MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

ISO 27001
LL-C (Certification)

SOUHRNNĚ – 3C

Cloud Computingu ČR

Centrální nákupy SW produktů

Dohledové Centrum eGovernmentu MV

Ing. Miroslav Tůma, Ph.D.

odbor Kybernetické bezpečnosti a koordinace ICT

Ministerstvo vnitra ČR

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

- **Strategický rámec Národního cloud computingu – eGovernment cloud ČR**
- **Centralizované zadávání státu**
- **Dohledové centrum eGovernmentu**

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Hlavní cíle eGovernment cloudu (eGC)

- **Vychází z úkolu Akčního plánu k Národní strategii KB 2015-2020**
- **Strategický rámec - zásadní principy fungování eGovernmentu cloudu (eGC) a potřebné kroky nezbytné k jeho vybudování a využívání v prostředí ČR**

- **Zefektivnění ICT provozu a podpory IS/aplikací (IS) státní správy**
  - Konsolidace datových center – přesun IS státu (IaaS - Infrastructure as a Service)
  - Sdílení ICT zdrojů (infrastruktura, HW, základní SW, budovy, personál)
  - Snížení nákladů na provoz IS státní správy
  - Škálovatelnost výkonu provozní platformy podle potřeb jednotlivých IS
  - Zaměření státní správy na klíčové procesy, ne na ICT

- **Garance potřebné bezpečnosti a spolehlivosti provozu IS státní správy**

- **Standardizace provozního prostředí IS státní správy**

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Základní principy eGovernment cloudu

- **Strategický rámec je postaven na následujících předpokladech:**
  - **státní část eGC -** služby datových center, plně pod kontrolou státu s připojením ke garantované komunikační infrastruktuře státu (KIVS, ITS a CMS)
  - **komerční část eGC** - služby datových center komerčních subjektů včetně připojení na privátní komunikační infrastrukturu (popř. i vč. připojení na garantovanou komunikační infrastrukturu státu)
  - eGC poskytuje výpočetní výkon (IaaS) pro IS státní správy (neumisťuje se vlastní HW, ale pouze IS státní správy)
  - Umisťování aplikací bude ctít principy:
    - Stávající IS budou migrovány do eGC postupně tak, aby byly efektivně využity dosud investované finanční prostředky - tzn. migrace „nenásilnou“ formou.
    - Nové / inovované IS musí být umístěny do eGC.
    - IS a data státu, která mají pro stát strategický význam, musí být ve státní části eGC, tj. nemohou být umístěny do komerční části eGC(existence přesně specifikovaných výjimek a pravidel pro umisťování do eGC)

MINISTERSTVO VNITRA ČESKÉ REPUBLIKY

Základní fáze Strategického rámce eGC

0. **Předložení Strategického rámce eGC Vládě ČR** **10/2016**
   - ➢ Dopracování, MPŘ

1. **I. FÁZE – přípravná** **2016 - 2017**
   - ➢ Realizace projektu „Příprava vybudování eGovernment Cloudu“

2. **II. FÁZE – realizační** **2018 - 2019**
   - ➢ Vybudování eGovernment Cloudu

3. **III. FÁZE – standardizační** **2019 - 2022**
   - ➢ Výpočetní výkon – IaaS
     - ministerstva, úřady, státní instituce – povinné (výjimky)
     - kraje, obce – dobrovolné

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Projekt „Příprava vybudování eGC“

