MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

ISO 27001
LL-C (Certification)

Certifikace Ministerstva vnitra v oblasti kyberbezpečnosti

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Agenda

- Informace o průběhu implementace ISMS na základě požadavků ZoKB v resortu MV
- Představení zabezpečení jednotlivých KII a VIS dle ZoKB
- Dohledové centrum eGovernmentu (SOCCR) – kybernetické bezpečnostní dohledy

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Organizace kybernetické bezpečnosti

- **Vzájemná spolupráce při implementaci ISMS, dohled nad jejím dodržováním a návrhy implementace bezpečnostních opatření v čase**

  - **Výbor pro řízení kybernetické bezpečnosti**
  - **Manažer kybernetické bezpečnosti**
  - **Auditor kybernetické bezpečnosti**
  - **Architekt kybernetické bezpečnosti**
  - **Tým kybernetické bezpečnosti**
  - **Garanti aktiv**

Milan Chovanec
ministr vnitra

Praha . října 2015
Č. j.: MV-155331-1/OKB-2015
Počet listů: 1

POVĚŘENÍ

Dle § 6 vyhlášky 316/2014 Sb., a dle zákona o kybernetické bezpečnosti č. 181/2014 Sb., s účinností ode dne podpisu tohoto dokumentu

pověřuji

Ing. Bohuslava Zůbka
vedoucího oddělení kybernetické bezpečnosti
odboru kybernetické bezpečnosti a koordinace ICT,
OEČ 689320

Funkcí: Manažer kybernetické bezpečnosti resortu Ministerstva vnitra České republiky.

Tato listina byla vyhotovena ve dvou stejnopisech, z nichž jeden převzal jmenovaný a druhý zaměstnavatel.

V Praze dne - 5 -11- 2015

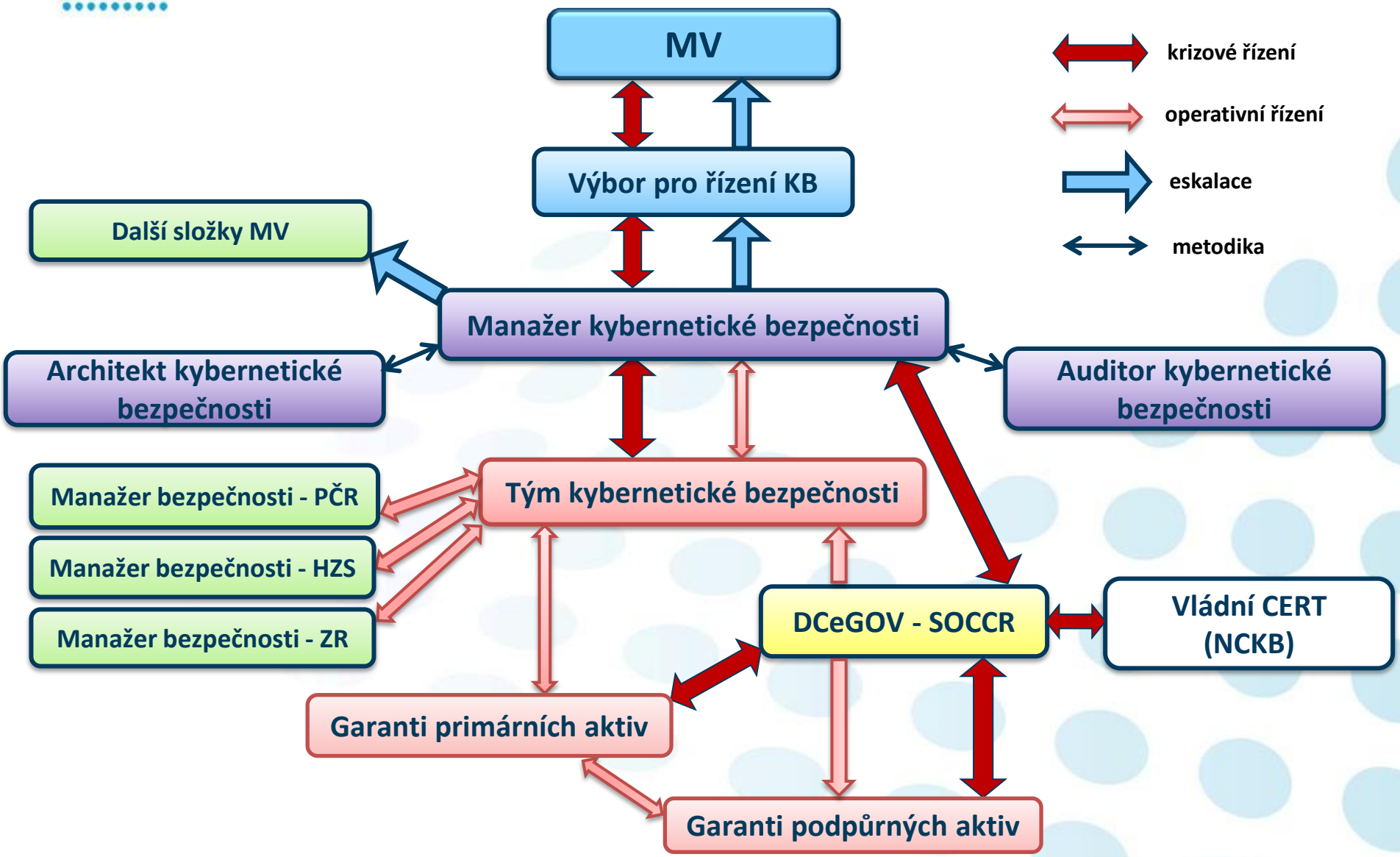
Milan Chovanec
ministr vnitra

Jmenovaný pověření převzal
V Praze dne 9. 11. 2015

Ing. Bohuslav Zůbek

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Organizace kybernetické bezpečnosti - řízení

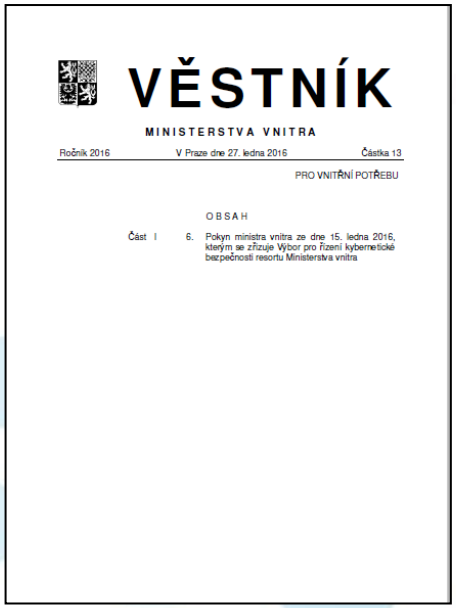


MINISTERSTVO VNITRA ČESKÉ REPUBLIKY

Výbor pro řízení kybernetické bezpečnosti

PMV č. 6/2016, kterým se zřizuje Výbor pro řízení kybernetické bezpečnosti resortu Ministerstva vnitra

- ***Příloha č. 1 – Statut Výboru pro řízení kybernetické bezpečnosti resortu Ministerstva vnitra***
  - *Kompetence a odpovědnost Výboru*
  - *Složení Výboru KB*
  - *Předseda, místopředseda a tajemník Výboru*
  - *Členové Výboru*
  - *Administrativní zajištění činnosti Výboru*
  - *Pracovní skupiny*
  - *Zmocnění pro NMV pro řízení sekce ICT*



VĚSTNÍK

MINISTERSTVA VNITRA

Ročník 2016 V Praze dne 27. ledna 2016 Částka 13

PRO VNITŘNÍ POTŘEBU

OBSAH

Část I 6. Pokyn ministra vnitra ze dne 15. ledna 2016, kterým se zřizuje Výbor pro řízení kybernetické bezpečnosti resortu Ministerstva vnitra

- ***Příloha č. 2 – Jednací řád Výboru pro řízení kybernetické bezpečnosti resortu MV***
  - *Zajištění činnosti Výboru*

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Tým kybernetické bezpečnosti

Tým KB – poradní tým pro manažera kybernetické bezpečnosti resortu MV

- **Centrální výkonný útvar s celoresortní působností jehož cílem je zajištění kybernetické bezpečnosti resortu Ministerstva vnitra**

- **Složení** - zástupci organizačních složek resortu MV(15 členů týmu):
  - Ministerstvo vnitra
  - Policie České republiky
  - Generální ředitelství hasičského záchranného sboru
  - Správy základních registrů
  - ČPOZ
  - Externí spolupracovníci

