

Digitale Soevereiniteit

+ open source software

By Marcel Kornegoor



Agenda

- Welkom!
- Wie ben ik?
- Over AT Computing
- Het IT-thema van 2026: Digitale soevereiniteit
- Vijf aspecten

About me

Marcel Kornegoor

Co-owner & director @ AT Computing

- 15 years of experience in IT.
- Huge fan of open source software.
- Likes to share knowledge.
- Co-founder of DOSBA.
- Husband, father, cyclist and nerd by night.

<https://dosba.nl>

<https://linkedin.com/in/mkornegoor>



AT Computing — Who We Are & What We Do

AT Computing is a **Dutch open-source IT consultancy and training company** that helps organizations design, implement, and manage reliable, automated IT environments.

What We Do

-  **Training & Education** — Hands-on courses in Linux, Ansible, Kubernetes, Python, and more.
-  **Consultancy** — Independent advice and support for open-source infrastructure and automation.
-  **Staffing & Expertise** — Experienced specialists available to strengthen IT teams.
-  **Custom Solutions** — Tailor-made training and implementation trajectories for specific needs.

Why Choose AT Computing?

- Deep expertise in **open-source technologies**.
- **Independent** — no vendor lock-in or sales agenda.
- Trusted partner since **1985**, known for quality and practical knowledge.

Proud member of:



Digitale Soevereinität

Definitie

Van Dale: *oppermachtige heerschappij*

Praktische betekenis

In hoeverre heb je controle over jouw digitale assets





Photo by Athena Sandrini



Ontwikkelingen

- Sancties tegen ICC (via Microsoft)
- Activeren van diplomaten (ambassadeurs) om tegen EU soevereiniteit te lobbyen
- Ook verregaande bedreiging in de eigen techsector: Anthropic vs DoD
- Overheidsinstanties blijven dienstverlening outsourcen...
- De Amerikaanse techsector ontplooit "soevereine" initiatieven
- Enorme beweging naar SaaS



Gewetensvragen

vraag je af...

- Kan ik er altijd bij?
- Kan iemand anders erbij?
- Kan ik altijd weg?
- Vervolg vraag: is dat erg?