- **Pracovní skupina pod RVIS** složená ze zástupců - MV, MF, NBÚ, resortů, zpravodajských služeb a odborné veřejnosti připraví souhrnnou analytickou zprávu obsahující zejména:
  - Požadavky na státní a komerční část - provozní, bezpečnostní, SLA, …
  - Analýzu IS státu - stanovení strategických IS státu
  - Stanovení standardů eGC – platforem, služeb, …
  - Stanovení jasných a přesně specifikovaných výjimek
  - Zajištění právní podpory (z.č. 365, z.č. 137, …)
  - Kalkulace potřebných kapacit státní části
  - Analýzu datových center státu – současné kapacity
  - Pravidla financování státní části eGC
  - Proces umístění IS do eGC – metodika migrace
  - Metodiku hodnocení efektivity umístění IS do eGC – TCO
  - …
- Výstupy projektu „Příprava vybudování eGovernment cloudu“ budou předloženy Vládě ČR ke schválení zahájení vlastní realizace eGC

MINISTERSTVO VNITRA ČESKÉ REPUBLIKY

Aktuální stav centralizovaného zadávání státu pro SW produkty

➢ Microsoft

- Smlouva uzavřena v 12/2014 na 4,6 mld. Kč bez DPH s pěti dodavateli, expiruje 11/2018
- Dosud bylo čerpáno 2,042 mld. Kč bez DPH, zbývá dočerpat 2,558 mld. Kč s DPH
- Do dnešního dne využilo rámcovou smlouvu 115 subjektů OVM
- Celková dosažená sleva je zatím 697 mio, což činí 24,94 % z ceníkových cen

➢ VMware

- Dne 15. 8. 2016 vydalo MV na základě doporučení hodnotící komise rozhodnutí o výběru pěti dodavatelů.
- K dnešnímu dni došly proti tomuto rozhodnutí dvě námitky, které se v současné době posuzují.

MINISTERSTVO VNITRA ČESKÉ REPUBLIKY

Aktuální stav centralizovaného zadávání státu pro SW produkty

➢ Cisco Systems

- Výběr 5 dodavatelů RS – následně budou prováděny minitendry a uzavírány prováděcí smlouvy
- Termín zahájení výběrového řízení - říjen 2016
- Vzhledem k účinnosti nového ZZVZ budou osloveni všichni pověřující zadavatelé s dodatkem ke smlouvě o centralizovaném zadávání z důvodu úprav proti stávajícímu ZVZ

➢ IBM

- Rámcová smlouva je koncipována na možnost nákupů:
  i. dle ceníku s vysoutěženou slevou
  ii. formou AYCE (All you can eat) z předem vydefinovaných balíčků pro jednotlivé subjekty nebo s možností uzavírat AYCE v době trvání rámcové smlouvy
  iii. formou AYCE které budou požadovány i v průběhu trvání RS
- Termín zahájení výběrového řízení - listopad/prosinec 2016

Aktuální stav centralizovaného zadávání státu pro SW produkty

➢ Oracle

- ➢ Soutěž vybere pět dodavatelů RS – následně budou prováděny minitendry a uzavírány prováděcí smlouvy
- ➢ Nákup bude možný dle ceníku s vysoutěženou slevou nebo formou ULA (Unlimited Licence Agreement)
- ➢ RS umožní pořizování:
  - technické podpory pro stávající licence 22 % z ceny licence plus garantované maximálně 3 % meziročního navýšení
  - pořízení nových licencí včetně podpory (garance max. 2% meziročního navýšení
- ➢ Možnost uzavření Smlouvy k centralizovanému zadávání
- ➢ Předpokládaný termín zahájení soutěže říjen/listopad 2016
- ➢ I v případě této soutěže osloví MV pověřující zadavatele s dodatkem ke smlouvě z důvodu úprav dle nového ZVZ

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Aktuální stav centralizovaného zadávání státu pro SW produkty

Ke všem připravovaným soutěžím dosud lze formou podepsání Smlouvy o centralizovaném zadávání přistoupit!