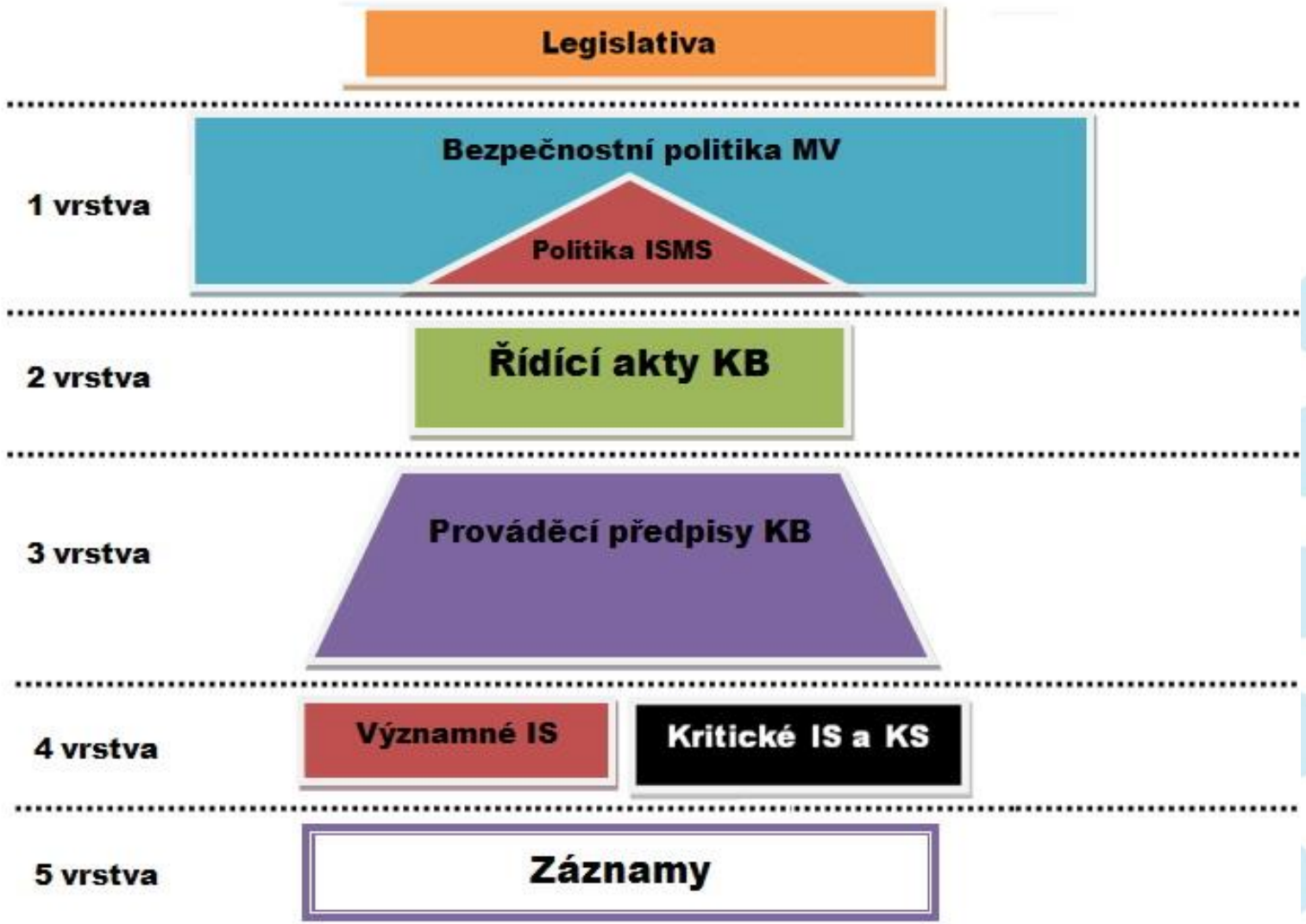
MINISTERSTVO VNITRA ČESKÉ REPUBLIKY

Tým kybernetické bezpečnosti

- **Oprávnění:**
  - **Zpracovává a předkládá Výboru KB stanoviska a návrhy s doporučeními zavedení bezpečnostních opatření, a to:**
    - Opatření organizační - procesní pravidla a organizačně personální opatření,
    - Opatření technická - nové technologie, změny technických standardů (operačních systémů a zařízení) ve vztahu k ZoKB.
  - **Předkládá návrhy změn bezpečnostních SLA vůči dodavatelům**
  - **Předkládá návrhy projektové a provozní dokumentace všech IS KII, KS KII a VIS včetně dokumentace pro školitele, uživatelských a administrátorských příruček**
- **V případě krize – incidentu – jsou manažerem KB, vybraní členové Týmu KB, případně další specialisté v rámci jejich odborné specializace přizváni k provedení činností nezbytných pro zvládnutí kybernetických incidentů v kritickém kybernetickém režimu**

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

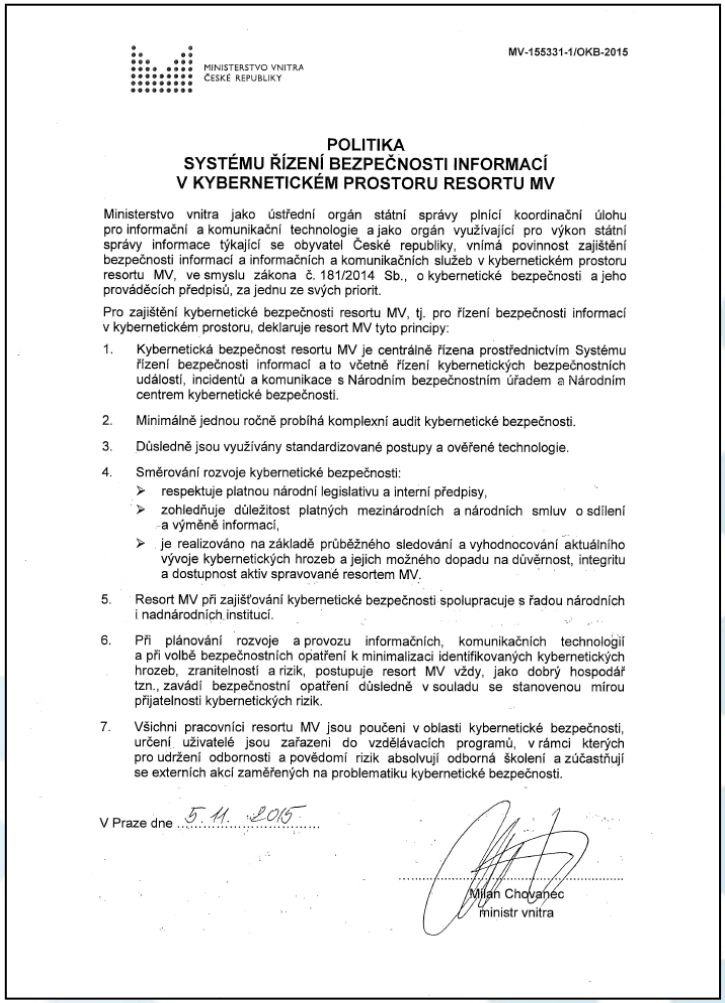
Systém řízení bezpečnosti informací



MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Politika Systému řízení bezpečnosti informací

1. Centrální řízení KB prostřednictvím ISMS
2. Komplexní audit minimálně jednou ročně
3. Důsledné využívání standardizace a ověřených technologií
4. Směr rozvoje KB (v souladu s platnou národní i nadnárodní právní úpravou, zohledňuje aktuální hrozby a rizika)
5. Aktivní spolupráce při řešení KB s národními i nadnárodními institucemi včetně bezpečnostních složek
6. Plánovitý rozvoj a provoz ICT při volbě bezpečnostních opatření k minimalizaci kybernetických hrozeb
7. Bezpečnostní povědomí a plánované vzdělávání



MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

MV-155331-1/OKB-2015

POLITIKA
SYSTÉMU ŘÍZENÍ BEZPEČNOSTI INFORMACÍ
V KYBERNETICKÉM PROSTORU RESORTU MV

Ministerstvo vnitra jako ústřední orgán státní správy plnící koordinační úlohu pro informační a komunikační technologie a jako orgán využívající pro výkon státní správy informace týkající se obyvatel České republiky, vnímá povinnost zajištění bezpečnosti informací a informačních a komunikačních služeb v kybernetickém prostoru resortu MV, ve smyslu zákona č. 181/2014 Sb., o kybernetické bezpečnosti a jeho prováděcích předpisů, za jednu ze svých priorit.

