

The rocky road to Dublin

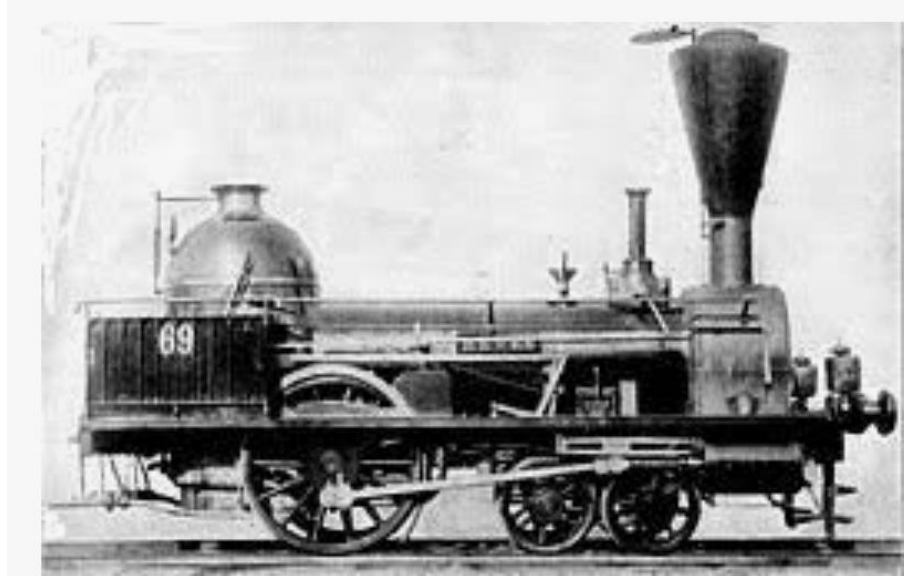
**avagy egy nagybank kalandozásai
a publikus felhő világában**

"Then off to reap the corn, leave where I was born
Cut a stout blackthorn to banish ghosts and goblins
A brand new pair of brogues, rattlin' o'er the bogs
Frightenin' all the dogs on the rocky road to Dublin."

Irish folk song

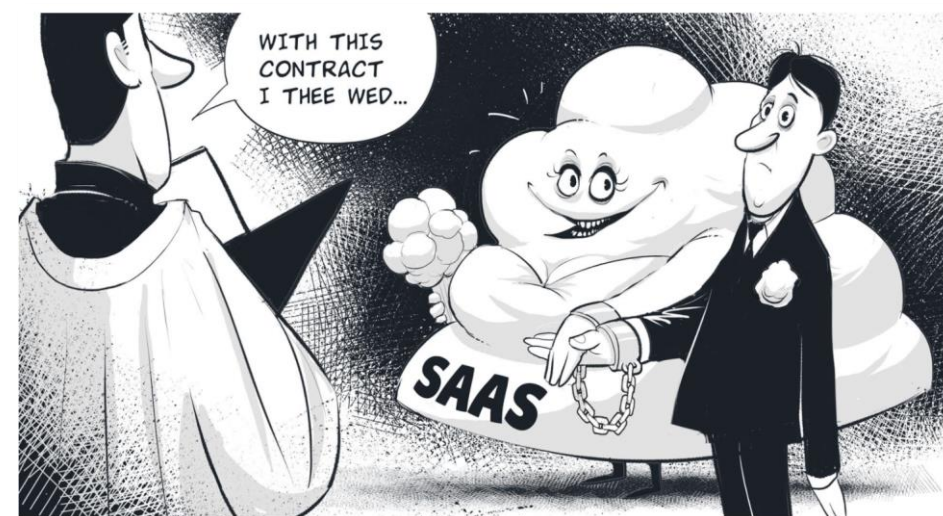
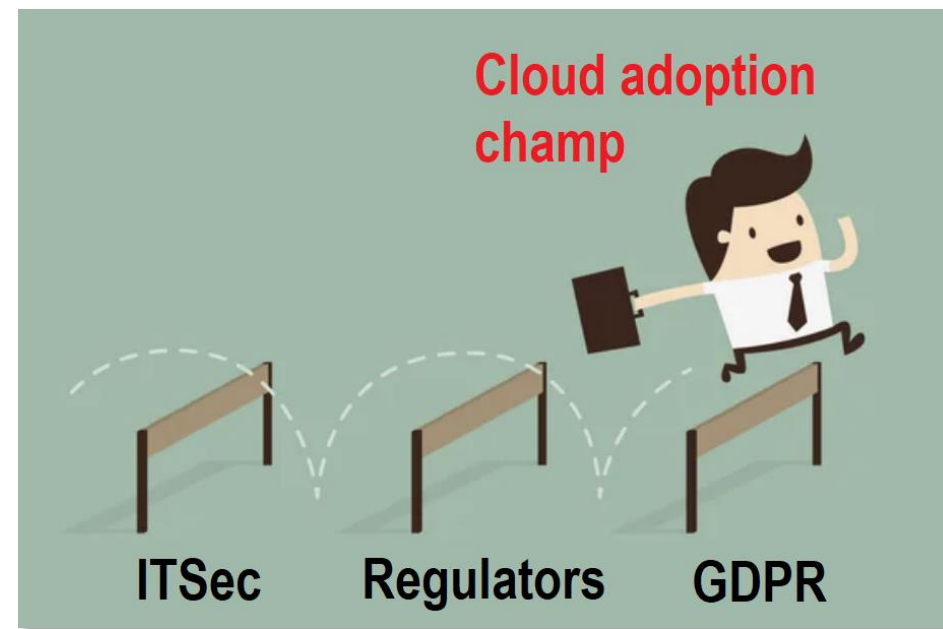
C. & P. photography