Business Continuity Management

Risico management

Kans, Impact, Nabijheid

Heeft eigenlijk alles van doen met... 🥁

Exit strategie

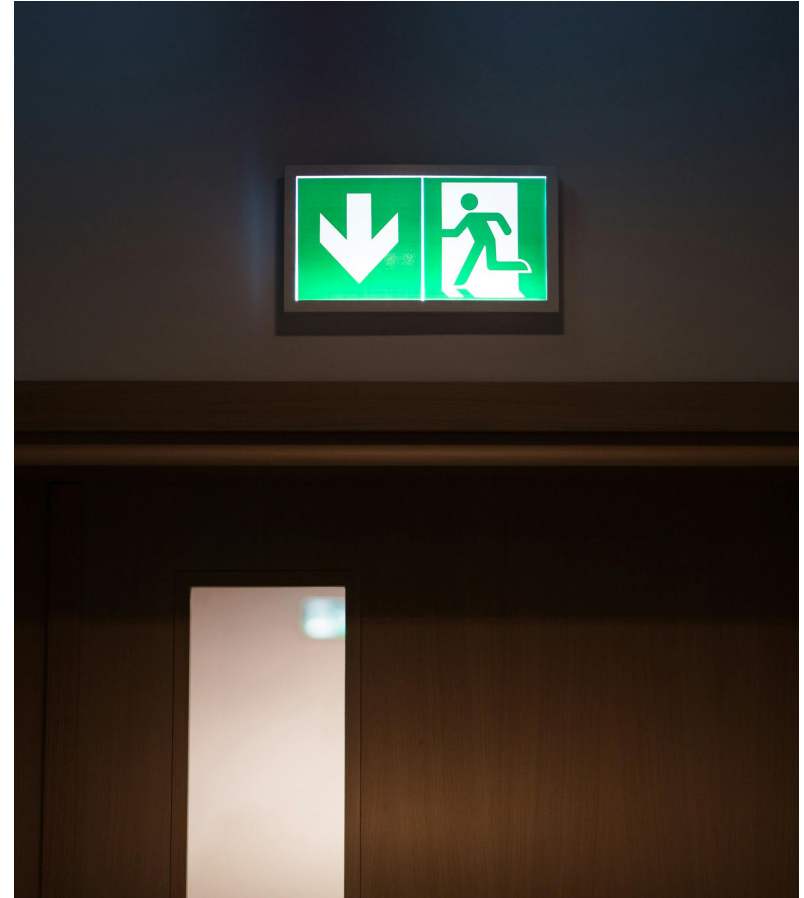
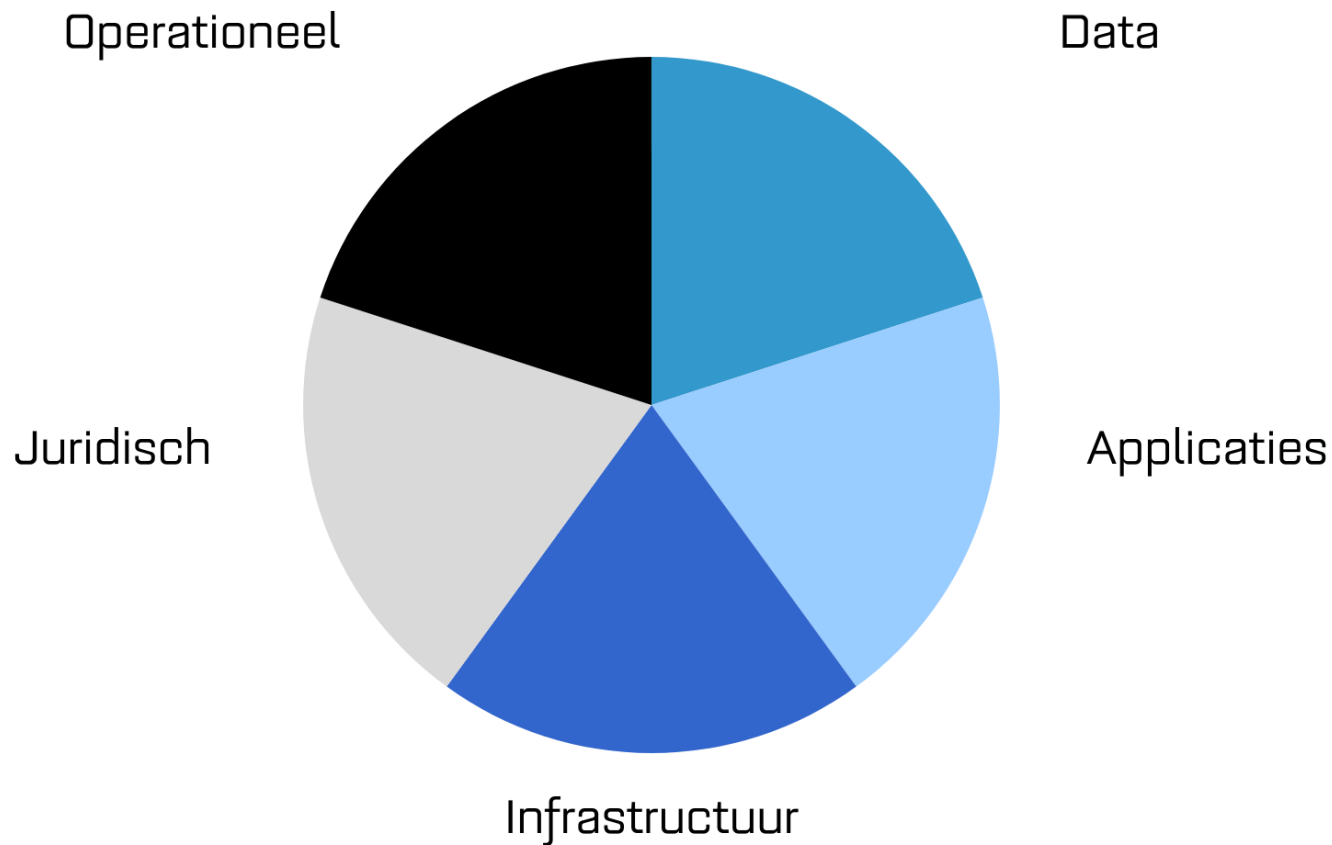


Photo by Jakub Zerdzicki

Vijf essentiële risicogebieden



Aanpak in dit webinar

Per risicogebied:

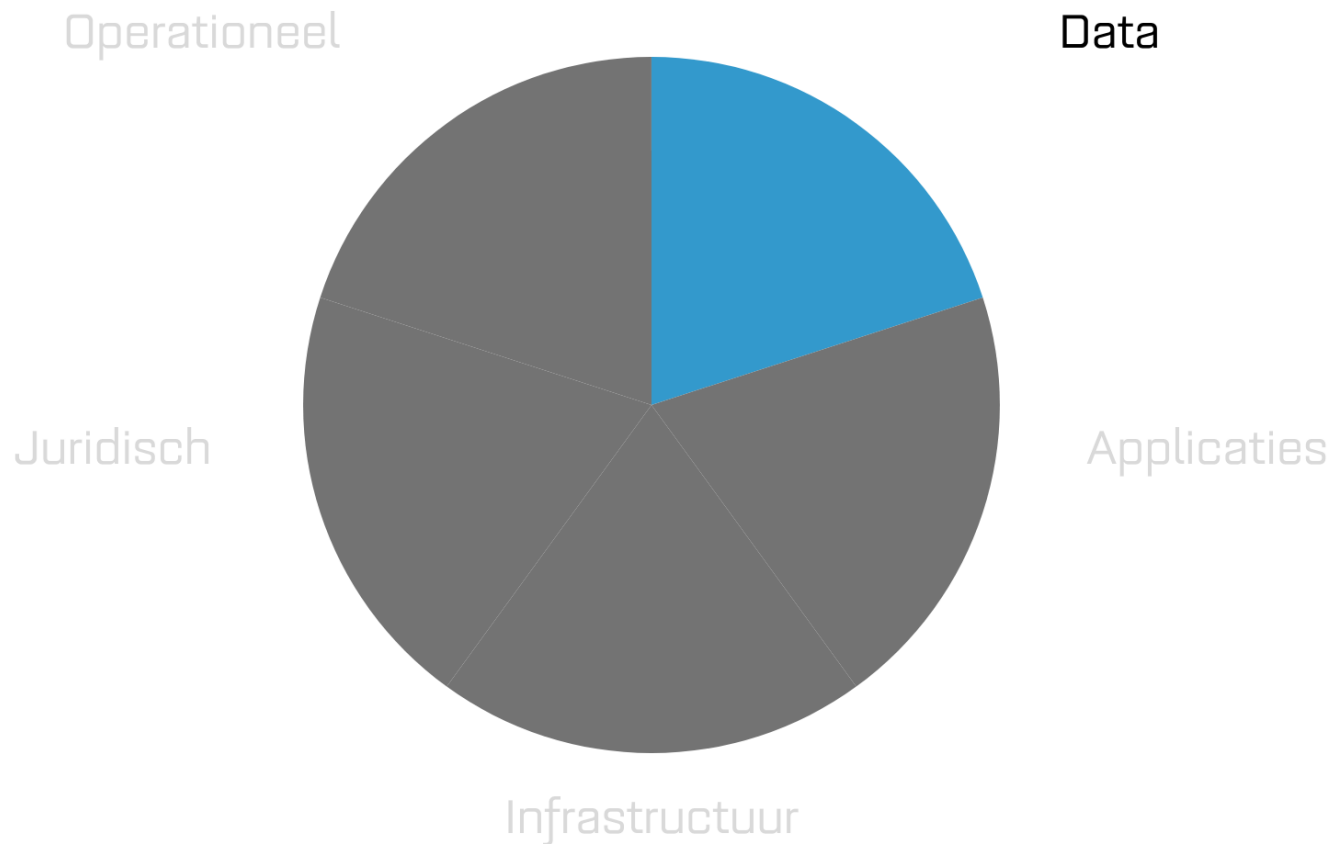
- welk(e) risico('s) loop je?
- welke beheersmaatregelen kun je treffen?

vrijwaring: dit is slechts een overzicht van een uurtje

iedere situatie is anders

er zijn nog meer risico's...

...en ook nog meer beheersmaatregelen



De risico's

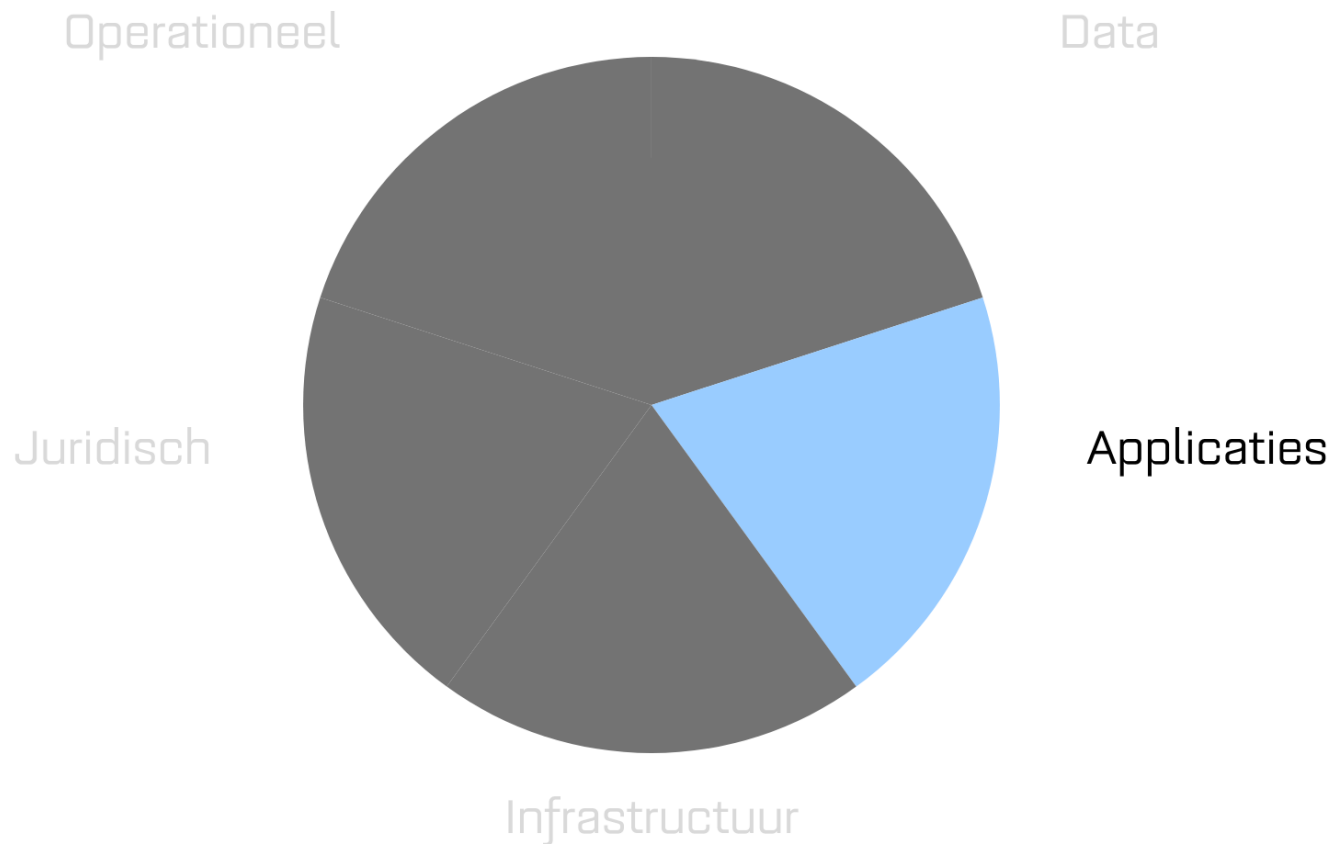
- Waar staat de data fysiek opgeslagen?
- Welke wetgeving is op de data van toepassing?
- Waar zijn de encryptiesleutels? (*at rest & in transit*)
- Wie kunnen er bij voor beheer?
- Wat kan/mag/doet een leverancier met de data? (AI-modellen trainen?)