Pro zajištění kybernetické bezpečnosti resortu MV, tj. pro řízení bezpečnosti informací v kybernetickém prostoru, deklaruje resort MV tyto principy:

1. Kybernetická bezpečnost resortu MV je centrálně řízena prostřednictvím Systému řízení bezpečnosti informací a to včetně řízení kybernetických bezpečnostních událostí, incidentů a komunikace s Národním bezpečnostním úřadem a Národním centrem kybernetické bezpečnosti.
2. Minimálně jednou ročně probíhá komplexní audit kybernetické bezpečnosti.
3. Důsledně jsou využívány standardizované postupy a ověřené technologie.
4. Směrování rozvoje kybernetické bezpečnosti:
   - respektuje platnou národní legislativu a interní předpisy,
   - zohledňuje důležitost platných mezinárodních a národních smluv o sdílení a výměně informací,
   - je realizováno na základě průběžného sledování a vyhodnocování aktuálního vývoje kybernetických hrozeb a jejich možného dopadu na důvěrnost, integritu a dostupnost aktiv spravované resortem MV.
5. Resort MV při zajišťování kybernetické bezpečnosti spolupracuje s řadou národních i nadnárodních institucí.
6. Při plánování rozvoje a provozu informačních, komunikačních technologií a při volbě bezpečnostních opatření k minimalizaci identifikovaných kybernetických hrozeb, zranitelností a rizik, postupuje resort MV vždy, jako dobrý hospodář tzn., zavádí bezpečnostní opatření důsledně v souladu se stanovenou mírou přijatelnosti kybernetických rizik.
7. Všichni pracovníci resortu MV jsou poučeni v oblasti kybernetické bezpečnosti, určení uživatelé jsou zařazeni do vzdělávacích programů, v rámci kterých pro udržení odbornosti a povědomí rizik absolvují odborná školení a zúčastňují se externích akcí zaměřených na problematiku kybernetické bezpečnosti.

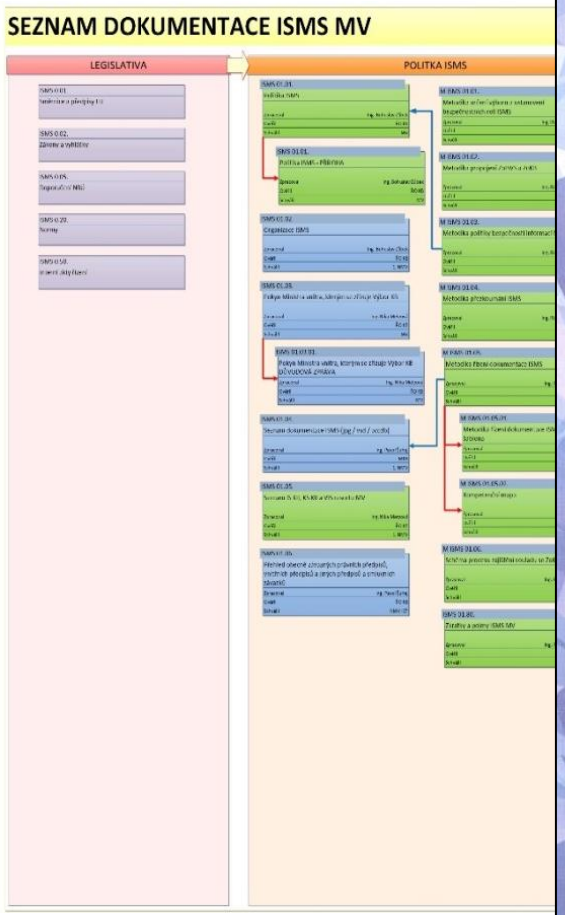
V Praze dne 5. 11. 2015

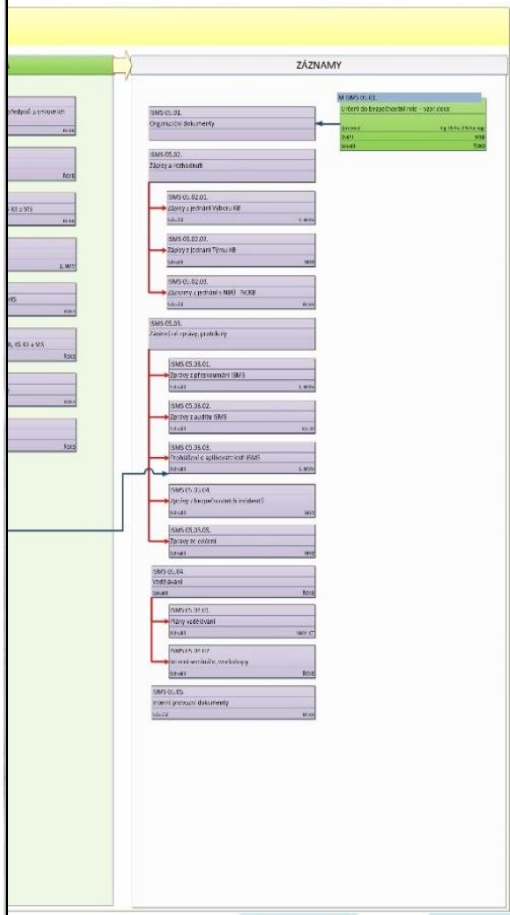
Milan Chovanec
ministr vnitra

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Systém řízení bezpečnosti informací

- **ISMS certifikace IS**





MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Bezpečnostní povědomí - vzdělávání

- **Prezenční školení zástupců organizačních složek resortu MV**
- **Celkem 51 (53) útvarů (MV, PČR, HZS, OSS) – cca 70 tisíc**
- **Webový portál pro základní samovzdělávání v oblasti KB:**

  - Potvrzení seznámení se s materiály KB podmínkou pro zachování / zřízení přístupu do kybernetického prostoru MV

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Bezpečnostní povědomí - vzdělávání

- **Plán návazných školení resortu Ministerstva vnitra**
- **Rozdělení dle rolí:**
  - uživatel
  - podle pracovního místa
  - …
- **Příprava e-Learningu ve spolupráci s NBÚ**

	anonymní uživatelé		identifikovaní uživatelé					
	pasivní	aktivní	každý uživatel	uživatelé s přístupem do sítě MV	operátor VIS nebo KII	uživatelé mobilního zařízení	Garant primárního aktiva	privilegovaní uživatelé
vzdělávací modul								
základní modul (BASIC)			X	X	X	X	X	X
sdílené informační prostředí a ICT služby				X	X	X	X	X
VIS a KII					X		X	
mobilní zařízení						X	X	X
správa uživatelů							X	(x)
zvolená forma informování / vzdělávání uživatele								
úvodní okno zobrazující na přístupové stránce k systému užívací podmínky		X						
eLearning			X					
eLearning + doporučená literatura				X		X	X	
korespondenční kurz + osobní konzultace					X			
osobní návštěva kurzu + doporučená literatura								X
zvolená forma ověření seznámení se s pravidly + přijetí pravidel / dosažení znalostí								
"kliknutím" odsouhlasené přijetí zobrazených podmínek (uživatel přijímá omezení i rizika)		X						
"kliknutím" odsouhlasené prohlášení o seznámení se se vzdělávacími podklady			X					
úspěšně zodpovězený elearningový test				X		X	X	
složení závěrečného testu					X			X