A miért

- Egy új, a bankban **még nem létező képesség** kiépítése – a.k.a. „need for speed”
 - **A világon keletkező IT innováció** zöme a CSP*-knél jelenik meg a piacon – ehhez itt lehet hozzáférni
 - **Kísérletezés** – egy on prem HW igény a jóváhagyástól az átadásig több hónapot vesz igénybe, egy cloud sandbox pár napot. (a CSP szempontjából pár percet.)
- 
- **„A gőzmozdony effektus”** – az on-prem adatközpontok hatékonysága kb. 20%, de 100%-ot fizetsz ki.
 - **Skálázhatóság** – oldalra, nem felfelé! (már ha az alkalmazás réteg képes rá.)
 - **NEM a költséghatékonyság** az elsődleges cél, de a költségek láthatóvá tétele egy klassz melléktermék.
 - **A végső ok:** a számítástechnikai infrastruktúra „utility”-vé válása elkerülhetetlen, ne ide tegyük a tétet.

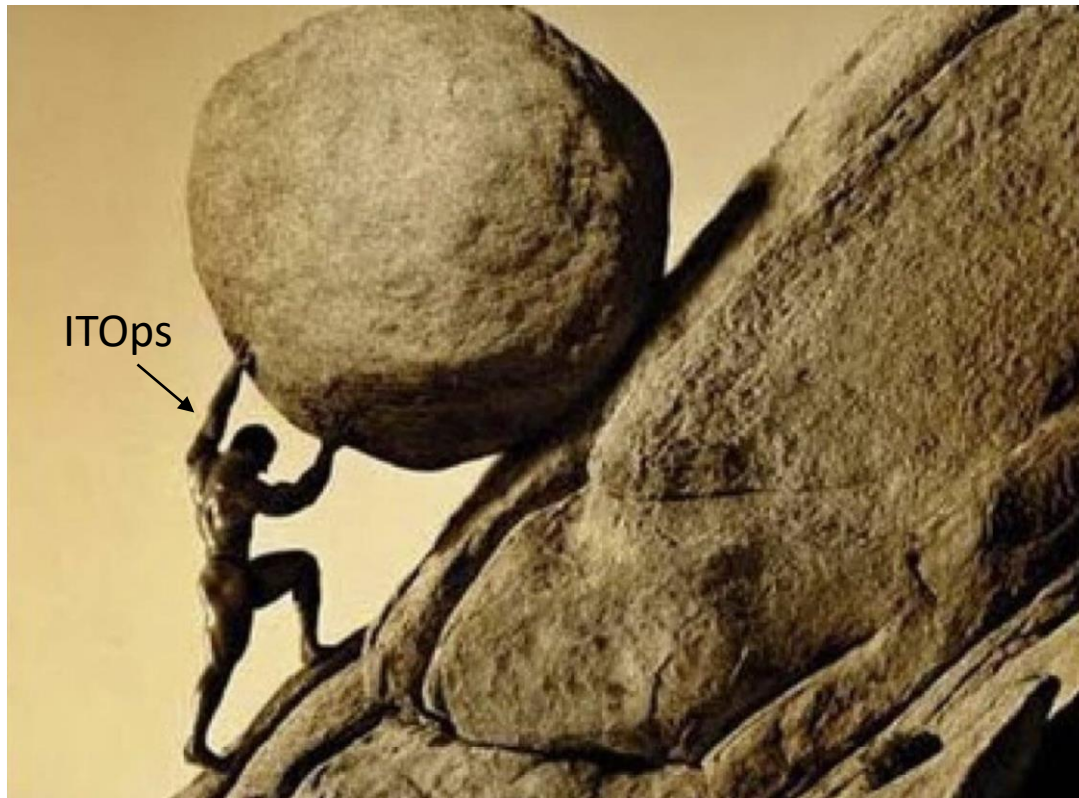
A miért ne

- A szabályzói előírásoknak való megfelelés – van belőle néhány.
- Az ITSec kockázatok: az on-prem adatközpont védelme az internetről érkező támadás ellen („a legjobb tűzfal a két centis légrés.”)
- A szállítói kitettség – túlárazza a portékáját, netán tönkremegy szegény vagy odaadja az adatainkat valaki másnak.
- A CSP is hibázhat: szolgáltatás kiesés, adatvesztés.
- Lehet, hogy nem is ő a tuti: egy másik CSP több innovációt hoz... (akkor vegyek kettőt?)
