# ANALÝZA RIZIK CLOUDOVÉHO ŘEŠENÍ Z POHLEDU UŽIVATELE

Václav Žid

# Osnova příspěvku

- Proč cloud computing?
- Pro jaké služby jsme cloud zvažovali?
- Jaká je podpora cloudu v USA, EU a v ČR?
- Výzvy
- Možnosti hodnocení bezpečnosti cloudu
- Závěrem

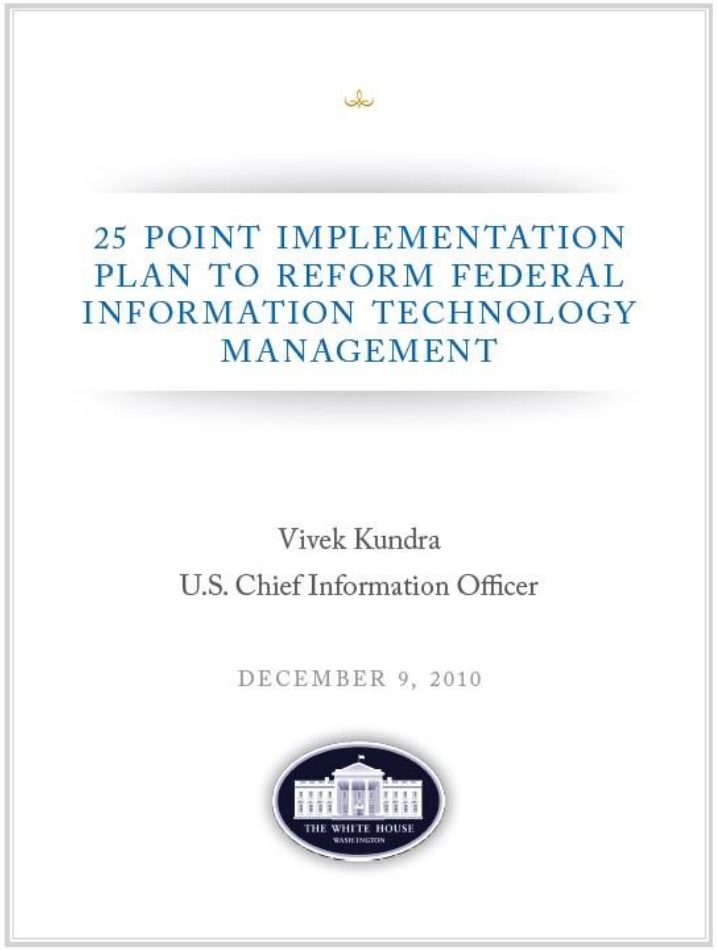
# Proč cloud computing?

- Ekonomická situace a rozpočtová opatření
- Snižování celkových nákladů na ICT
- Snižování počtu pracovníků v ICT
- Infrastruktura na konci životního cyklu
- Reforma ICT
- Zachování nebo zvyšování kvality služeb
- Budování bezpečnějšího ICT
- Požadavky uživatelů
- ICT musí být pružné a musí se přizpůsobovat měnícím se požadavkům
- Všichni o cloudu mluví, každý jej chce, cloud umí všechno…