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

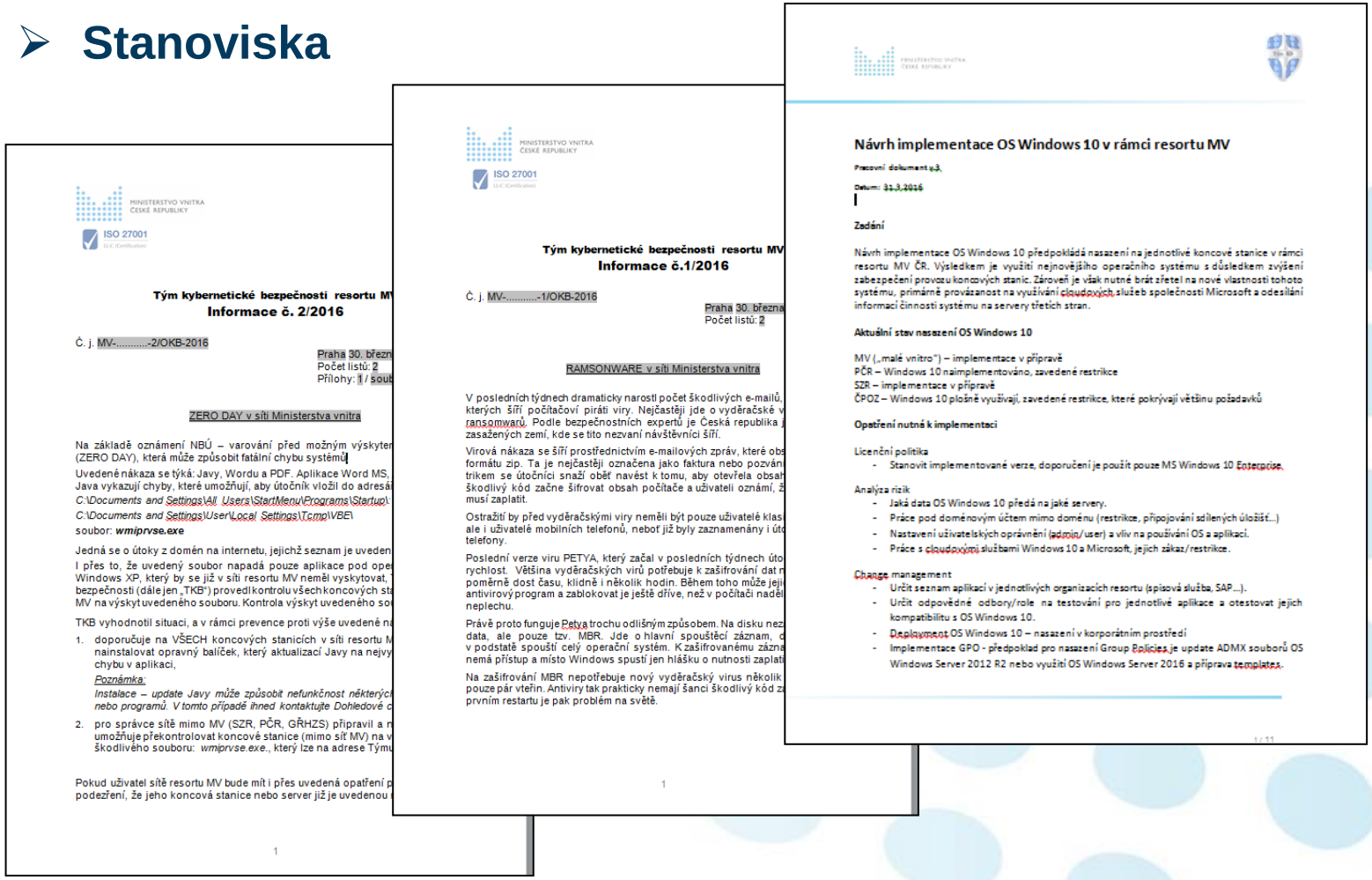
Bezpečnostní povědomí

- **Informování o hrozbách a způsobech jejich zvládání**
- **Odbor kybernetické bezpečnosti a koordinace ICT & Tým KB:**
  - Monitoring veřejných zdrojů
  - Katalog hrozeb
  - Katalog Best Practices
  - Bezpečnostní zásady
  - Sdílené informace NBÚ
  - Znalostní databáze DCeGOV
- **Distribuční kanál**
  - kyberinfo@mvcr.cz

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Bezpečnostní povědomí

- **Informace – opatření pro resort MV**
- **Stanoviska**



ISO 27001

Tým kybernetické bezpečnosti resortu MV
Informace č. 2/2016

Č. j. MV-.....-2/OKB-2016

Praha 30. březn
Počet listů: 2
Přílohy: 1 / soub

ZERO DAY v síti Ministerstva vnitra

Na základě oznámení NBÚ – varování před možným výskyte
(ZERO DAY), která může způsobit fatální chybu systémů.

Uvedené nákaza se týká: Javy, Wordu a PDF. Aplikace Word MS,
Java vykazují chyby, které umožňují, aby útočník vložil do adresá
C:\Documents and Settings\All Users\StartMenu\Programs\Startup
C:\Documents and Settings\User\Local Settings\Temp\VBE
soubor: ***wmiprvse.exe***

Jedná se o útoky z domén na internetu, jejichž seznam je uveden

I přes to, že uvedený soubor napadá pouze aplikace pod ope
Windows XP, který by se již v síti resortu MV neměl vyskytovat,
bezpečnosti (dále jen „TKB") provedl kontrolu všech koncových st
MV na výskyt uvedeného souboru. Kontrola výskyt uvedeného so

TKB vyhodnotil situaci, a v rámci prevence proti výše uvedené n

1. doporučuje na VŠECH koncových stanicích v síti resortu M
   nainstalovat opravný balíček, který aktualizací Javy na nejvy
   chybu v aplikaci,
   Poznámka:
   Instalace – update Javy může způsobit nefunkčnost některých
   nebo programů. V tomto případě ihned kontaktujte Dohledové c
2. pro správce sítě mimo MV (SZR, PČR, GŘHZS) připravil a n
   umožňuje překontrolovat koncové stanice (mimo síť MV) na v
   škodlivého souboru: *wmiprvse.exe.*, který lze na adrese Tým

Pokud uživatel sítě resortu MV bude mít i přes uvedená opatření p
podezření, že jeho koncová stanice nebo server již je uvedenou

1

ISO 27001

Tým kybernetické bezpečnosti resortu MV
Informace č.1/2016

Č. j. MV-.....-1/OKB-2016

Praha 30. března
Počet listů: 2

RAMSONWARE v síti Ministerstva vnitra

V posledních týdnech dramaticky narostl počet škodlivých e-mailů,
kterých šíří počítačoví piráti viry. Nejčastěji jde o vyděračské v
ransomwarů. Podle bezpečnostních expertů je Česká republika
zasažených zemí, kde se tito nezvaní návštěvníci šíří.

Virová nákaza se šíří prostřednictvím e-mailových zpráv, které obs
formátu zip. Ta je nejčastěji označena jako faktura nebo pozván
trikem se útočníci snaží oběť navést k tomu, aby otevřela obsah
škodlivý kód začne šifrovat obsah počítače a uživateli oznámí, ž
musí zaplatit.

Ostražití by před vyděračskými viry neměli být pouze uživatelé klas
ale i uživatelé mobilních telefonů, neboť již byly zaznamenány i útc
telefony.

Poslední verze viru PETYA, který začal v posledních týdnech úto
rychlost. Většina vyděračských virů potřebuje k zašifrování dat n
poměrně dost času, klidně i několik hodin. Během toho může jeji
antivirový program a zablokovat je ještě dříve, než v počítači naděl
neplechu.

Právě proto funguje Petya trochu odlišným způsobem. Na disku nez
data, ale pouze tzv. MBR. Jde o hlavní spouštěcí záznam, d
v podstatě spouští celý operační systém. K zašifrovanému zázna
nemá přístup a místo Windows spustí jen hlášku o nutnosti zaplati

Na zašifrování MBR nepotřebuje nový vyděračský virus několik
pouze pár vteřin. Antiviry tak prakticky nemají šanci škodlivý kód z
prvním restartu je pak problém na světě.

1

Návrh implementace OS Windows 10 v rámci resortu MV

Pracovní dokument v.3.

Datum: 31.3.2016

Zadání

Návrh implementace OS Windows 10 předpokládá nasazení na jednotlivé koncové stanice v rámci resortu MV ČR. Výsledkem je využití nejnovějšího operačního systému s důsledkem zvýšení zabezpečení provozu koncových stanic. Zároveň je však nutné brát zřetel na nové vlastnosti tohoto systému, primárně provázanost na využívání cloudových služeb společnosti Microsoft a odesílání informací činnosti systému na servery třetích stran.

Aktuální stav nasazení OS Windows 10

MV („malé vnitro") – implementace v přípravě
PČR – Windows 10 naimplementováno, zavedené restrikce
SZR – implementace v přípravě
ČPOZ – Windows 10 plošně využívají, zavedené restrikce, které pokrývají většinu požadavků

Opatření nutná k implementaci

Licenční politika
- Stanovit implementované verze, doporučení je použít pouze MS Windows 10 Enterprise.

Analýza rizik
- Jaká data OS Windows 10 předá na jaké servery.
- Práce pod doménovým účtem mimo doménu (restrikce, připojování sdílených úložišť...)
- Nastavení uživatelských oprávnění (admin/user) a vliv na používání OS a aplikací.
- Práce s cloudovými službami Windows 10 a Microsoft, jejich zákaz/restrikce.

Change management
- Určit seznam aplikací v jednotlivých organizacích resortu (spisová služba, SAP...).
- Určit odpovědné odbory/role na testování pro jednotlivé aplikace a otestovat jejich kompatibilitu s OS Windows 10.
- Deployment OS Windows 10 – nasazení v korporátním prostředí
- Implementace GPO - předpoklad pro nasazení Group Policies je update ADMX souborů OS Windows Server 2012 R2 nebo využití OS Windows Server 2016 a příprava templates.