Kontakt MV pro centralizované zadávání státu:

Ing. Ivo Rosypal
ivo.rosypal@mvcr.cz

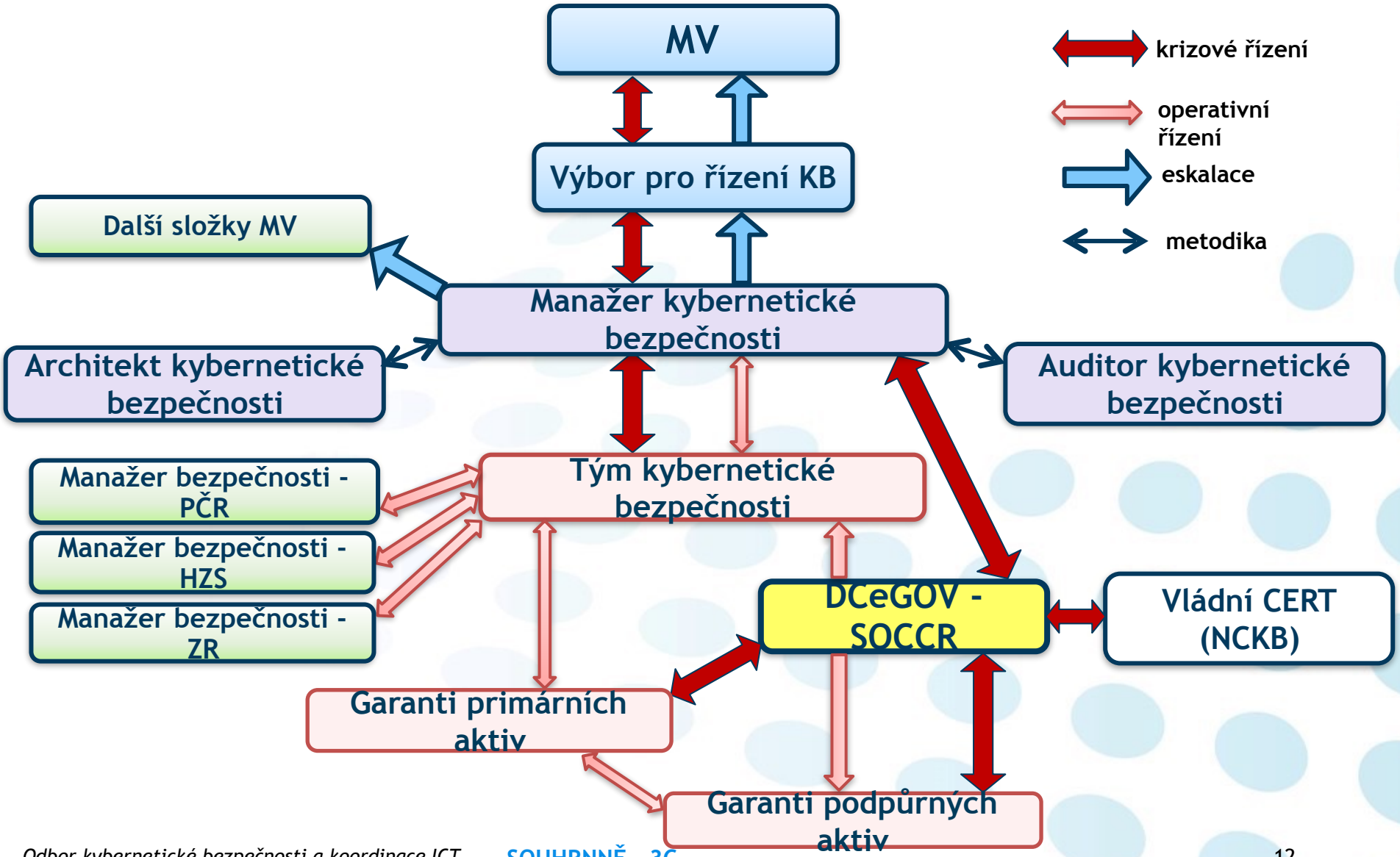
MINISTERSTVO VNITRA ČESKÉ REPUBLIKY

Dohledové centrum eGovernmentu (DCeGOV)

