Postupy pro zavedení a řízení bezpečnosti informací

ELAT s.r.o

Lukáš Vondráček

Preambule...

„Prosil bych šroubek M6 – asi takhle tlustej...“

Standardy

- ISO / IEC 27000
- SAS 70 /NIST

  a další ...

1.1 Mezinárodní normy ISMS řady ISO/IEC 27xxx

- ISO 27000 - definuje pojmy a terminologický slovník pro všechny ostatní normy z této série.
- ISO 27001 (BS7799-2) - hlavní norma pro Systém řízení bezpečnosti informací (ISMS), dříve známá jako BS7799 část 2, podle které jsou systémy certifikovány. Poslední revize normy byla publikována v říjnu 2013.
- ISO 27002 (ISO/IEC 17799 & BS7799-1) - norma byla prvně publikována v červnu 2005 jako ISO/IEC 17799:2005. V červenci 2007 došlo k jejímu přejmenování na ISO/IEC 27002:2005, kdy obsah předchozí normy byl zachován. Poslední revize normy byla vydána v říjnu 2013.
- ISO 27003 - návod pro návrh a zavedení ISMS v souladu s ISO 27001.
- ISO 27004 - norma byla publikována v prosinci 2009 pod názvem "Information technology - Security techniques - Information security management - Measurement". Normu přeložila společnost Risk Analysis Consultants.
- ISO 27005 - norma byla publikována v červnu 2008 pod názvem "Information technology - Security techniques - Information security risk management" a následně v červnu 2011 revidována.

1.1 Mezinárodní normy ISMS řady ISO/IEC 27xxx

- ISO 27006 - norma byla poprvé publikována v březnu 2007 pod názvem “Information technology - Security techniques - Requirements for bodies providing audit and certification of information security management systems”.
- ISO 27007 - norma byla publikována v listopadu 2011 pod názvem "Information technology — Security techniques — Guidelines for information security management systems auditing".
- ISO 27008 - norma byla publikována v listopadu 2011 pod názvem "Information technology — Security techniques — Guidelines for auditors on information security management systems controls". Obsahuje doporučení auditorům ISMS a doplňuje ISO 27007.

1.1 Mezinárodní normy ISMS řady ISO/IEC 27xxx

- ISO 27010 - norma byla publikována v dubnu 2012 pod názvem "ISO/IEC 27010:2012 Information technology — Security techniques — Information security management for inter-sector and inter-organisational communications". Poskytuje doporučení pro řízení bezpečnosti informací při interní a mimo firemní komunikaci.
- ISO 27011 - norma byla publikována v roce 2008 pod názvem "ISO/IEC 27011:2008 Information technology — Security techniques — Information security management guidelines for telecommunications organizations based on ISO/IEC 27002". Obahuje doporučení a požadavky na řízení bezpečnosti informací v prostředí telekomunikačních operátorů.
- ISO 27013 - norma byla publikována v říjnu 2012 pod názvem "ISO/IEC 27013:2012 — Information technology — Security techniques — Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1". Norma poskytuje doporučení pro implementaci ISO/IEC 20000 a ISO/IEC 27001.

1.1 Mezinárodní normy ISMS řady ISO/IEC 27xxx

- ISO 27014 - norma byla publikována v první polovině roku 2013 pod názvem "ITU-T Recommendation X.1054 & ISO/IEC 27014:2013 Information technology — Security techniques — Governance of information security". Norma organizacím poskytuje doporučení při návrhu Information Security Governance.
- ISO 27015 - norma byla publikována v listopadu 2012 pod názvem "ISO/IEC TR 27015:2012 Information technology — Security techniques — Information security management guidelines for financial services".Obsahuje doporučení a požadavky na řízení bezpečnosti informací v prostředí finančních institucí (banky, pojišťovny apod.).
- ISO 27016 - norma byla publikována v roce 2014 jako technická zpráva (Technical Report) pod názvem ISO/IEC TR 27016:2014 — IT Security — Security techniques — Information security management – Organizational economics. Poskytuje doporučení pro nastavení bezpečnostního programu s ohledem na předpokládané finanční výsledky.