- Egy IaaS-ről még csak-csak leszállunk, no de egy SaaS-ről hogyan?
- És kafa monopóliumommal most mi lesz?!
- Ez a változás az üzleti folyamatok újragondolását is igényli, a technológia - szokás szerint – csak enabler. És ha az üzletnek erre most nincs ideje?



<https://www.loadbalancer.org/blog/vendor-lock-in-sucks-how-do-i-leave-my-cloud-software-provider/>

A nyilvános felhő megítélése nem egységes



<https://www.davelabowitz.com/blog/sisyphus-and-leadership/>

IT Ops: Van egy tök jó on prem infránk, használjátok azt. Majd mi eldöntjük, hogy mit hová rakjunk, ez a szakterületünk. BTW: már a fülemen is lóg egy lámpás, **gyertek vissza később.**



Eugène Delacroix - a Szabadság vezeti a népet

https://en.wikipedia.org/wiki/La_Marseillaise

A fejlesztők: „Előre ország népe, harcra, ma diadal vár, hív hazánk!” a fejlesztői lélek végre megszabadul az infrastruktúra test összes nyűgjétől! **Felhőt akarunk MOST!**

A Tizedes meg a többiek



[A tizedes, meg a többiek](#)

Az oroszok már a spájzban vannak... Itt az ideje megszámolni őket: lehet, hogy kell egy CASB?



Cloud Access Security Broker

<https://securevoy.com/cloud-access-security-broker-casb/>

Az igazi probléma - Ez nem egyetlen projekt, hanem az egész IT átalakítása.