- Dle požadavků ZoKB a Vyhlášky č. 316/2014 Sb., o kybernetické bezpečnosti zajišťuje na centrální úrovni bezpečnostní dohledy nejen pro KII a VIS resortu MV
- V souladu úkolem Akčního plánu k Národní strategii KB 2015-2020 MV vybudovalo resortní CERT/CSIRT pracoviště pro ochranu základních registrů a dalších důležitých systémů pro fungování eGovernmentu
- Zajišťuje jednotné řízení a zvládání bezpečnostních i provozních událostí a incidentů včetně funkční rozhraní pro hlášení KBI na NCKB
- Sbírá a vyhodnocuje provozní a bezpečnostní události v režimu 24x7

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Organizační zapojení DCeGOV



MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

DCeGOV – základní vlastnosti

➢ Základní pilíře DCeGOV

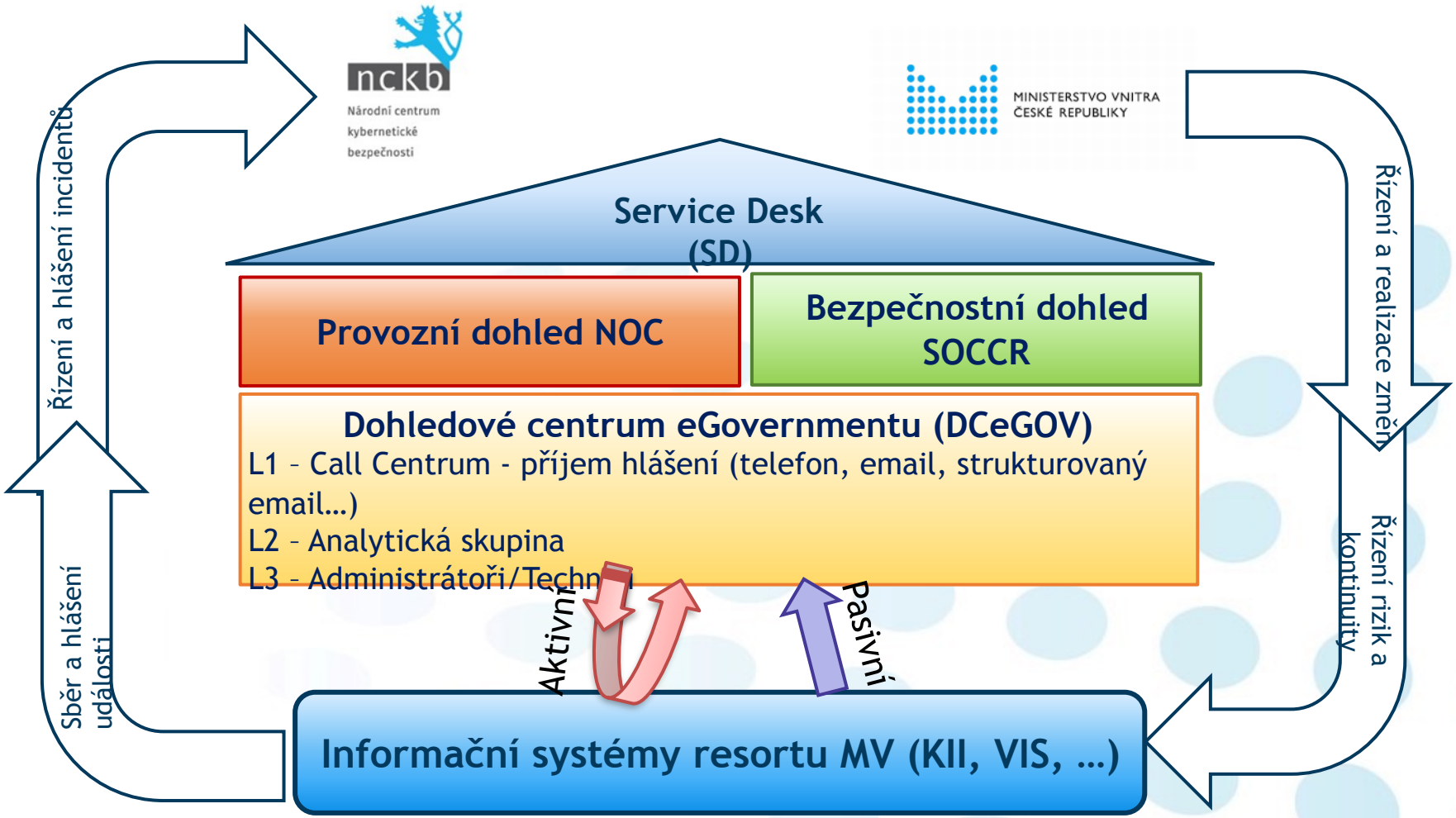
- CALL CENTRUM / příjem událostí
- SOCCR / bezpečnostní proaktivní dohled
- NOC / provozní proaktivní dohled