1.1 Mezinárodní normy ISMS řady ISO/IEC 27xxx

- ISO 27018 - norma byla publikována v srpnu 2014 pod názvem ISO/IEC 27018:2014 —Information technology — Security techniques — Code of practice for protection of Personally Identifiable Information (PII) in public clouds acting as PII processors. Poskytovatelům cloudových služeb dává vhodná bezpečnostní opatření pro zabezpečení soukromí zákazníků.
- ISO 27019 - norma byla publikována jako Technická zpráva (Technical Report) pod názvem "ISO/IEC TR 27019:2013 — Information technology — Security techniques — Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy industry". Norma pomáhá organizacím v energetickém průmyslu interpretovat a aplikovat normu ISO/IEC 27002, aby byla zajištěna bezpečnost jejich systémů pro elektronické řízení procesů.

1.1 Mezinárodní normy ISMS řady ISO/IEC 27xxx

- ISO 27031 - norma byla publikována v březnu 2011 pod názvem "ISO/IEC 27031:2011 Information technology — Security techniques — Guidelines for information and communications technology readiness for business continuity".Obsahuje doporučení pro zajištění kontinuity činností organizace (business continuity).
- ISO 27032 - norma pod označením "Guidelines for cybersecurity" vyšla v červnu 2012, obsahuje bezpečnostní doporučení týkající se kyberprostoru.
- ISO 27033 - soustava norem poskytující doporučení pro implementaci protiopatření vztahujících se k bezpečnosti sítí. Prozatím bylo vydáno pět částí normy.
- ISO 27034 - soustava norem poskytující doporučení pro tvorbu, implementaci a užívání aplikačního softwaru. Byla vydána první část normy.

1.1 Mezinárodní normy ISMS řady ISO/IEC 27xxx

- ISO 27035 - norma byla publikována v roce 2011 pod názvem "Information security incident management". Norma se věnuje řízení incidentů bezpečnosti informací.
- ISO 27036 - soubor norem "Information security for supplier relationships" bude obsahovat doporučení organizacím pro hodnocení a snižování rizik týkajících se outsourcovaných služeb. Prozatím byla vydány první tři části.
- ISO 27037 - norma byla publikována v říjnu 2012 pod názvem "ISO/IEC 27037:2012 — Information technology — Security techniques — Guidelines for identification, collection, acquisition, and preservation of digital evidence". Norma obsahuje doporučení pro zjišťování, sběr, získávání a uchovávání digitálních důkazů.

1.1 Mezinárodní normy ISMS řady ISO/IEC 27xxx

- ISO 27038 - norma byla publikována v roce 2014 pod názvem "ISO/IEC 27038:2014 — Information technology — Security techniques — Specification for digital redaction". Norma obsahuje doporučení pro publikování digitálních dokumentů.
- ISO 27799 - doporučení a požadavky na řízení bezpečnosti informací ve zdravotnických zařízeních.

1.1 Mezinárodní normy ISMS řady ISO/IEC 27xxx

Připravované normy:

- ISO 27009 - noma bude definovat požadavky pro používání ISO/IEC 27001 ve specifických odvětvích.
- ISO 27012 - projekt pro tvorbu normy, která měla poskytovat bezpečnostní doporučení pro státní správu při elektronické komunikaci s občany, byl zrušen.
- ISO 27017 - norma by měla poskytovat doporučení pro zabezpečení cloud computingu.
- ISO 27018 - norma by měla poskytovat doporučení ohledně ochrany osobních údajů v cloud computingu.
- ISO 27023 - norma by měla mapovat a srovnávat poslední vydání norem ISO/IEC 27001 a ISO/IEC 27002 s vydáními předchozími.
- ISO 27039 - norma by měla obsahovat doporučení pro výběr, nasazení a provoz systémů pro detekci a prevenci bezpečnostních průniků (Intrusion Detection and Prevention Systems - IDPS).
- ISO 27040 - norma by měla obsahovat doporučení pro bezpečné ukládání dat.
- ISO 27041 - norma by měla obsahovat doporučení pro zajištění důkazů pro digitální metody vyšetřování.
- ISO 27042 - norma by měla obsahovat doporučení pro analýzu a vyhodnocování digitálních důkazů.
- ISO 27043 - norma by měla obsahovat doporučení pro zásady a postupy při vyšetřování digitálních důkazů.
- ISO 27044 - norma by měla obsahovat doporučení pro SIEM (Security Incident and Event Management).
- ISO 27050 - čtyřdílná norma by se měla zabývat problematikou zkoumání elektronických stop (Electronic discovery).

1.2 Standardy používané v USA

- Federal Information Security Management Act of 2002 („FISMA“)
- Federální zákon o managementu bezpečnosti informací. Vyžaduje, aby každý federální úřad zavedl program bezpečnosti informací a informačních systémů, včetně služeb poskytovaných nebo řízených jiným úřadem nebo dodavatelem.

1.2 Standardy používané v USA

- FIPS PUB 199 Standardy pro kategorizaci bezpečnosti federálních informací a informačních systémů
- FIPS PUB 200 Minimální požadavky na bezpečnost federálních informací a informačních systémů NIST Special Publications 800 series (NIST SP 800 series)

1.2 Standardy používané v USA

- Příručky pro posuzování, výběr a implementaci bezpečnostních opatření v informačních systémech a ICT technologiích

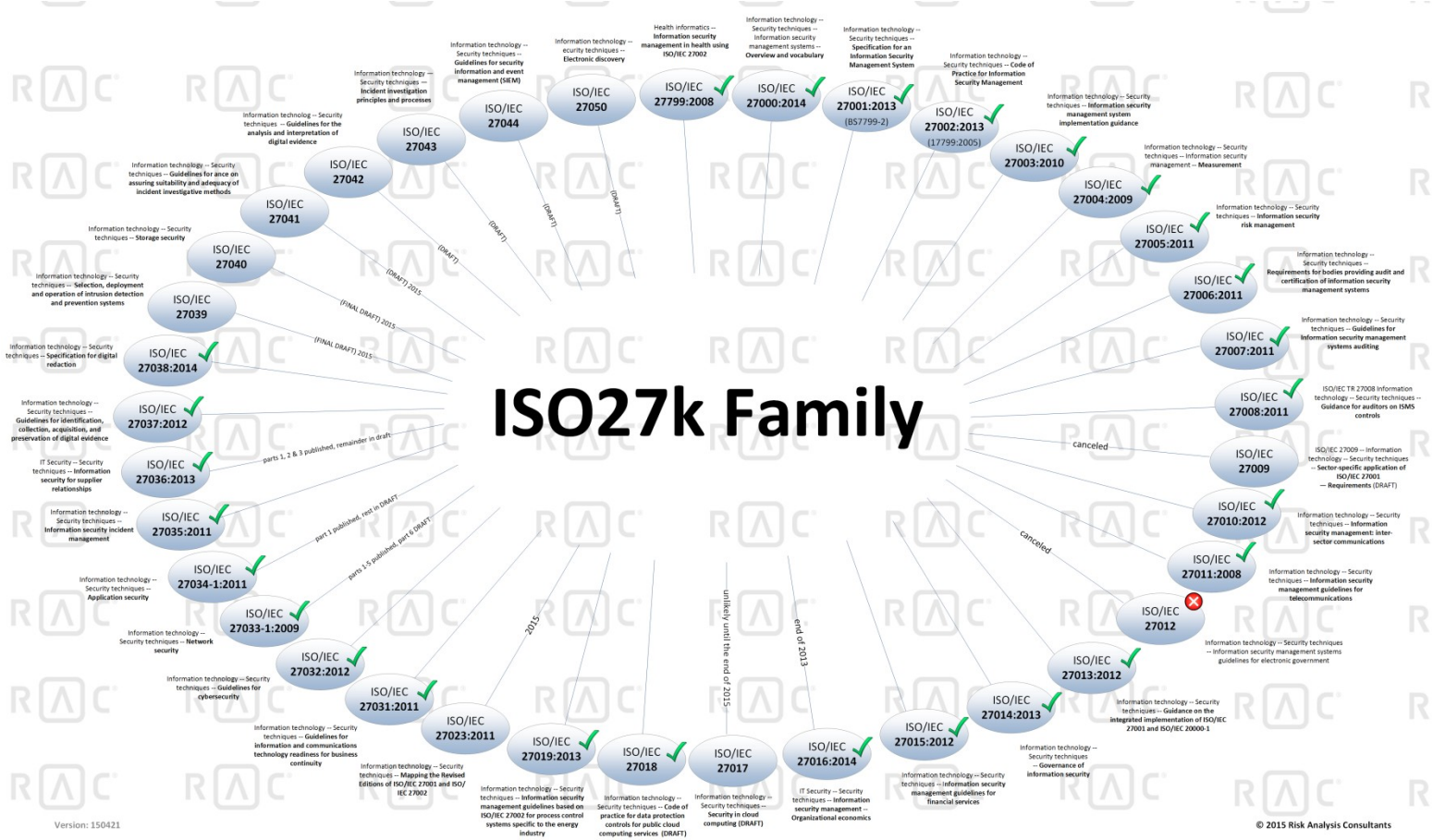
Zdroje: http://csrc.nist.gov/publications/PubsSPs.html