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Bezpečnostní povědomí - Intranet MV

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

PRO UŽIVATELE

- Základní informace

DOPORUCENI NBU

- Bezpečnostní role
- Proces určování KII
- Pomůcka k auditu

PŘIHLÁŠENÍ

Uživatel:

Heslo:

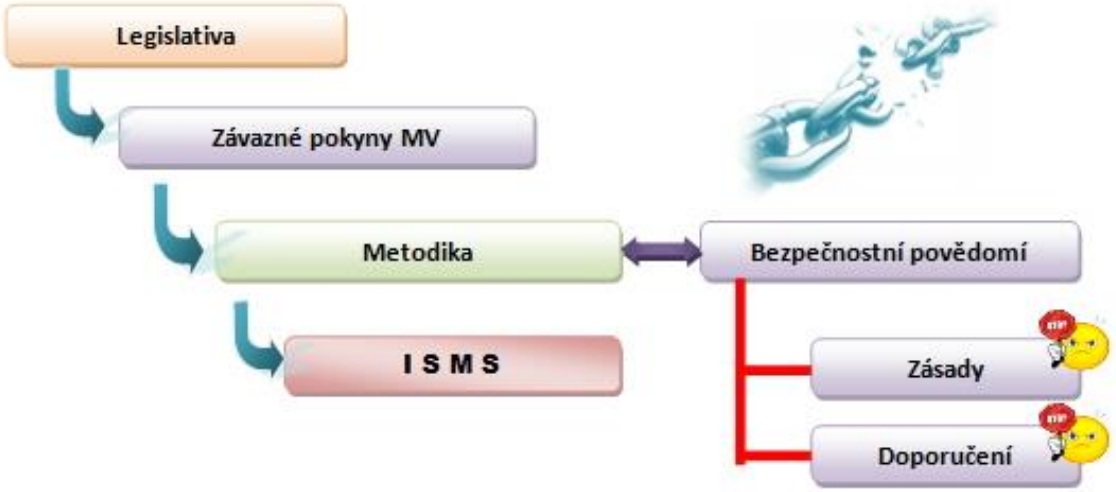
OK | SOS přihlášení

ISO 27001
LL-C (Certification)

Kybernetická bezpečnost resortu Ministerstva vnitra

Ministerstvo vnitra jako ústřední orgán státní správy plnící koordinační úlohu pro informační a komunikační technologie a jako orgán využívající pro výkon státní správy informace týkající se obyvatel České republiky, vnímá povinnost zajištění bezpečnost informací a informačních a komunikačních služeb v kyberprostoru resortu MV, ve smyslu zákona č.181/2014 Sb., o kybernetické bezpečnosti a vyhlášky č. 316/2014 Sb., o kybernetické bezpečnosti, za jednu ze svých priorit.

Pro zajištění kybernetické bezpečnosti (dále jen „KB"), tj. pro řízení bezpečnosti informací ve „svém" kyberprostoru, zavedl resort MV systém řízení bezpečnosti informací (ISMS). Ten zahrnuje určení povinností a odpovědností za vytvoření a dodržování zdokumentovaných bezpečnostních zásad a postupů, umožňuje průběžnou automatickou aktualizaci znalostní databáze (evidence) kritických a významných informačních a komunikačních systémů včetně jejich garantů a významnosti primárních aktiv a podpůrných aktiv.



Dohledové centrum, email: dohled@mvcr.cz , telefon: 974 801 131

MINISTERSTVO VNITRA ČESKÉ REPUBLIKY

KII a VIS resortu Ministerstva vnitra

- **Celkem 27 prvků kritické informační infrastruktury a významných informačních systémů v resortu MV**
  - 9 významných informačních systémů (VIS)
  - 18 prvků kritické informační infrastruktury (KII)
  - Dalších cca 120 informačních a komunikačních systémů a aplikací
- **Tvorba bezpečnostní dokumentace pro KII a VIS**
- **Zavádění opatření a napojení na Dohledové centrum MV (DCeGOV) – bezpečnostní monitoring**
- **Hlášení kybernetických bezpečnostních incidentů na NCKB a komunikace s NBÚ a NCKB**
- **Zajištění bezpečnosti celého kybernetického prostoru resortu MV**

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Seznam systémů KII / VIS a jejich garantů aktiv

Kód systému	Zkratka systému	Název systému	Garanti primárního aktiva	Garanti podpůrného aktiva
K01	Pegas	Komunikační systém pro IZS	Mgr. Václav Hladík	Miloš Andrle
K02	ISDS	Informační systém datových schránek	Ing. Ondřej Menoušek	Ing. Pavel Chyla
K03	CZP	Informační systém CZECH Point	RNDr. Renáta Horáková	Ing. Michal Souček
K04	AIS EO	Agendový informační systéme evidence osob	Ing. Martina Brejchová	Ing. Vladimír Daráni
K05	AIS ECD	Agendový informační systém Evidence cestovních dokladů	Ing. Martina Brejchová	Ing. Vladimír Daráni
K06	AIS EOP	Agendový informační systém elektronických občanských průkazů	Ing. Martina Brejchová	Ing. Vladimír Daráni
K07	FAIS	Formulářový agendový informační systém	Ing. Radovan Pártl	Ing. Helena Šebková
K08	ROB	Registr obyvatel	Ing. Martina Brejchová	Radovan Pártl
K09	RPP	Registr práv a povinností	PhDr. Jan Tretera	Radovan Pártl
K10	RACS	Systém řízení přístupů do základních registrů	Ing. Radovan Pártl	Ing. Helena Šebková
K11	AIS C	Agendový informační systém cizinců	Mgr. Eva Tuhá	Ing. Marie Smejkalová
K12	CIS	Cizinecký informační systém	Ing. Silvie Líznerová	Ing. Marie Smejkalová
K13	VIS	Vízový informační systém	Bc. Miroslav Souček	Ing. Jan Toman
K14	SIS	Schengenský informační systém	Ing. Jaroslav Beránek	Ing. Jan Toman
K15	CRZ	Centrální registr zbraní	ing. Ludmila Nezvedová	Ing. Miloš Chloupek
K16	ITS	Integrovaná telekomunikační síť MV	Ing. Vladimír Velas	Vladimír Dolejš
K17	CMS	Centrální místo služeb	Martin Linhart	Tomáš Vlček
K18	158	Tísňové volání 158	Ing. František Habada	JUDr. Zapletal Milan
V01	AIS PČR	Agendový informační systém Policie České republiky	Ing. Karel Matucha	Ing. Jan Smejkal
V02	PVS	Portál veřejné správy	Ing. Ondřej Menoušek	Ing. Pavel Chyla
V03	EKIS	Ekonimický informační systém	Ing. Miloslav Žila	Ing. Miloslav Žila
V04	AZYL II	Informační systém pro evidenci udělení azylu	Mgr. Žaneta Blažková	Ing. Jana Bednářová
V05	DP-2	IS soc. zabezpečení, výpočet a výplata dávek soc. zabezpečení	Ing. Ladislav Jedlička	Ing. Vladimír Kittler
V06	GINIS	Informační systém elektronické spisové služby	Ing. Tomáš Kalinec	Ing. Jana Bednářová
V07	ISVS	Informační systém o informačních systémech veřejné správy	Ing. Radek Horáček	Ing. Jana Bednářová
V08	Systém SO	Informační systém - registr státního občanství	Mgr. Petr Šťastný	Ing. Vladimír Kittler
V09	IS oSS	Informační systém o státní službě	RNDr. Josef Postránecký	Ing. Miloslav Žila

MINISTERSTVO VNITRA ČESKÉ REPUBLIKY

Bezpečnostní dokumentace (BD) VIS a KII

POVINNÁ BEZPEČNOSTNÍ DOKUMENTACE (vyhláška č. 316/2014 Sb.)	KII	VIS
RESORTNĚ PLATNÁ BEZPEČNOSTNÍ DOKUMENTACE		
Plán rozvoje bezpečnostního povědomí (OBECNÉ BEZPEČNOSTNÍ POVĚDOMÍ)	X	X
Bezpečnostní politika (RESORTU)	X	X
Přehled právních, vnitřních a jiných předpisů a smluvních závazků (RESORT)	X	X
Metodika pro identifikaci a hodnocení aktiv a pro identifikaci a hod. rizik	X	X
Zvládání kybernetických bezpečnostních incidentů	X	X
Zpráva z přezkoumání systému řízení bezpečnosti informací	X	
BEZPEČNOSTNÍ DOKUMENTACE PRO KONKRÉTNÍ SYSTÉM		
Přehled právních, vnitřních a jiných předpisů a smluvních závazků	X	X
Bezpečnostní politika (VIS/KII)	X	X
Zpráva o hodnocení aktiv a rizik	X	X
Prohlášení o aplikovatelnosti	X	X
Plán zvládání rizik	X	X
Strategie řízení kontinuity činností	X	X
Plán rozvoje bezpečnostního povědomí (povědomí k danému VIS / KII)	X	X
Zpráva z auditu kybernetické bezpečnosti (porovnání souladu se ZoKB)	X	
PROVOZNÍ DOKUMENTACE PRO KONKRÉTNÍ SYSTÉM		
Uživatelská příručka	X	X
Příručka systému	X	X
Bezpečnostní směrnice pro činnost bezpečnostního správce systému	X	X