De beheersmaatregelen

- Data classificatie -> (**opzet** (*beleid*), **bestaan** (*implementatie*), **werking** (*toetsing*))
- Juridische toetsing en terughoudendheid (ga van het slechtste uit)
- Zorg ervoor dat je altijd zelf grip op encryptie hebt (*customer managed keys*)
- Zorg altijd voor een back-up van belangrijke data op een plek waar je *wel* volledige controle hebt

Nuances

- Niet alle data is even spannend of belangrijk -> soms maakt het simpelweg geen biet uit
- Wees bewust van het verschil tussen *toegang* tot data en *inzien* van de data



De risico's

- Is het een zelf ontwikkelde of open source applicatie?
- Heb je toegang tot de broncode? (Stichting OpenCommit)
- Kun je de applicatie (eenvoudig) verhuizen?
- Gebruikt de applicatie open standaarden?
- Is er een API en is de API vrij toegankelijk?

Kernvraag

hoe vrij ben ik om met de applicatie te doen wat ik wil?

Cloud delivery models...

IaaS  -> PaaS  -> SaaS 

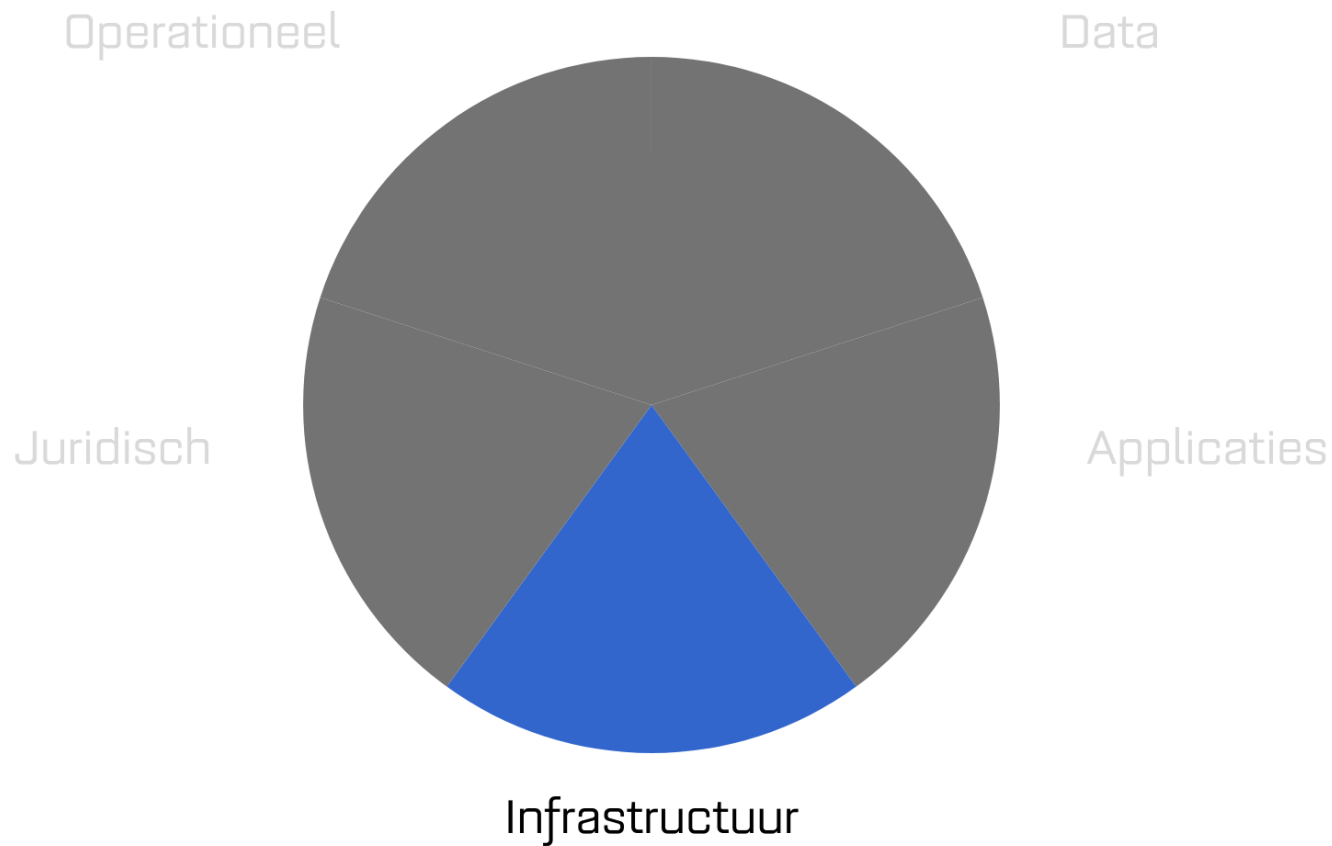
De beheersmaatregelen

- Gebruik zo min mogelijk SaaS
- Gebruik zoveel mogelijk open standaarden
- Zorg dat de API volledige import/export van data ondersteunt
- Gebruik open source software

Zonder toegang tot de
broncode is
soevereiniteit
onmogelijk



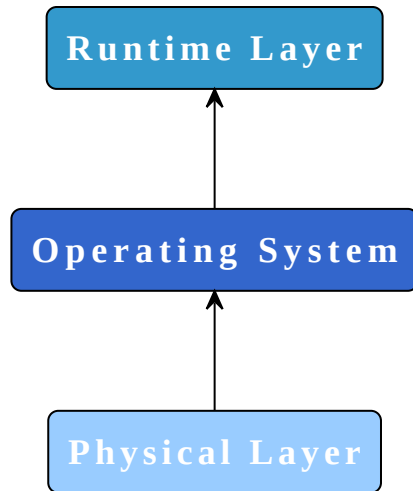
Photo by Zak H



Infrastructure

De risico's

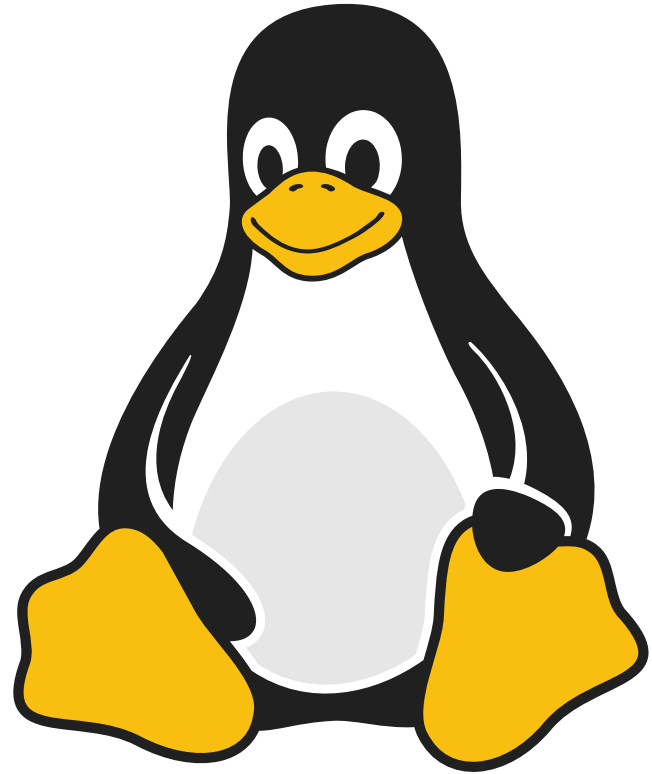
- Waar staat de fysieke infrastructuur?
- Wie heeft controle over de hardware?
- Wie heeft controle over encryptie? -> Trusted Platform Modules (TPM)
- Welk OS draai je?
- Welke runtime gebruik je?
- Zit er een 🇺🇸 Amerikaans moederbedrijf in de keten (US Cloud Act)