1.3 Standardy používané ve Spolkové republice Německo

- BSI Standard 100-1: Information Security Management Systems (ISMS)
- BSI-Standard 100-2: IT-Grundschutz Methodology
- BSI-Standard 100-3: Risk Analysis based on IT-Grundschutz
- BSI-Standard 100-4: Business Continuity Management

Zdroje: https://www.bsi.bund.de/EN/Publications/BSIStandards/BSIStandards_node.html

Standardy

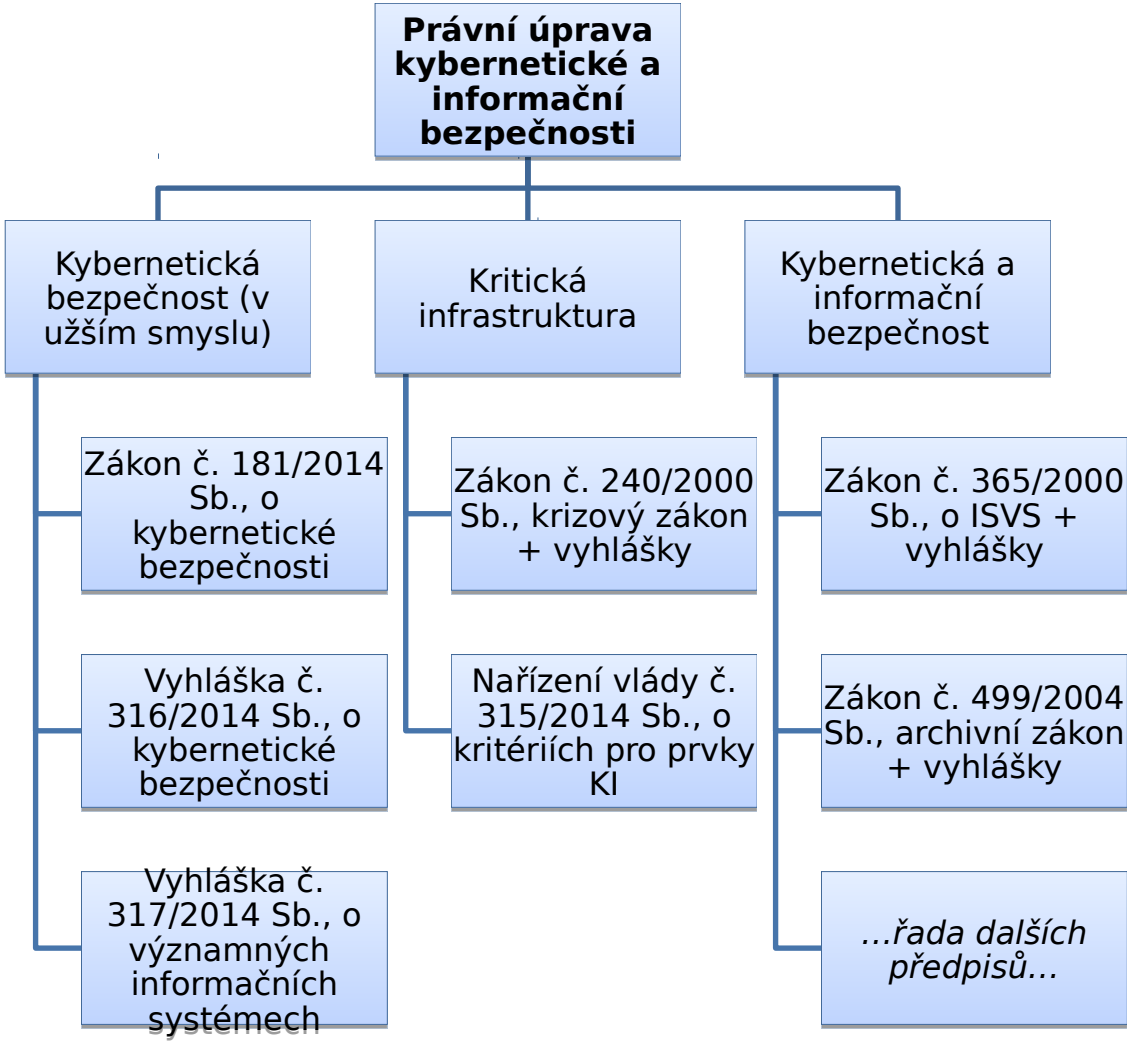

ISO27k Family
ISO/IEC 27000:2014
ISO/IEC 27001:2013 (BS7799-2)
ISO/IEC 27002:2013 (17799:2005)
ISO/IEC 27003:2010
ISO/IEC 27004:2009
ISO/IEC 27005:2011
ISO/IEC 27006:2011
ISO/IEC 27007:2011
ISO/IEC 27008:2011
ISO/IEC 27009
ISO/IEC 27010:2012
ISO/IEC 27011:2008
ISO/IEC 27012
ISO/IEC 27013:2012
ISO/IEC 27014:2013
ISO/IEC 27015:2012
ISO/IEC 27016:2014
ISO/IEC 27017
ISO/IEC 27018
ISO/IEC 27019:2013
ISO/IEC 27023:2011
ISO/IEC 27031:2011
ISO/IEC 27032:2012
ISO/IEC 27033-1:2009
ISO/IEC 27034-1:2011
ISO/IEC 27035:2011
ISO/IEC 27036:2013
ISO/IEC 27037:2012
ISO/IEC 27038:2014
ISO/IEC 27039
ISO/IEC 27040
ISO/IEC 27041
ISO/IEC 27042
ISO/IEC 27043
ISO/IEC 27044
ISO/IEC 27050
ISO/IEC 27799:2008
canceled
canceled
2015
unlikely until the end of 2015
end of 2013
Version: 150421
© 2015 Risk Analysis Consultants

Související normy

- ČSN ISO/IEC 10007:2004 (01 0334) Informační technologie - Systémy managementu jakosti - Směrnice managementu konfigurace.
- ČSN ISO/IEC 15408 Informační technologie - Bezpečnostní techniky -Kritéria pro hodnocení bezpečnosti IT.
- ISO/IEC TR 18044:2004 Information technology - Security techniques - Information security incident management.
- ČSN ISO/IEC 19011:2012 Směrnice pro auditování sytému managementu.
- ČSN ISO/IEC 20000 Informační technologie - Management služeb.
- ČSN ISO/IEC 27001:2014 Informační technologie - Bezpečnostní techniky - Systémy managementy bezpečnosti informací - Požadavky.
- ISO/IEC Guide 73:2002, Risk management - Vocabulary - Guidelines for us in standards.