MINISTERSTVO VNITRA ČESKÉ REPUBLIKY

Plánovaný průběh zpracování BD (VIS a KII)

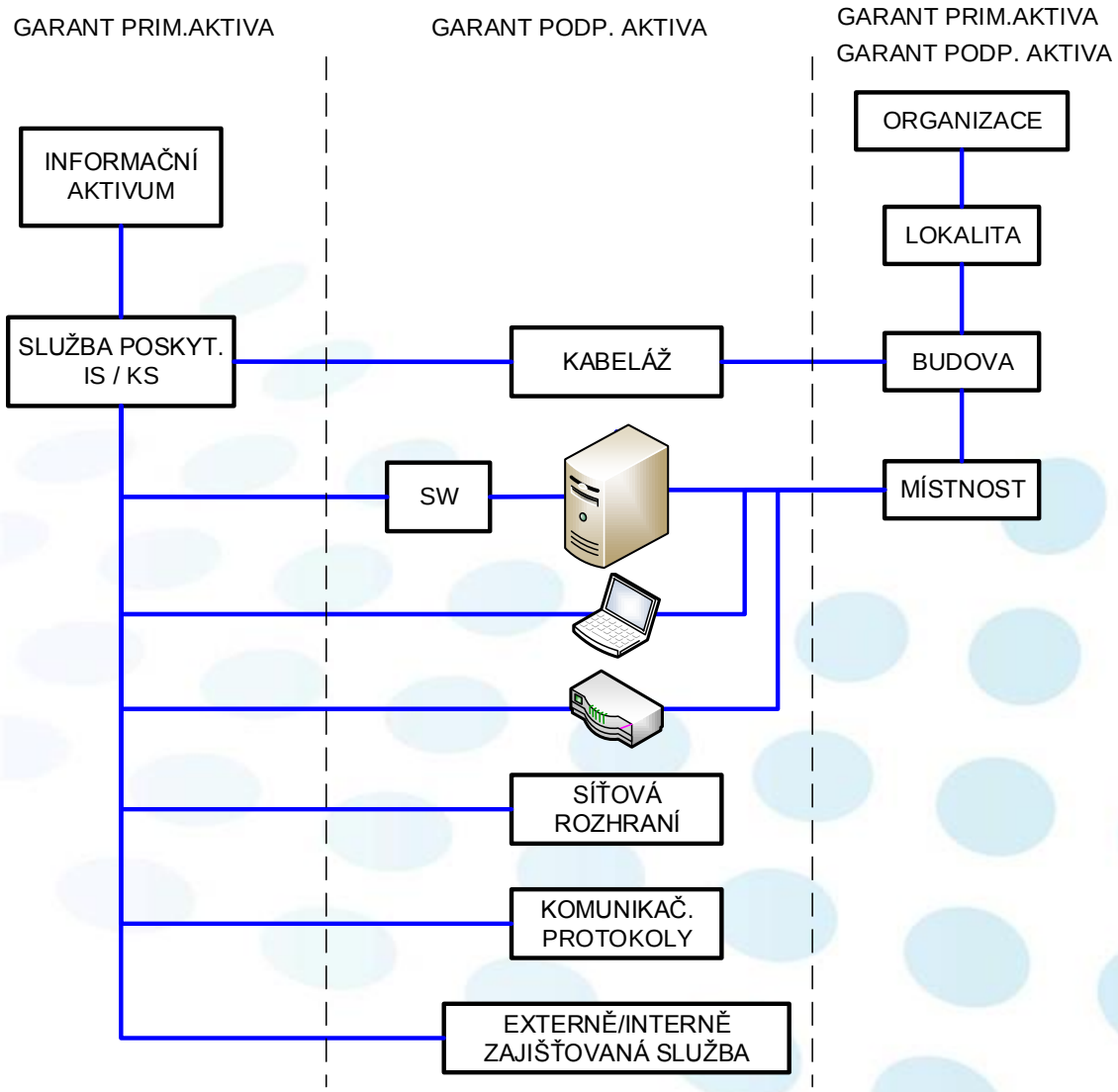
Posloup. kroků	Bezpečnostní dokumentace	KIS	VIS	Poskytne (inf./dok.)	Kdo zprac. BD	Číslo týdne 3	4	5	6	7	8	9	10	11	12	13	Cíl
1	Přehled právních, vnitřních a jiných předpisů a smluvních závazků (VIS/KII)	x	x	GPrA	GPrA/ČP				Kp.								BEZPEČNOSTNÍ DOKUMENTACE SYSTÉMU VIS / KII
2	Bezpečnostní politika (VIS/KII)	x	x	GPrA	GPrA/ČP				Kp.								
3	**Hodnocení aktiv a rizik (proces)**					RAMSES											
3.1	Úvodní jednání -> identifikace aktiv a vytv.modelu	x	x	GPrA	ČPOZ	3h	3h	3h									
3.2	přiřazení hrozeb a zranitelností	x	x						3h	3h	3h						
3.3	stav opatření (doporučeno, atd.)	x	x									3h	3h				
4	Zpráva o hodnocení aktiv a rizik	x	x	GPrA	ČPOZ									Kp.			
5	Prohlášení o aplikovatelnosti	x	x	GPrA	ČPOZ										Kp.		
6	Plán zvládání rizik	x	x	GPrA	ČPOZ										Kp.		
7	Strategie řízení kontinuity činností (VIS/KII)	x	x	GPrA	GPrA/ČP										Kp.		
8	Plán rozvoje bezpečnostního povědomí (VIS/KII)	x	x	GPrA	ČPOZ										Kp.		
9	Zpráva z auditu KB + porovnání souladu se ZoKB (VIS/KII)	x	x	GPrA	Auditor											Kp. Kp.	
Provozní dokumentace		**KIS**	**VIS**	**Poskytne**	**Kdo ul.**		4	5	6	7	8	9	10	11	12	13	
1	Uživatelská příručka	x	x	GPrA	GPrA/ČP				PD								
2	Příručka systému	x	x	GPrA	GPrA/ČP				PD								
3	Bezpeč. směrnice pro činnost bezp. správ. systému	x	x	GPrA	GPrA/ČP				PD								

LEGENDA

- 3h - doba trvání procesu v hodinách
- BD - zpracovaný bezpečnostní dokumentace (BD)
- Kp. - kapitola bezpečnostní dokumentace
- PD - provozní dokument
- → - postup zpracování / zajištění podkladů pro BD
- → - odkaz na dokumentaci BD / PD

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Model aktiv



MINISTERSTVO VNITRA ČESKÉ REPUBLIKY

Hodnocení aktiv

Kategorie dat		Dostupnost												Důvěrnost			Integrita										
		15m	1H	3H	12H	1D	2D	1W	2W	1M	2M	B	T	I	C	O	SE	WE	DM	In	Or	Rc	Nd	Rp	Mr	Tm	Os
DA Informační		**1**	**2**	**2**	**3**	**4**	**5**	**7**	**7**	**9**	**9**	**1**	**1**	**4**	**7**	**10**	**1**	**1**	**6**	**3**	**1**	**1**	**1**	**1**	**1**	**1**	**1**
ID	Informace datové	1	1	1	1	2	2	3	3	4	4	1	1	4	7	10	1	1	6	3	1	1	1	1	1	1	1
IH	Informace hlasové	1	2	2	3	4	5	7	7	9	9	1	1	4	7	10	1	1	1	3	1	1	1	1	1	1	1
DA Managementové		**3**	**4**	**5**	**6**	**7**	**8**	**9**	**9**	**9**	**9**	**6**	**9**	**1**	**4**	**8**	**3**	**5**	**9**	**9**	**2**	**1**	**4**	**1**	**3**	**3**	**2**
PrT	Přenosová trasa	3	4	5	6	7	8	9	9	9	9	5	9	1	1	2	3	5	9	1	1	1	3	1	3	1	2
SprS	Správa sítě Pegas	1	2	3	4	5	6	7	8	9	9	6	9	1	4	8	1	5	9	9	2	1	4	1	1	3	1