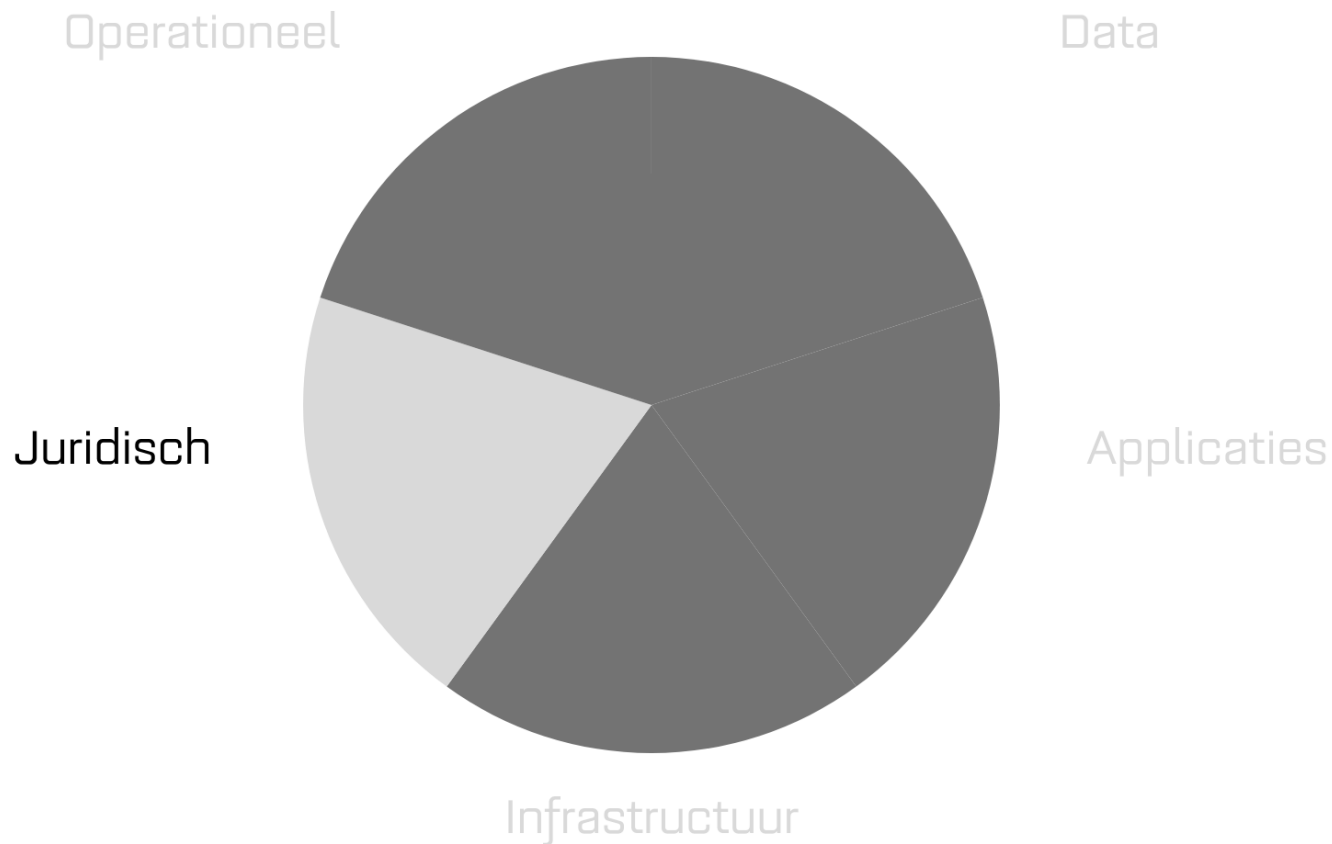


De beheersmaatregelen

- Gebruik zoveel mogelijk open standaarden
- Gebruik zoveel mogelijk open source software
- Zorg dat je eenvoudig van leverancier kunt wisselen
- Vitale infrastructuur

on-premises of  /  IaaS





De risico's

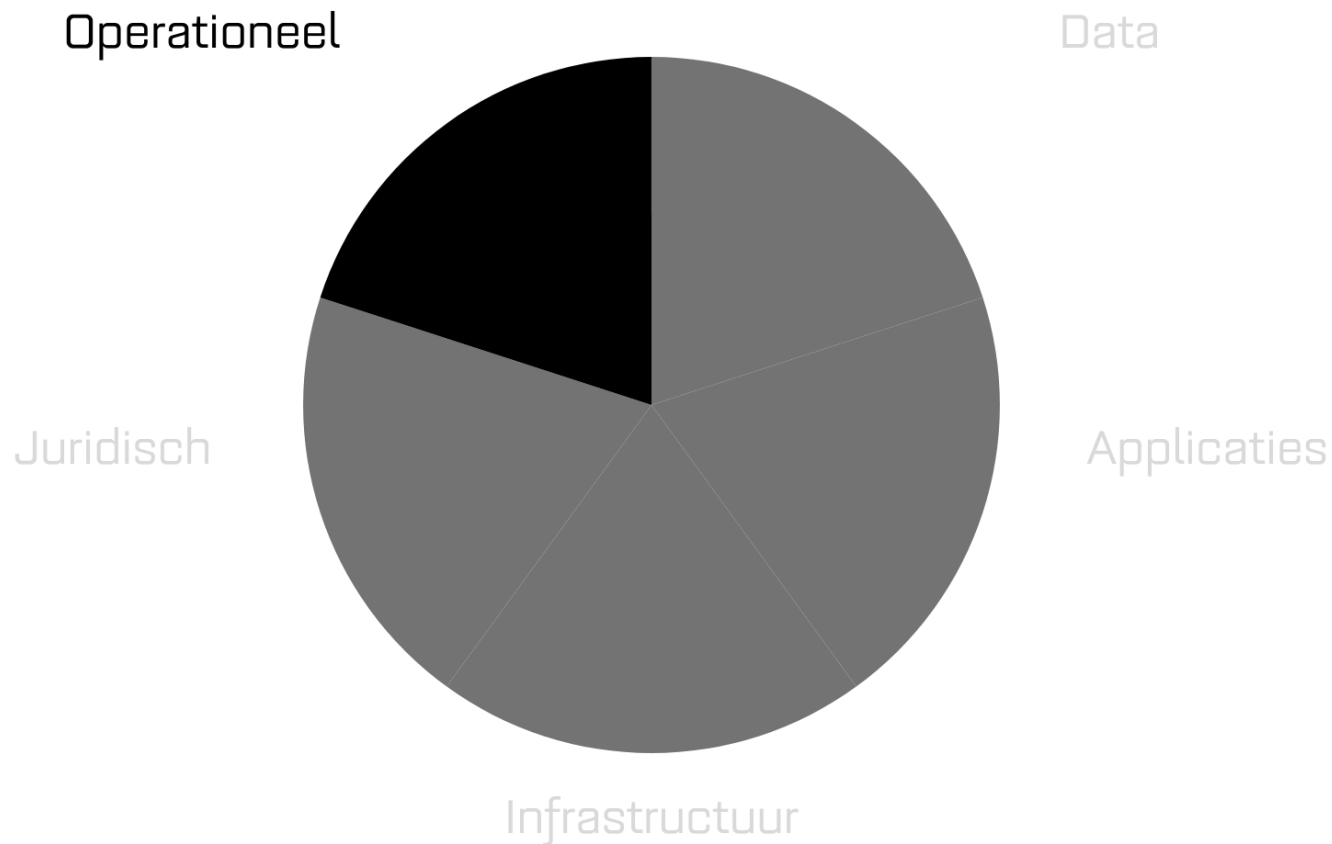
- Is er buitenlandse wetgeving van toepassing (*US Cloud Act*)?
- Wat staat er precies in de SLA (Service Level Agreement)?
- Welke verplichtingen heeft de leverancier richting (buitenlandse) overheden?
- Zijn er exit-clausules benoemd?
- Hoe transparant is de dienstverlener?