- a další ...

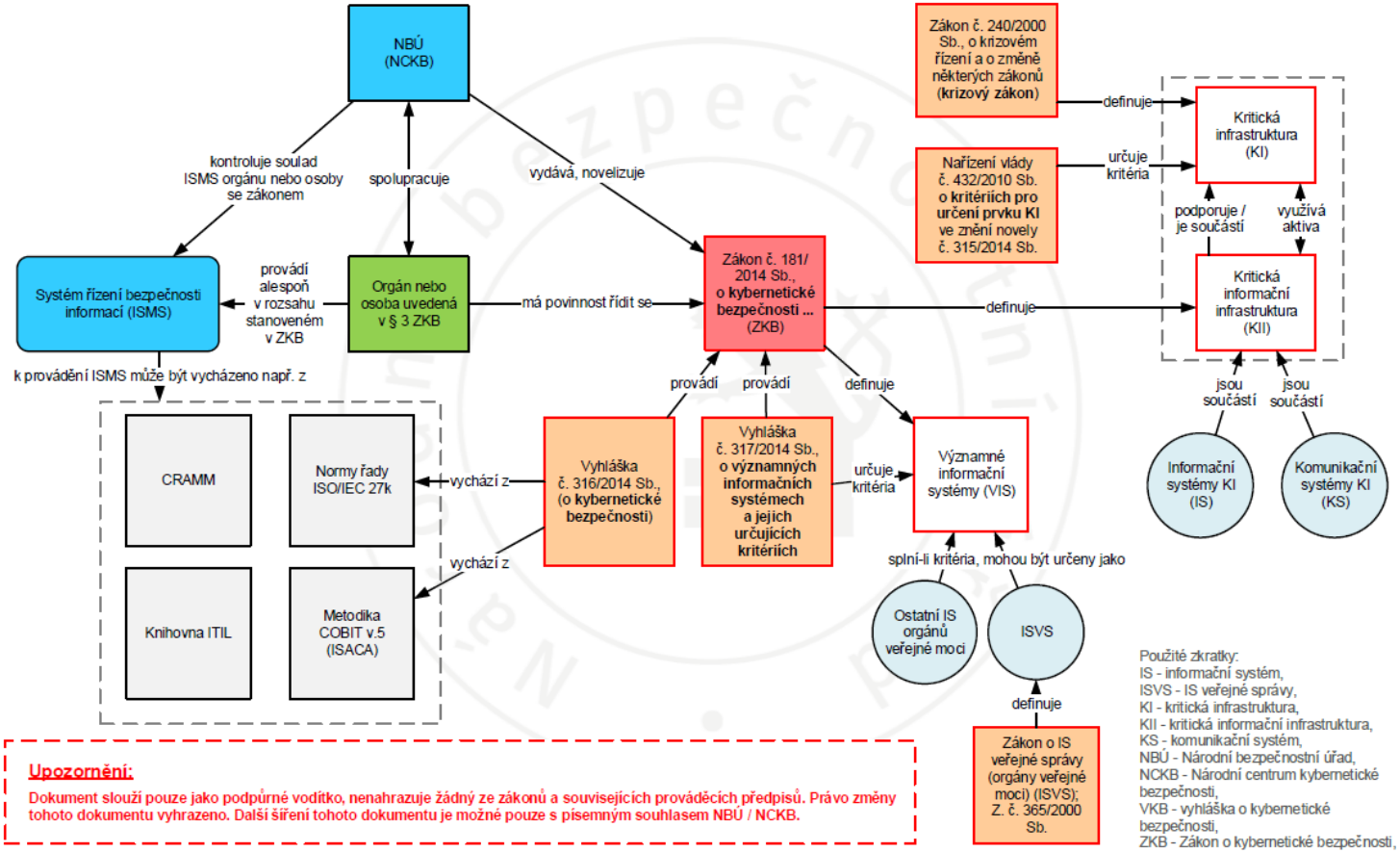
- **Zákon č. 181/2014 Sb., o kybernetické bezpečnosti (ZoKB)**
  - Upravuje práva a povinnosti osob a působnost a pravomoci orgánů veřejné moci v oblasti kybernetické bezpečnosti.
  - Nevztahuje se na informační nebo komunikační systémy, které nakládají s utajovanými informacemi
  - Výjimka zohledňující specifika činnosti zpravodajských služeb a Policie České republiky (§ 33)