# Pro jaké aplikace jsme cloud zvažovali?

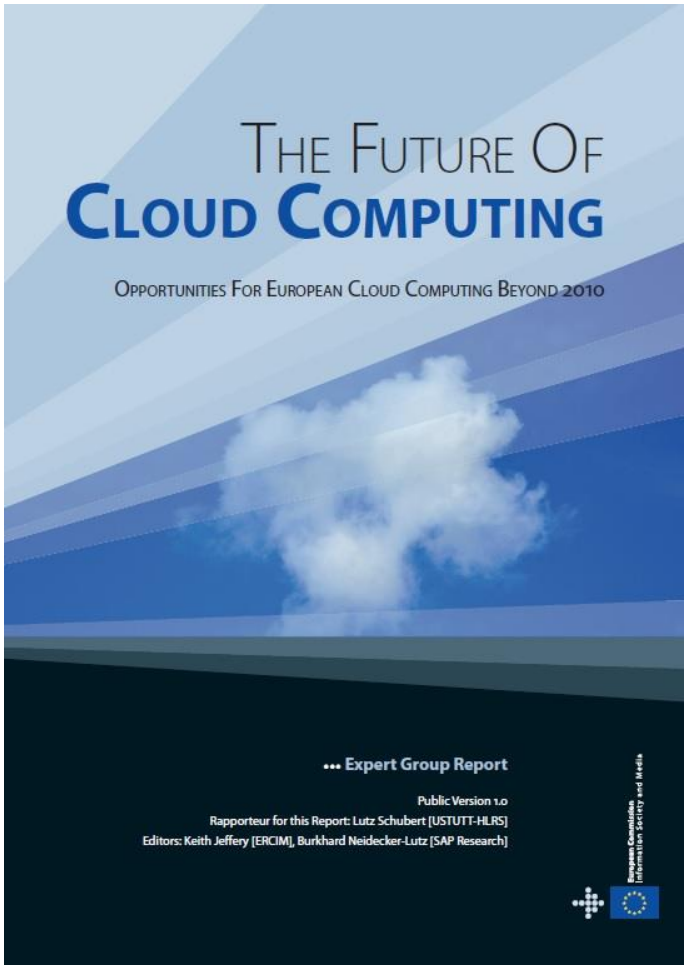
- Pro aplikace, které potřebujeme mít přístupné přes Internet pro většinu uživatelů
- Pro aplikace, které nakládají s běžnými necitlivými informacemi
- Pro standardní nebo standardizované aplikace, které lze jednoduše nastavovat
- Pro aplikace, které lze ovládat přes webový prohlížeč
- Pro aplikace, kde mi nevadí, že přicházím o správu a kontrolu nastavení

# Jaká je situace v USA, EU a v ČR?




- Přijmutí politiky „Cloud First“
  - Využití komerčních cloud technologií tam, kde je to možné
  - Spuštění privátních vládních cloudů
- Výhody:
  - Ekonomické
  - Flexibilita
  - Rychlost
- Katalog služeb

# Jaká je situace v USA, EU a v ČR?




- EC by měla stimulovat výzkum a vývoj v oblasti cloud computing
- EC by spolu s členskými státy měla nastavit regulační rámec
- Výhody:
  - Elasticita, Agilita, QoS
  - Pay per use, ROI

# Jaká je situace v USA, EU a v ČR?

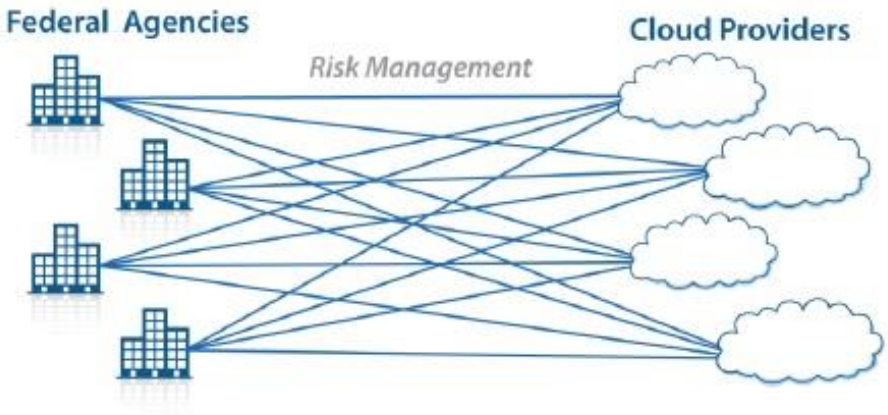

- MV představilo Klaudii symbolizující prostředky cloud computing
- Privátní cloud veřejné správy
- Přechod k modelu poskytování a odebírání služeb