- A felhőben lévő infratraktúra szabályzása – **mit szabad és mit nem** aka. Landing Zone létrehozása - ok, ezt tudtuk
- Az on prem és a felhő címtárak összekötése – ezt sejtettük (de hány domain-ünk is van?)
- Az autentikáció: Do you speak SAML 2.0, oAuth2? – hagyjatok békén, most funkciót reszelek!
- A meglévő CI/CD folyamat (és eszközpark) szinkronba hozatala a felhőbeli párjával
- A CSP saját K8S megoldása vs. OpenShift – A hegylakó dilemma: There can be only one!
- Nem minden backend szolgáltatás tehető ki a felhőbe. A kapcsolódás dev. feladat.



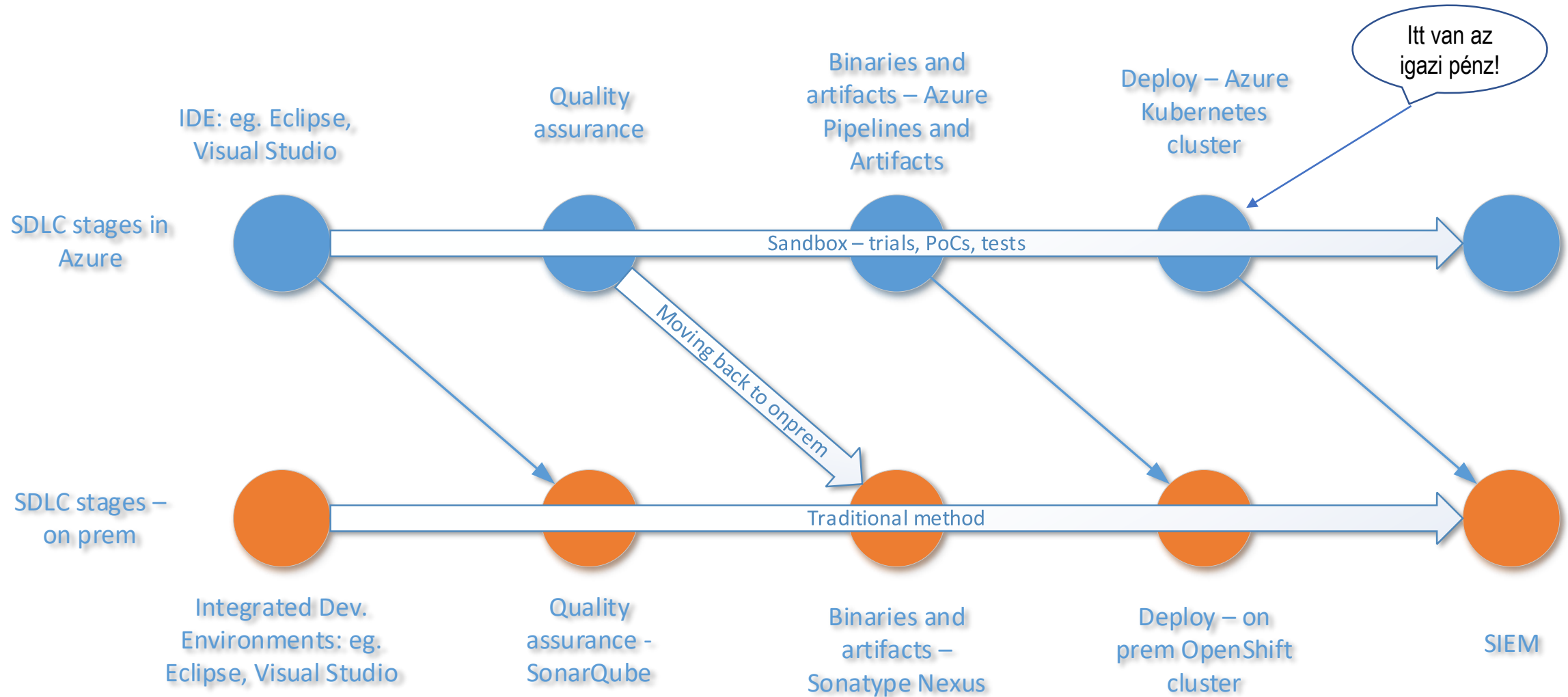
Edvard Munch:
Az ismeretlen fejlesztő sikolya