Nedostupnost

15m Nedostupnost menší než 15 minut
1H Nedostupnost 1 hodina
3H Nedostupnost 3 hodiny
12H Nedostupnost 12 hodin
1D Nedostupnost 1 den
2D Nedostupnost 2 dny
1W Nedostupnost 1 týden
2W Nedostupnost 2 týdny
1M Nedostupnost 1 měsíc
2M Nedostupnost 2 měsíce

Dopady komunikace

In Vložení falešné zprávy
Or Popření původu
Rc Popření přijetí
Nd Nedoručení
Rp Opakování
Mr Chyba směrování
Tm Monitorování komunikačního prostoru

Důvěrnost

I Neoprávněné prozrazení identifikovatelným osobám
C Neoprávněné prozrazení smluvním poskytovatelům služeb
O Neoprávněné prozrazení cizím osobám

Integrita

SE Chyby menšího rozsahu
WE Chyby většího rozsahu
DM Úmyslná modifikace

MINISTERSTVO VNITRA ČESKÉ REPUBLIKY

Výběr bezpečnostních opatření

➢ U navržených opatření identifikujeme jejich stav:

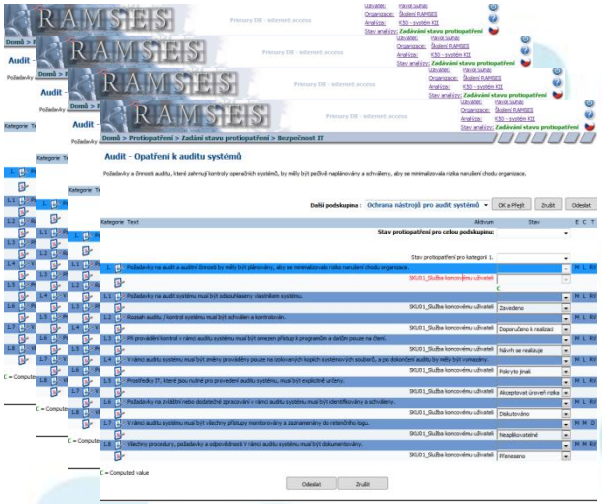
Zadání stavu protiopatření pro bezpečnost IT

Filtr
Stav: (Vše)
Využít právo editora

17%	Identifikace a autentizace	
0%	Řízení logického přístupu	
0%	Účtování / Zaznamenávání událostí	
43%	Audit	
0%	Nástroje auditu	Volba aktiv
91%	Přezkoumání logu událostí	Volba aktiv
100%	Vyšetřování incidentů	Volba aktiv
0%	Opatření k auditu systémů	Volba aktiv
0%	Ochrana nástrojů pro audit systémů	Volba aktiv
0%	Opakované použití objektu	
0%	Testování bezpečnosti	
0%	Integrita softwaru	
0%	Ochrana proti škodlivým programům	
0%	Mobilní zařízení a práce na dálku	
0%	Opatření pro změnu softwaru	
0%	Distribuce softwaru	
0%	Opatření pro vstup / výstup systému	
0%	Opatření pro provoz	
0%	Opatření pro administraci systémů	
0%	Opatření pro programátory aplikací	
0%	Opatření pro údržbu softwaru	
0%	Opatření pro údržbu hardwaru	

ČÍSELNÍK STAVU OPATŘENÍ

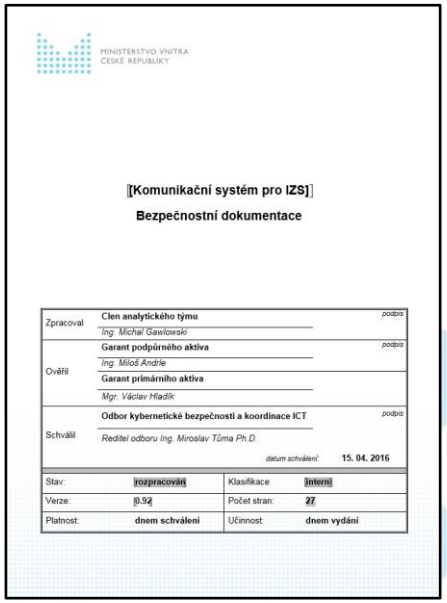
- ZAVEDENO
- DOPORUČENO K REALIZACI
- NÁVRH SE REALIZUJE
- POKRYTO JINAK
- AKCEPTOVAT ÚROVEŇ RIZIKA
- DISKUTOVÁNO
- NEAPLIKOVATELNÉ
- PŘENESENO

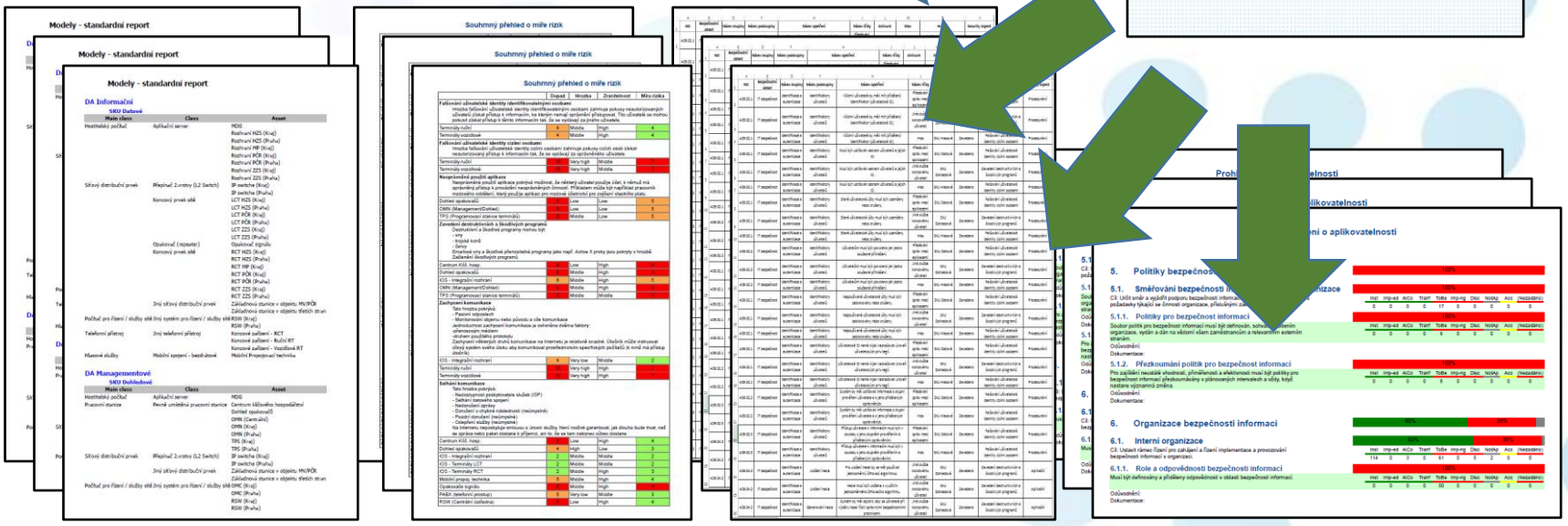


MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Bezpečnostní dokumentace

- **Manažerský souhrn**
  - Garanti / aktiva / vazby
  - Prohlášení o aplikovatelnosti
  - Plán zvládání rizik
  - atd …
- **Přílohy s podrobnostmi**





MINISTERSTVO VNITRA ČESKÉ REPUBLIKY

Dohledové centrum eGovernmentu - DCeGOV

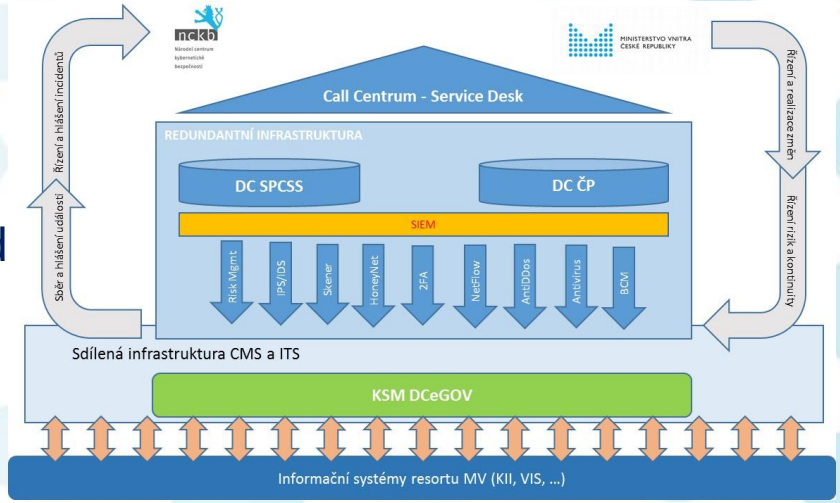
Dohledové centrum eGovernmentu zajišťuje pro resort MV provozní a bezpečnostní dohled, monitoring ICT, řízení jednotlivých událostí a incidentů ICT.