# Výzvy

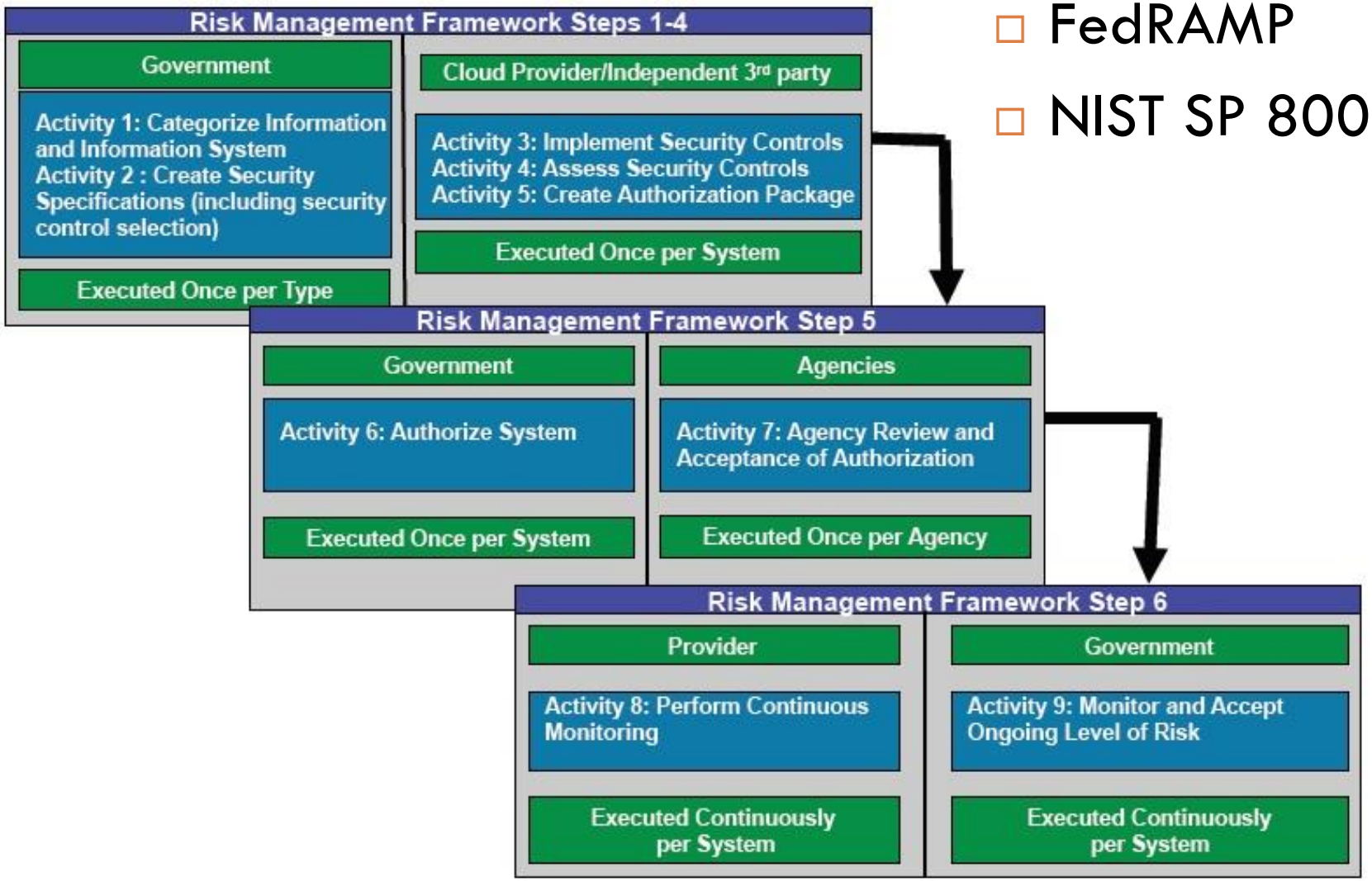
- Definovat typ cloudových služeb které bude organizace odebírat
- Popsat jak jsou tyto cloudové služby zabezpečeny a nakolik jsou v souladu s bezpečnostními požadavky organizace
- Provést pečlivou analýzu rizik a stanovit bezpečnostní opatření nezbytná k zachování bezpečnostní úrovně našeho prostředí, procesů a dat po migraci do cloudu
- Získat nezbytné záruky, že aktiva a činnost organizace budou vystaveny pouze rizikům která jsou akceptovatelná
- Neexistence standardů