➢ Základní vlastnosti DCeGOV

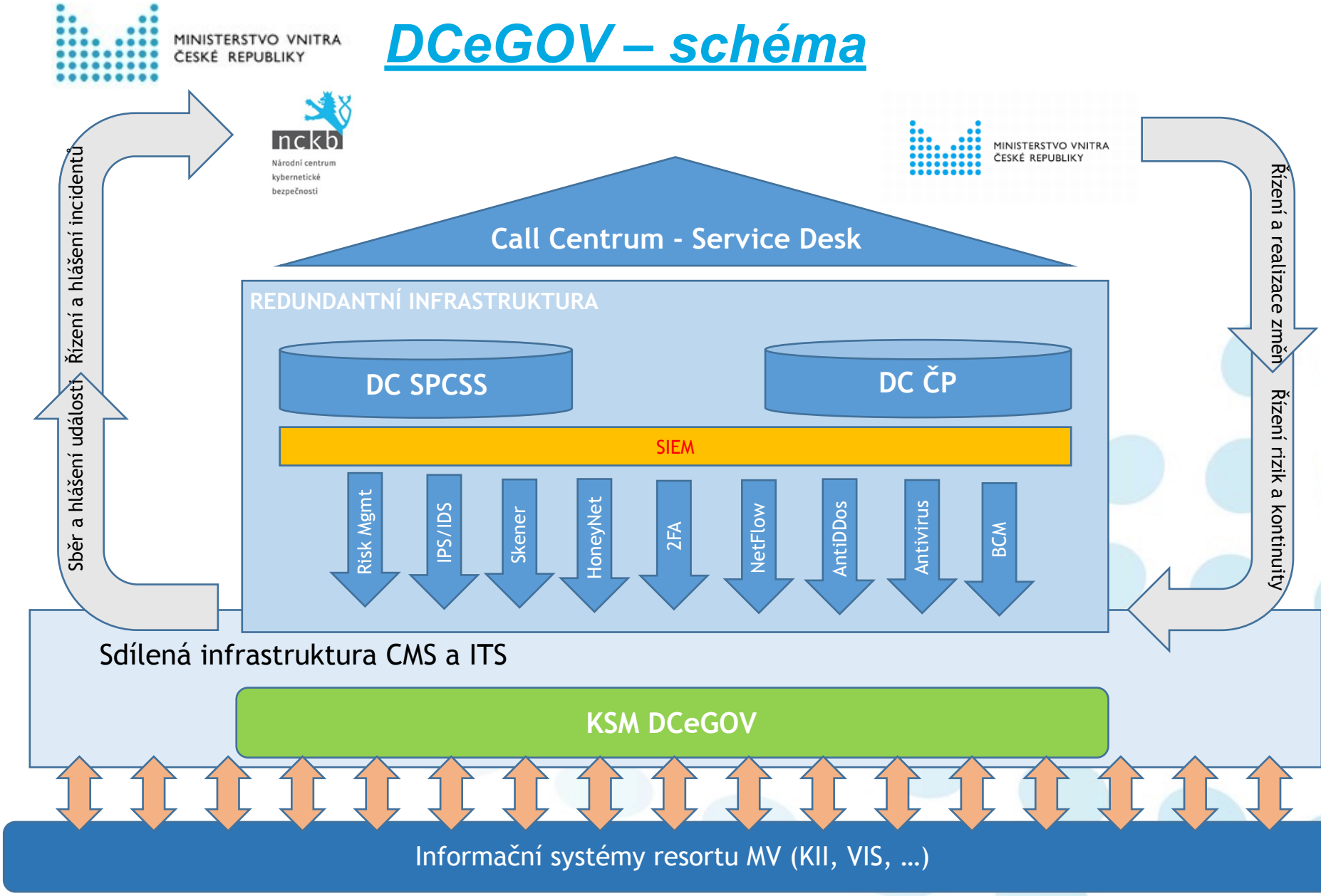
- Soulad se ZoKB (Zák.č.181/2014 Sb.) a ISO standardy
- Geograficky redundantní řešení - vysoká dostupnost
- Řídí bezpečnost systémů v aktivním a pasivním módu
- Zajišťuje proaktivní dohled
- 14 konektorů na úrovni krajů pro napojení krajských prvků a rozšíří monitoring do všech přípojných uzlů síti MV
- Vytváří efektivní procesy pomocí portálu Service Desk
- Koordinace týmů (SOCCR, TKB, …)
- Provoz 24x7x365
- Modulární architektura, vlastní aktivní ochrana, znalostní databáze