Cíle DCeGOV

- Sběr a vyhodnocování událostí nad IS a infrastrukturou resortu MV
- Identifikace a řešení provozních a bezpečnostních událostí a incidentů
- Zajištění komunikace s NCKB

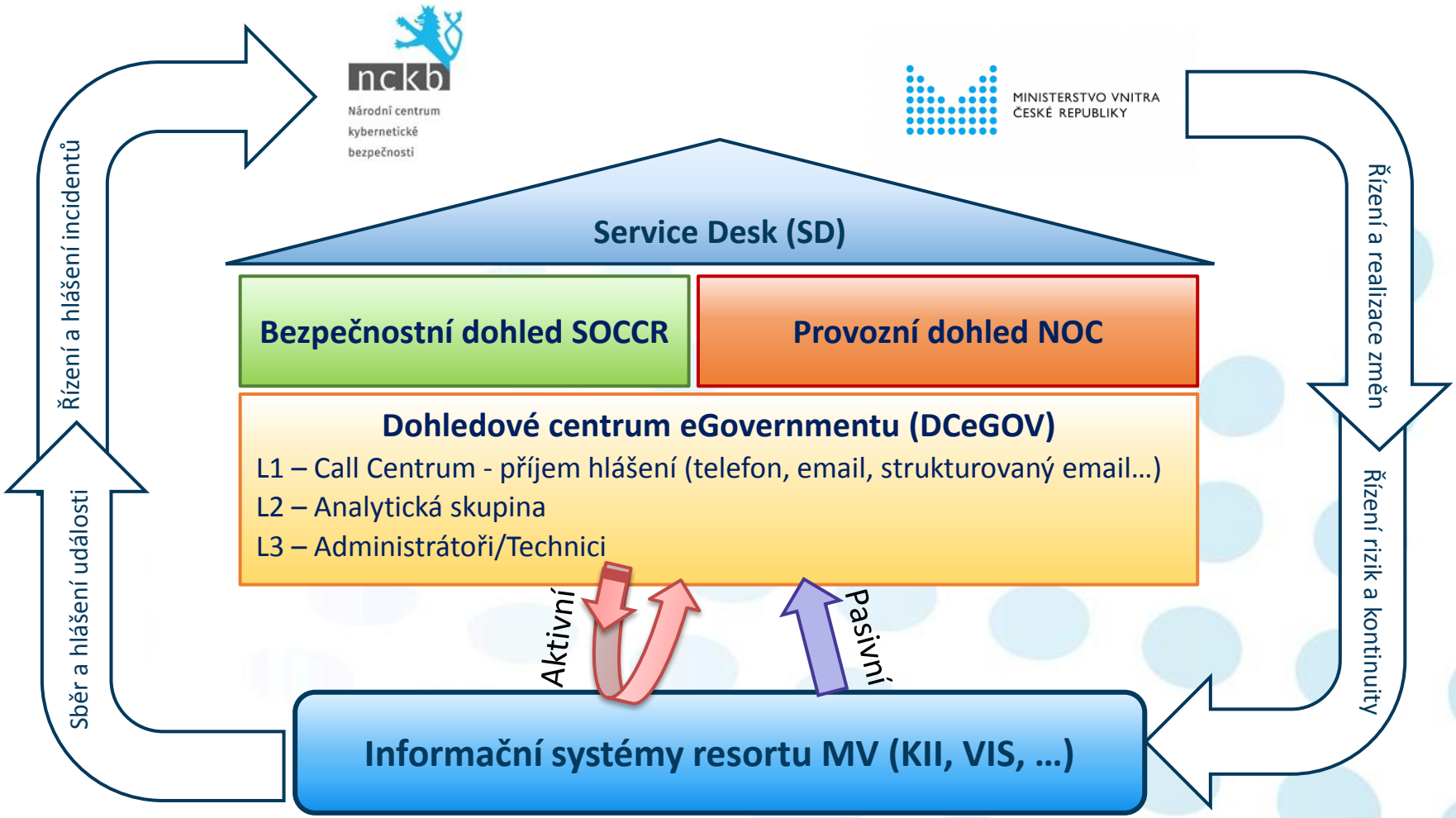
Základní pilíře DCeGOV

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



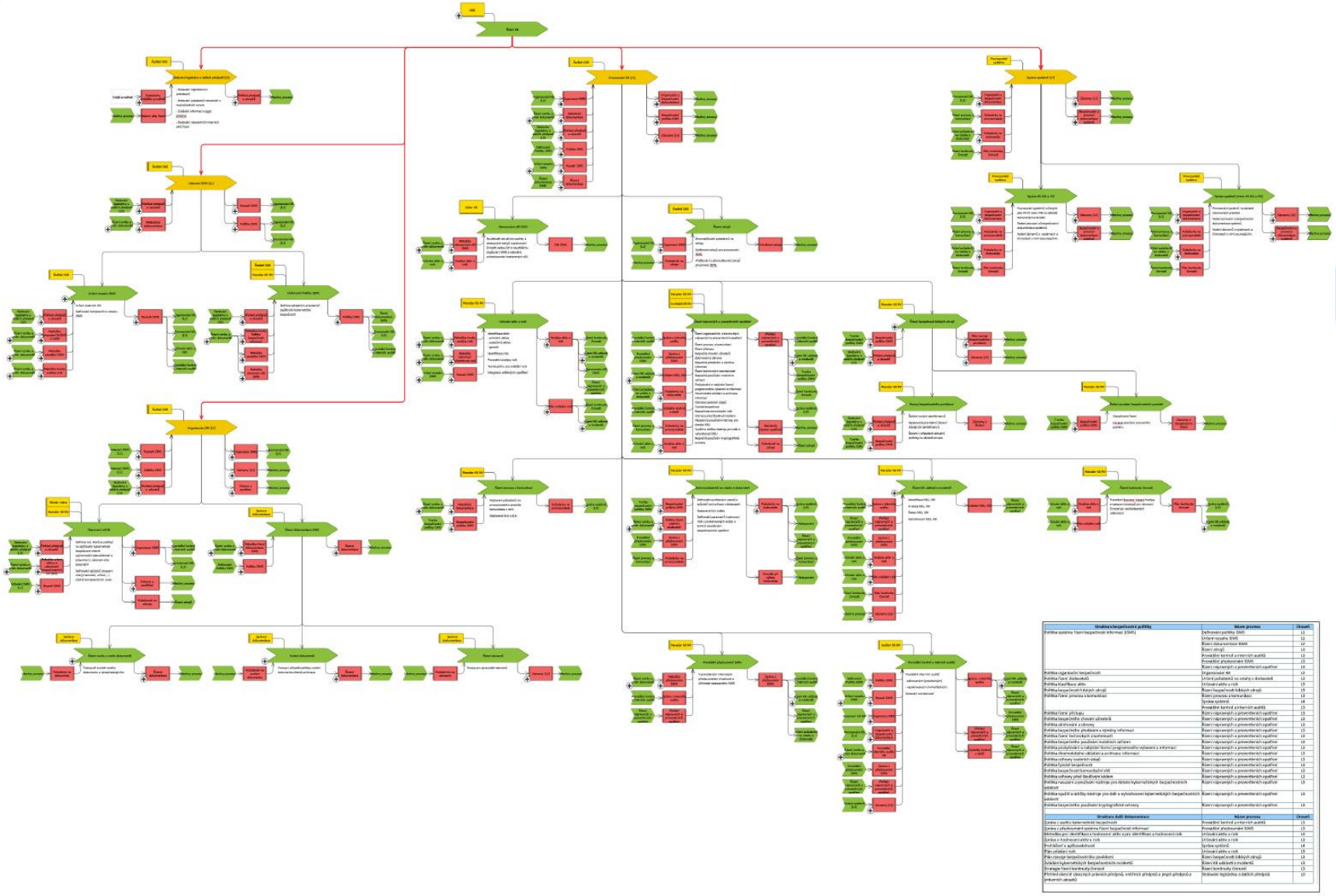
MINISTERSTVO VNITRA ČESKÉ REPUBLIKY

DCeGOV – základní vlastnosti



MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Vyhodnocení a zlepšování ISMS



MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Děkuji za pozornost a Váš čas

Ing. Miroslav Tůma, Ph.D.

odbor Kybernetické bezpečnosti a koordinace ICT

miroslav.tuma@mvcr.cz

GSM: +420 734 267 036