# Hodnocení bezpečnosti cloudu

- Problém: neefektivní risk management
- Řešení: FedRAMP cloud.cio.gov

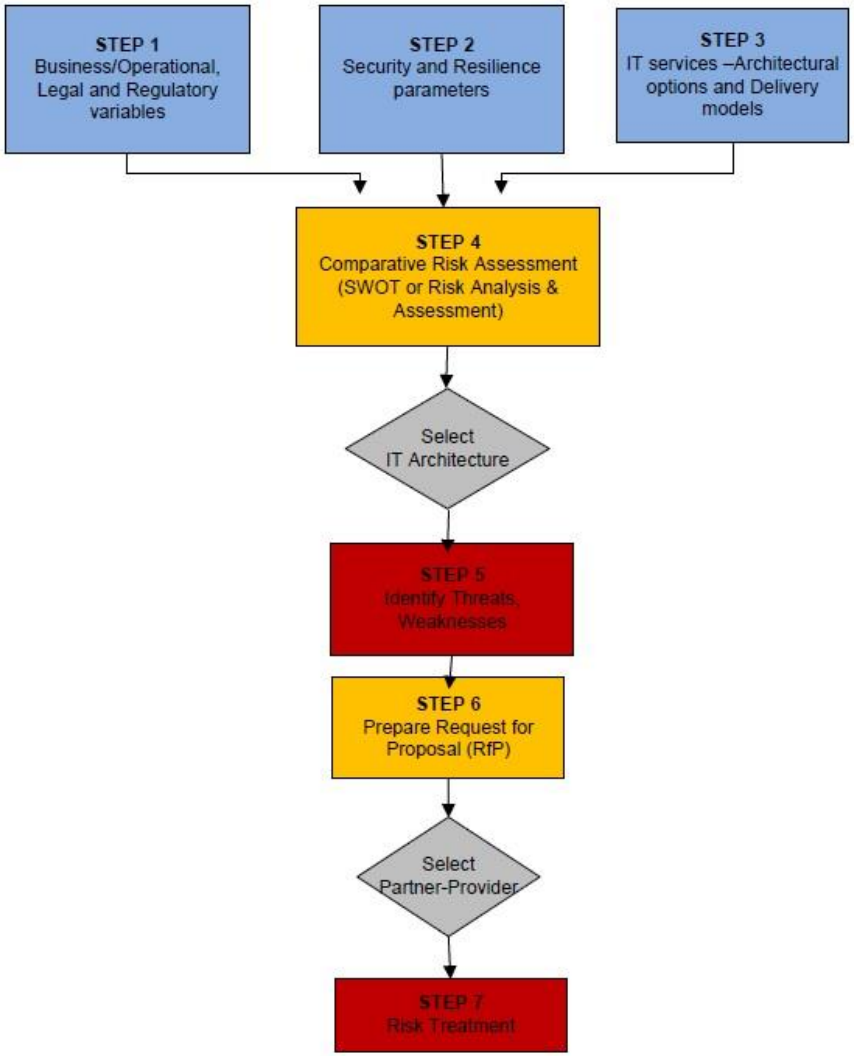



# Hodnocení bezpečnosti cloudu



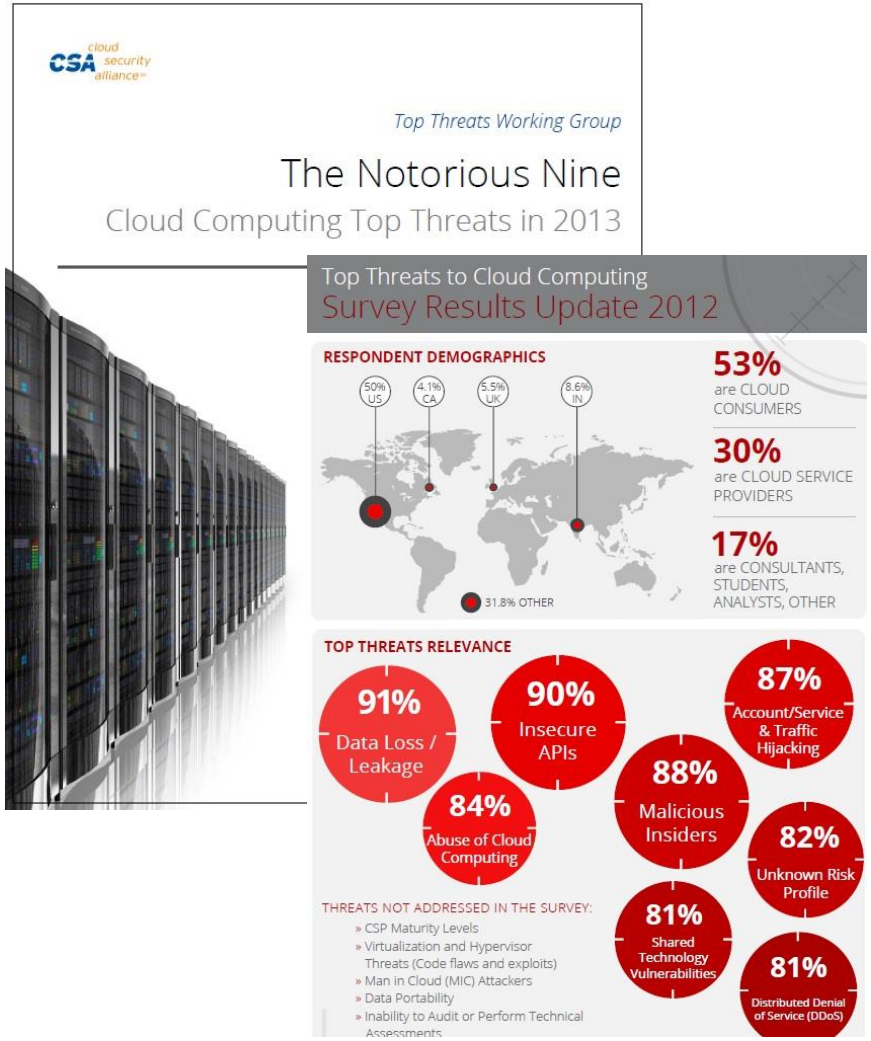

- FedRAMP
- NIST SP 800-37

# Hodnocení bezpečnosti cloudu




- ENISA
  - Security & Resilience in Governmental Clouds: Making an informed decision
  - Doporučuje postupný přístup zavádění
  - Vlády členských států by měli připravit strategie
  - Cloud a jeho vazba na ochranu kritické infrastruktury