Wees alert!

Er wordt expres verwarring gezaaid en vaak zeer zorgvuldig geformuleerd...

De beheersmaatregelen

- Zorgvuldig lezen en sceptisch zijn: alles is een risico!
- Onderschat de *US Cloud Act* niet
- Due diligence: doe onderzoek naar (mogelijke) leveranciers
- Bepaal vooraf welke risico's je wilt:
 - Vermijden
 - Verplaatsen/verzekeren
 - Verdragen
 - Verkleinen



De risico's

- Leverancier wordt overgenomen (Solvinity)
- Leverancier gaat failliet
- Leverancier past eenzijdig voorwaarden aan (HashiCorp / Microsoft)
- Toegang tot kennis of documentatie wordt beperkt

De beheersmaatregelen

- Wederom: exit strategie!
- Zorg voor een *back-up*: niet op 1 paard wedden 🐎
- Ook hier: gebruik waar mogelijk open source software
 - Je kunt *forken* als onderdeel van je exit strategie
 - Je kunt onderhoud/beheer overdragen aan een andere partij

Open source software geeft je *right to repair*:
gesloten software niet.

Checklist IT-soevereiniteit

<https://atcomputing.nl/checklist>

Uniek in 2026: direct te downloaden zonder gegevens achter te laten!

<https://atcomputing.nl/soeverein>



CHECKLIST IT-SOEVEREINITEIT

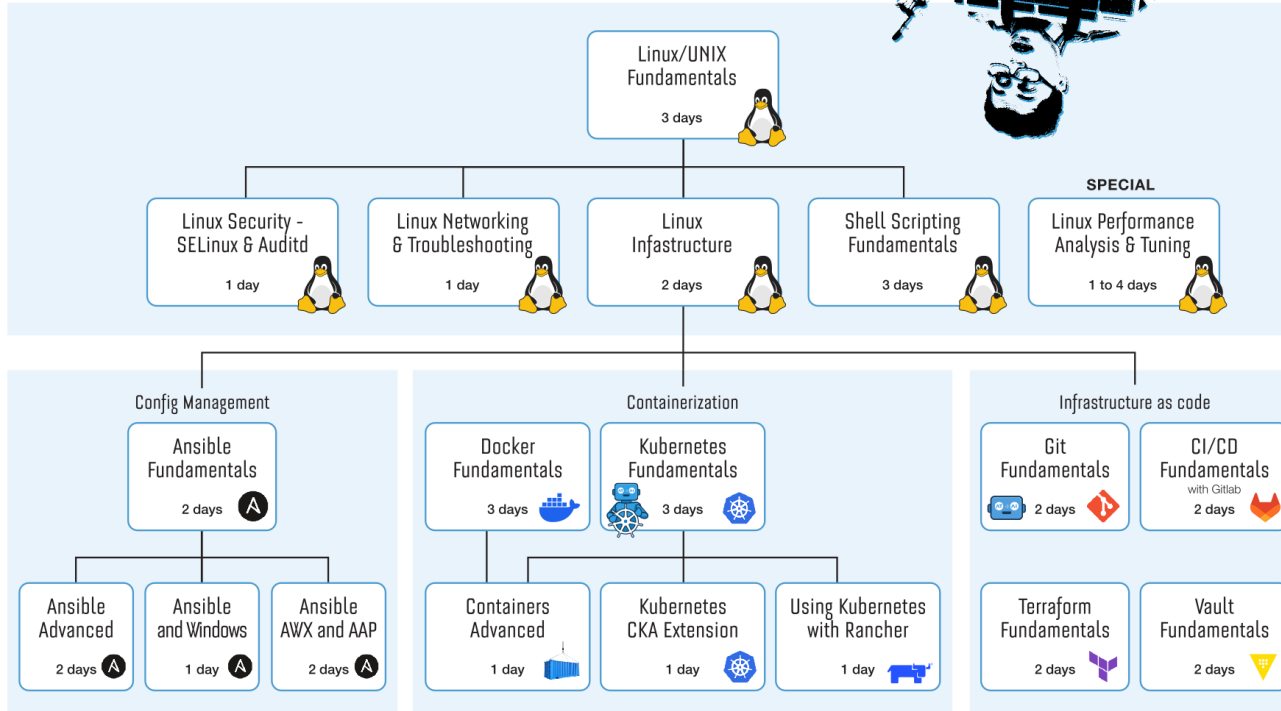
Inventariseer de (on)afhankelijkheid van jouw IT-landschap

