27018: Data privacy in de Cloud
  - Waar bevindt zich de data van de klant.
  - Policy voor vernietigen van data.

Aanpak en vragen

Selectie Cloud dienstverlening

ORDINA

Aanpak

- Doe inspiratie op middels informatiebronnen en begrijp de materie.
- Voer je risico analyse uit.
- Stel beleid op b.v.
  - Welke data niet / wel naar de Cloud
  - Bij bepaalde classificatie encryptie toepassen
  - Voordat data naar de Cloud gaat impact analyse uitvoeren

- Bovenstaande drie stappen → pakket van eisen.
- Advies: Begin klein en doe ervaring op.

Service Level Agreement

- Right to audit?
  - Maar bedenk…..bij de grote partijen als Amazon en Azure daar stuur je geen auditor heen.
  - https://www.microsoft.com/en-us/trustcenter
- Afspraken omtrent het behouden van certificeringen.
- Inzage in certificeringen.

Vragen?

Mochten ze later te binnen schieten: irmin.houwerzijl@ordina.nl