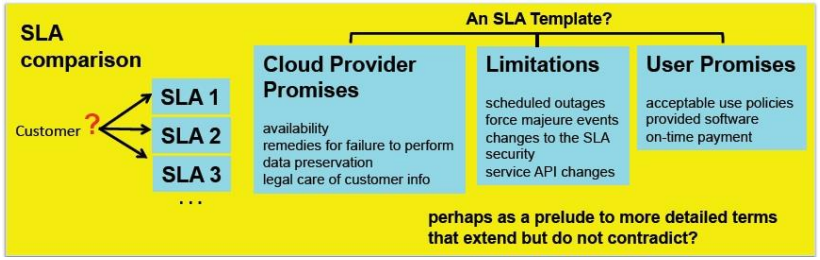
# Hodnocení bezpečnosti cloudu

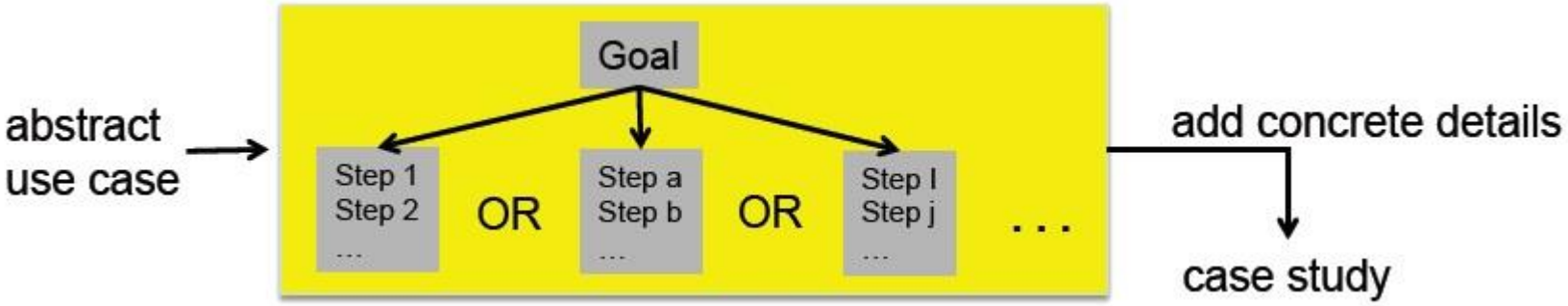



- Popis hrozeb a zranitelností
  - NIST – Cloud Computing Collaboration Site
  - Cloud Security Alliance
  - ENISA
- Součástí reportů jsou i doporučení implementace vhodných opatření

# Hodnocení bezpečnosti cloudu

- Use Cases – popis jak uživatelé v rámci cloudu mohou dosáhnout specifického cíle
- CIO Council udržuje knihovnu on-line dokumentace

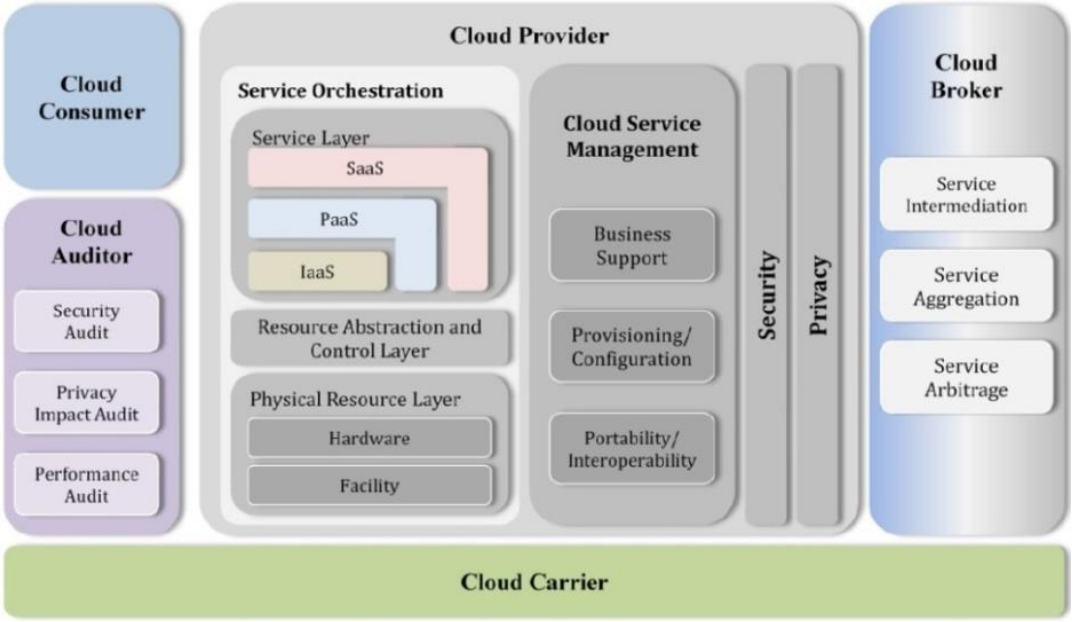


# Hodnocení bezpečnosti cloudu

- Vyšetření v oblastech
  - Důvěrnosti – data se nedostanou kam nemají
  - Integrity – nepoškozená data nebo systém
  - Dostupnosti – systém poběží
- Další oblasti spojené s cloudem
  - Důvěra v poskytovatele a jeho bezpečnostní model
  - Multi-tenancy
  - Exit strategy
  - Možnost šifrování
  - Závislost na hypervisorech
  - Dodržení právních norem
  - Nemožnost reagovat na nálezy auditů