ATYPICAL OPEN SOURCE LEARNING JOURNEY

for Cloud Engineers, DevOps Engineers & SysAdmins



Linux



 This training uses AI.

ATYPICAL OPEN SOURCE LEARNING JOURNEY

for Generative AI



Core GenAI

 **GenAI for DevOps - Build Your Own LLM Server**
1 day

 **GenerativeAI & Security**
1 day

Vibe Coding
1/2 day

Python Programming

For writing your own Gen AI / LLM powered apps or solutions.

Learn to Program with Python
5 days

Deep Learning with Pytorch
2 days

Create a REST API in Python with FastAPI
2 days

Python for Data Analysis - Introduction to PANDAS
2 days

Platform & Containerization

For running your own LLM or GenAI apps.

Kubernetes Fundamentals
3 days

Linux/UNIX Fundamentals
3 days

Terraform Fundamentals
2 days

Shell Scripting Fundamentals
3 days

Docker Fundamentals
3 days

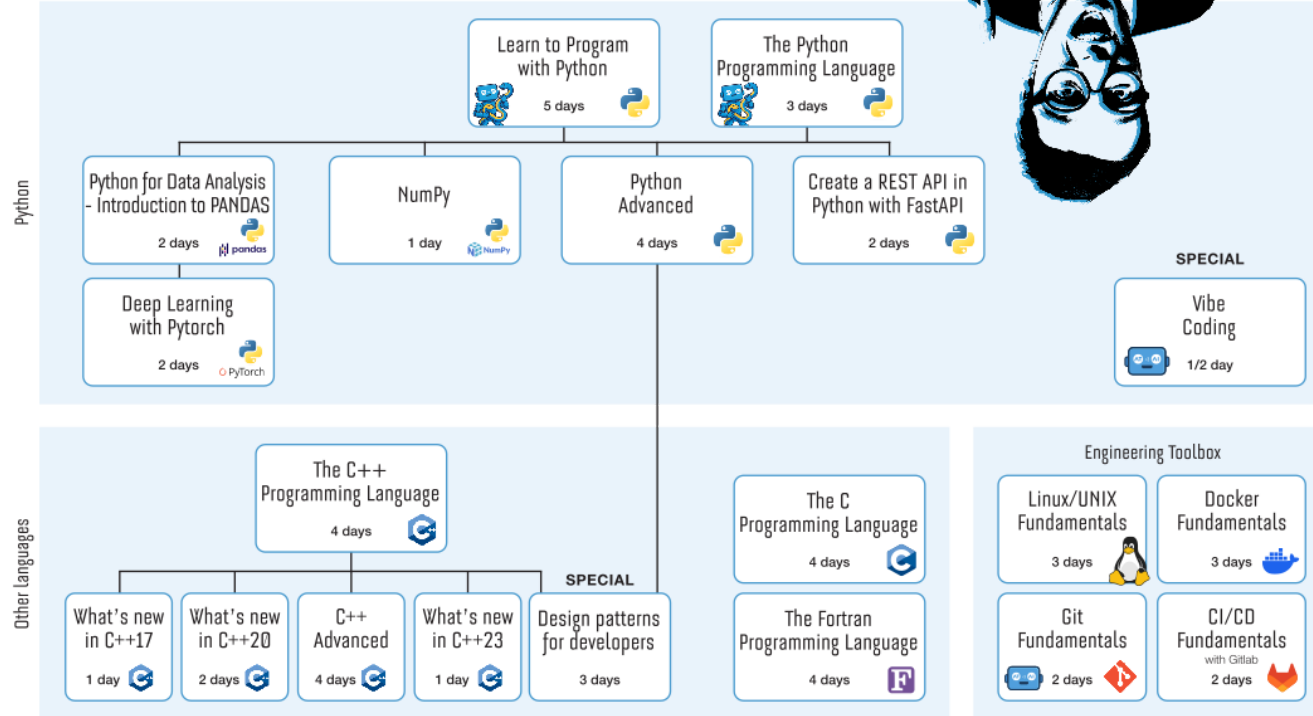
Git Fundamentals
2 days

CI/CD Fundamentals
with Gitlab
2 days

 This training uses AI.

ATYPICAL OPEN SOURCE LEARNING JOURNEY

for Software Engineers



 This training uses AI.

<https://atcomputing.nl/leerpaden>

Thank You!

Questions?

<https://atcomputing.nl>

marcel@atcomputing.nl