- Amikor a fejlesztő rájön, hogy a homokozójából nem éri el az on-prem rendszereket és adatokat...
- **Az interface-ek:** hogyan kössünk össze egy on-prem message queue-t a felhőbeli párjával?
- **A visszatérés:** ha tuti on-prem kell futtatnod az éles kódot vagy tárolnod az adatot (amikor a fejlesztő megint rájön)
- Az infra már tud oldalra skálázódni, mi a helyzet az alkalmazás réteggel? (milyen microservice?! „Adjál egy nagyobb vasat, de izibe!”)

A projekttel szembeni hozzáállás, amikor rájönnek, hogy mindenhez hozzá kell nyúlni:

„Milyen vércsoport lenni gringó egérkének?” /Macskafogó/

A „visszatérés” problémája: melyik ponton?



Az éles környezet meghatározásakor a kockázatarányosság elvét nem szabad figyelmen kívül hagyni.

Egy szó az IT Sec aggodalmakról

Azure compliance documentation and compliance offerings -
<https://www.azureguru.org/azure-compliance-documentation/>

Global	☒ ISO 27001:2013	☒ ISO 22301:2012	☒ SOC 1 Type 2	☒ CSA STAR Certification
	☒ ISO 27017:2015	☒ ISO 9001:2015	☒ SOC 2 Type 2	☒ CSA STAR Attestation
	☒ ISO 27018:2014	☒ ISO 20000-1:2011	☒ SOC 3	☒ CSA STAR Self-Assessment
US Gov	☒ FedRAMP High	☒ DFARS	☒ DoE 10 CFR Part 810	☒ FIPS 140-2
	☒ FedRAMP Moderate	☒ DoD DISA SRG Level 5	☒ NIST SP 800-171	☒ ITAR
	☒ EAR	☒ DoD DISA SRG Level 4	☒ NIST CSF	☒ CJIS
Industry	☒ PCI DSS Level 1	☒ DoD DISA SRG Level 2	☒ Section 508 VPATs	☒ IRS 1075
	☒ GLBA	☒ FCA (UK)	☒ 21 CFR Part 11 (GxP)	☒ CDSA
	☒ FFIEC	☒ MAS + ABS (Singapore)	☒ MARS-E	☒ MPAA
Regional	☒ Shared Assessments	☒ 23 NYCRR 500	☒ NHS IG Toolkit (UK)	☒ DPP (UK)
	☒ FISC (Japan)	☒ HIPAA BAA	☒ NEN 7510:2011 (Netherlands)	☒ FACT (UK)
	☒ APRA (Australia)	☒ HITRUST	☒ FERPA	☒ SOX
	☒ Argentina PDPA	☒ China TRUCS / CCCPPF	☒ Germany IT-Grundschutz	☒ Singapore MTCS Level 3
	☒ Australia IRAP Unclassified	☒ EN 301 549	☒ India MeitY	☒ Spain ENS
	☒ Australia IRAP PROTECTED	☒ EU ENISA IAF	☒ Japan CS Mark Gold	☒ Spain DPA
	☒ Canada Privacy Laws	☒ EU Model Clauses	☒ Japan My Number Act	☒ UK Cyber Essentials Plus
	☒ China GB 18030:2005	☒ EU – US Privacy Shield	☒ Netherlands BIR 2012	☒ UK G-Cloud
	☒ China DJCP (MLPS) Level 3	☒ Germany C5	☒ New Zealand Gov CC	☒ UK PASF

A felhővel kapcsolatos ITSec problémáink jelentős része várhatóan a saját felkészületlenségünkől ill. tévedéseinkből adódik majd, nem pedig a felhőszolgáltatók hibájából. *(feltéve hogy a sok bal oldali plecsni igaz és a telkók sem tréfálnak meg.)*

A cloud-ra fel kell készülnünk, „cloud-ready-vé kell válnunk.