# Hodnocení bezpečnosti cloudu




- NIST cloud computing reference model definuje pět důležitých hráčů (SP 500-292):
  - Uživatel cloudu
  - Poskytovatel cloudu
  - Poskytovatel připojení
  - Auditor
  - Zprostředkovatel
- Každý z hráčů zasahuje do procesů cloud computingu

# Hodnocení bezpečnosti cloudu

- Zpráva od nezávislého auditora
- Obsahuje popis implementovaných opatření a výsledek testu
- Certifikace ISO 27001, dále SAS 70 Type II, SSAE 16 Type II, ISAE 3402 Type II

# Hodnocení bezpečnosti cloudu

- NIST pracuje na SP 500-299 „Cloud Computing Security Reference Architecture“
- Nastavuje podmínky pro pořízení cloudových služeb
  - Hráči v cloudu (consumer, provider, broker, auditor, carrier)
  - Modely služeb (IaaS, PaaS, SaaS)
  - Modely nasazení (Public, Private, Community, Hybrid)
- Výstupem je framework poskytující
  - NIST Cloud Computing Security Reference Architecture (SRA)
    - Stanovuje základní množinu bezpečnostních komponent
    - Stanovuje kdo z hráčů za kterou komponentu zodpovídá
  - Metodologii pro stanovení bezpečnostních požadavků
  - Risk Management Framework uzpůsobený cloudu (CRMF)

# Hodnocení bezpečnosti cloudu

**Risk Management Framework NIST SP 800-37**

- Step 1: Categorize Information System
- Step 2: Select Security Controls
- Step 3: Implement Security Controls
- Step 4: Assess Security Controls
- Step 5: Authorize Information System
- Step 6: Monitor Security Controls (Repeat process as necessary)

**Cloud-adapted Risk Management Framework**

- Step 1: Categorize Application/System to be migrated
- Step 2: Identify Security Requirements, Perform a Risk Assessment to Identify Security Components (CIA analysis) & Select Security Controls
- Step 3: Select best-fitting Architecture for the System
- Step 4: Assess Service Provider(s)
- Step 5: Approve Use of Service
- Step 6: Monitor Service Provider

# Hodnocení bezpečnosti cloudu

- Po pečlivém výběru zvolena technologie Google Apps
- Stupeň důvěry, že jsou rizika na akceptovatelné úrovni závisí na důvěře v poskytovatele a v naše hodnocení
- Tam, kde nebyla dostatečná úroveň důvěry jsme volili
  - zmírnění rizika implementací protiopatření
    - Pořízení aplikace CloudLock Security & Vault
  - akceptaci rizika
    - Data v různých lokalitách na území USA a EU
  - vyhnutí se riziku tím, že jsme danou službu nepovolili
    - Google +

# Závěrem

- Metodiky hodnocení rizik cloudových řešení existují (NIST, ENISA)
- Informace mapující hrozby a zranitelnosti jsou publikovány (NIST, ENISA, CSA)
- Poskytovatelé cloudových řešení jsou hodnoceny (FedRAMP)
- Cloud mění způsob doručování IT služeb a tím se mění i tradiční role ICT
- Pro využití služeb veřejného cloudu je vhodné disponovat technickými experty schopnými ohodnotit škálovatelnost, výkon, bezpečnost a přenositelnost cloudových řešení
- Spolu s uživateli je vhodné otestovat vyspělost cloudových služeb a posoudit připravenost organizace přijmout tato standardizovaná řešení
- Organizace by měla zvyšovat své znalosti v oblasti risk managementu a contract managementu

# Odkazy

National Institute of Standard and Technology:

http://collaborate.nist.gov/twiki-cloud-computing/bin/view/CloudComputing/CloudSecurity

European Network and Information Security Agency:

http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cloud-computing

One Stop Source for Federal CC Information:

http://cloud.cio.gov/

U.S. General Services Administration:

http://www.gsa.gov/portal/category/102371

Cloud Security Alliance:

https://cloudsecurityalliance.org/research/top-threats/

# Dotazy

Děkuji za pozornost

Ing. Václav Žid

vaclav.zid@px.mvcr.cz