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

DCeGOV – základní vlastnosti



DCeGOV – schéma



MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

DCeGOV – služby

- **Primární služby**
  - Log management
  - Provozní monitoring
- **Bezpečnostní služby**
  - Zabezpečení perimetru
  - Kontrola obsahu
  - Analýza datových toků
  - Analýza kapacitních ukazatelů
  - Aktualizace bezpečnostních opatření
  - Risk management
  - Řízení kontinuity
  - Analýza hrozeb
  - Proaktivní dohled
- **Podpůrné služby**
  - Patch management
  - Release management
  - Zálohování
  - Archivace
  - IDM
  - NTP (řízení přesného času)
  - Zabezpečený vzdálený přístup
  - SMS notifikace
  - e-mailové služby
  - Vícefaktorová autentifikace
  - …

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

DCeGOV – nástroje

Technologické nástroje

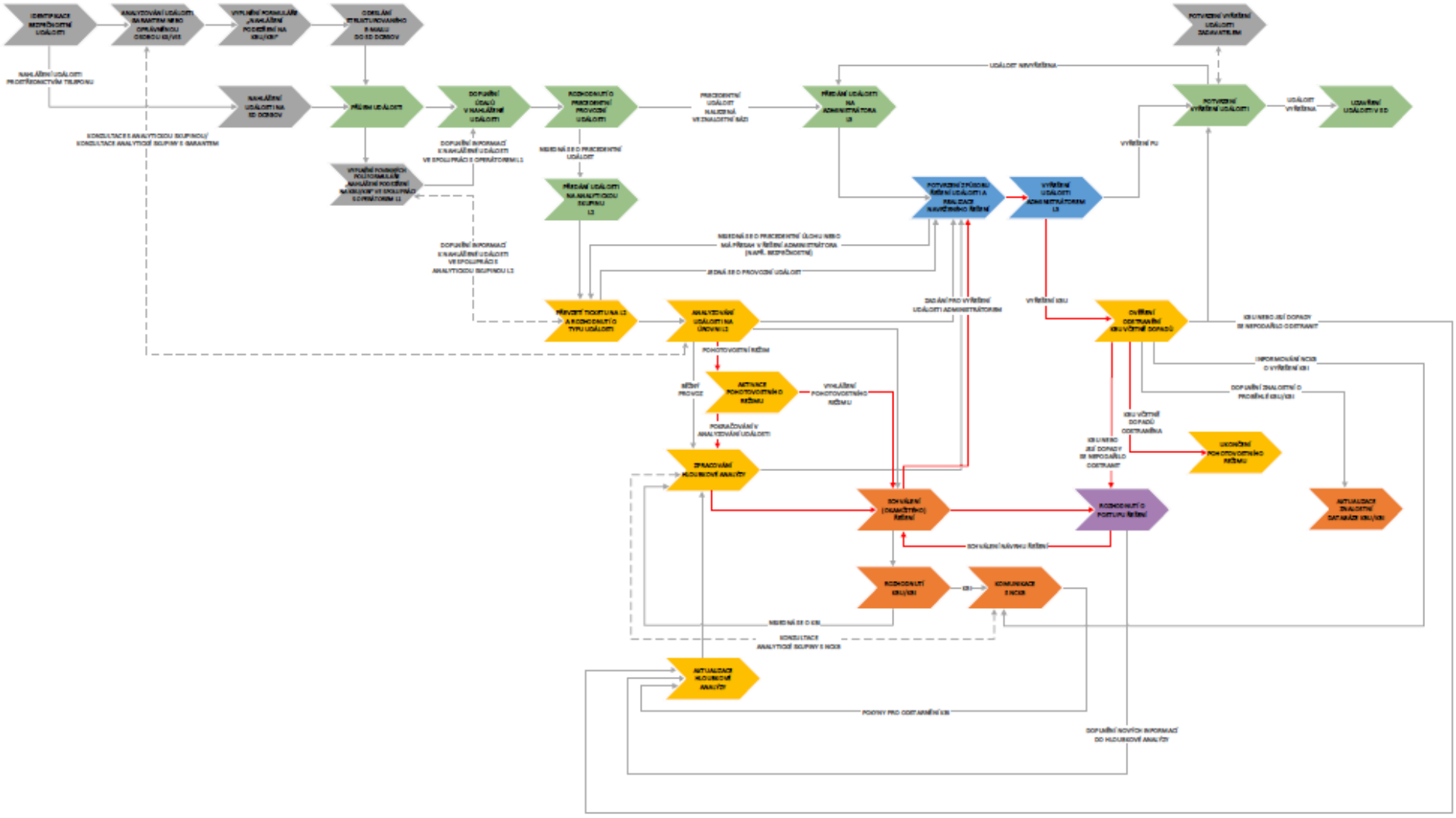
- CallCentrum
- ServiceDesk
- SIEM
- Logger
- HoneyNet
- Net Flow
- Vulnerability Management
- Řízení rizik a kontinuity
- Antivirus
- AntiDDos
- IDS/IPS
- 2 FA

Personál

- Operátoři
- Analytická skupina
  - Administrátoři
  - Správci
  - Analytici
- Kompetenční zázemí
  - Architekti
  - Vývoj
  - Bezpečnost
  - Tým kybernetické bezpečnosti
- Externí podpora
  - Dodavatelé
  - Partneři

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Procesní schéma DCeGOV



MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

DCeGOV – další rozvoj

- Analytické nástavby pro vyhodnocování NetFlow
- Nástroje pro identifikaci botnetů
- Technologie pro monitoring, filtraci a antimalware ochranu protokolů http, ftp, a to i šifrovaných
- Nástroje na simulace řízení kritických situací
- Billing
- Nástroje forenzní a BI analýzy pro resort
- Rešerše a sledování aktuálních hrozeb
- Rešerše a sledování aktuálního technologického rozvoje
- Spolupráce s významnými pracovišti typu SOC

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

… děkuji za pozornost a čas, přeji hezký den

Ing. Miroslav Tůma, Ph.D.

Ministerstvo vnitra ČR
ředitel odboru Kybernetické bezpečnosti a koordinace ICT