Futjuk a maratont... egy kicsit más feltételekkel



<https://edition.cnn.com/videos/world/2012/05/28/pkg-anderson-marathon-man.cnn>



<http://vicces-kepek.blogspot.com/2010/07/mumus.html>

- Szolgáltatáskihelyezés
- Data residency
- Exit plan

<https://www.rmb.hu/letoltes/7-2020-kulso-szolgaltato-igenybevetele.pdf>

[4-2019-felho.pdf \(rmb.hu\)](https://www.rmb.hu/letoltes/4-2019-felho.pdf)

<https://www.rmb.hu/letoltes/4-2019-felho.pdf>

https://www.efb.eu/wp-content/uploads/2020/06/EEF-Cloud-Banking-Forum_The-use-of-cloud-computing-by-financial-institutions.pdf

<https://www.eba.europa.eu/regulation-and-policy/internal-governance/recommendations-on-outsourcing-to-cloud-service-providers>

A hét (felhő) főbűn

1. A nyilvános felhő bevezetését egy közösen elfogadott cél és átgondolt irányítás (governance) nélkül nyomni – a kupi a felhőben is kupi.
2. A szabadság illúzióját túl komolyan venni. Lásd az [MNB 4/2019 –es ajánlását](#):
„A királynét megölni nem kell félnetek jó lesz ha mindenki egyetért én nem ellenzem”
3. Ráerőltetni a meglévő on-prem menedzsment és tooling eszközparkot a felhőben épülő infrastruktúrára.
4. Ragaszkodni a meglévő szervezeti felépítéshez - amikor x főosztály integrál valamit, ami már összerakott valaki más. (1 VM = x SNOW jegy) - lásd Conway törvénye. https://en.wikipedia.org/wiki/Conway%27s_law
5. A meglévő on-prem alkalmazásokat „as is” átmigrálni a felhőbe – Lehet, de minek?
6. Az ITSec kockázatokat figyelmen kívül hagyni: Egy felhőben lévő virtuális gép semmivel nem több, mint egy védelem nélküli szerver az internetre kötve, csak egy másik helyrajzi számon. a Titanic kapitányát idézve: *„Full speed a head and fuck the icebergs!”* (from the Famous last words collection...)
7. A régi ITSec mentalitás fenntartása: *„Mi majd mindent jól megvizsgálunk”* – pl. video traffic backhauling for on prem inspection.... Hoppá, ez nem fér át a csövön! (vagy a logok visszahozatala a DC-be vs. egress traffic charges)

A munka dimenziói

A munkatársak és a felsővezetés gondolkodás módja	Az alkalmazás réteg - hogyan fejlesszünk oldalra skálázódni képes, cloud native megoldásokat	Governance – a cloud önmagában nem mindenre gyógyír
	A CI/CD pipeline újragondolása	A szervezetnek is változnia kell
A munkatársak ismeretei	Tooling – Infrastructure as a Code (amikor az infrát létrehozó script is megy a source repo-ba)	Az ITSec kockázatok valódi megértése és helyén való kezelése - az interface-ek kulcs szerepe
	Networking – ez nem csupán plusz egy VPN a cloud felé	Compliance – az összes elvárásnak megfelelni és közben még alkotni is

Cloud architect



<https://cloudarchitectmusings.com/2016/02/08/between-a-rock-and-a-hard-place-will-openstack-become-niche/>

Zárszó



A nagy hajóknak nagy a fordulási sugara – ez a folyamat éveket fog igénybe venni.



De időnként a nagy hajóknak is fordulniuk kell. Most ezen idők egyikét éljük.

Ha van kedved e nagy hajó kormányzásában részt venni, csatlakozz hozzánk!

Felelősség kizárási nyilatkozat:

Az előadó nézetei nem feltétlenül tükrözik az OTP Bank Nyrt. véleményét, az előadás teljes anyagának vagy részletének OTP Bank Nyrt.-n kívül történő felhasználása csak az előadó (és adott esetben a kommunikációért felelős banki szervezeti egység) engedélyével lehetséges.