Právní úprava kybernetické a informační bezpečnosti
Kybernetická bezpečnost (v užším smyslu)
Kritická infrastruktura
Kybernetická a informační bezpečnost
Zákon č. 181/2014 Sb., o kybernetické bezpečnosti
Vyhláška č. 316/2014 Sb., o kybernetické bezpečnosti
Vyhláška č. 317/2014 Sb., o významných informačních systémech
Zákon č. 240/2000 Sb., krizový zákon + vyhlášky
Nařízení vlády č. 315/2014 Sb., o kritériích pro prvky KI
Zákon č. 365/2000 Sb., o ISVS + vyhlášky
Zákon č. 499/2004 Sb., archivní zákon + vyhlášky
...řada dalších předpisů...

ZÁKON O KYBERNETICKÉ BEZPEČNOSTI

Přehledové blokové schéma k zákonu a jeho prováděcím předpisům

Národní centrum kybernetické bezpečnosti



Upozornění:

Dokument slouží pouze jako podpůrné vodítko, nenahrazuje žádný ze zákonů a souvisejících prováděcích předpisů. Právo změny tohoto dokumentu vyhrazeno. Další šíření tohoto dokumentu je možné pouze s písemným souhlasem NBÚ / NCKB.

Použité zkratky:
IS - informační systém,
ISVS - IS veřejné správy,
KI - kritická infrastruktura,
KII - kritická informační infrastruktura,
KS - komunikační systém,
NBÚ - Národní bezpečnostní úřad,
NCKB - Národní centrum kybernetické bezpečnosti,
VKB - vyhláška o kybernetické bezpečnosti,
ZKB - Zákon o kybernetické bezpečnosti,

Více informací naleznete na www.GovCERT.cz

Pojmy - aktiva

- **Primární** *(dle § 2 písm. c) VyKB)*
  - Informace
  - Služba, kterou dotčený systém zpracovává nebo poskytuje
- **Podpůrná** *(dle § 2 písm. d) a e) VyKB)*
  - Technické vybavení, komunikační prostředky dotčeného systému a jeho programové vybavení
  - Objekty, ve kterých je tento systém umístěn
  - Zaměstnanci a dodavatelé podílející se na provozu, rozvoji, správě nebo bezpečnosti aktiva
  - **procesně-organizační pravidla, postupy a návody určující cíl a podmínky poskytování a využívání ICT služby**

Pojmy - opatření

- **Bezpečnostní opatření poskytne ochranu aktiva před hrozbou tím, že:**
  - Sníží míru zranitelnosti
  - Omezí dopad incidentu
  - Detekuje incidenty
  - Usnadňuje obnovu po incidentu

*V praxi se užívá vhodná kombinace více opatření

Pojmy - incident

bezpečnostní událost= událost, která může způsobit narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací[1)].

bezpečnostní incident = narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací[1)] v důsledku kybernetické bezpečnostní události.

3. Implementace ISMS

a. procesní:

- Bezpečnostní politika ISMS
- Navržená opatření
- Osvěta / školení

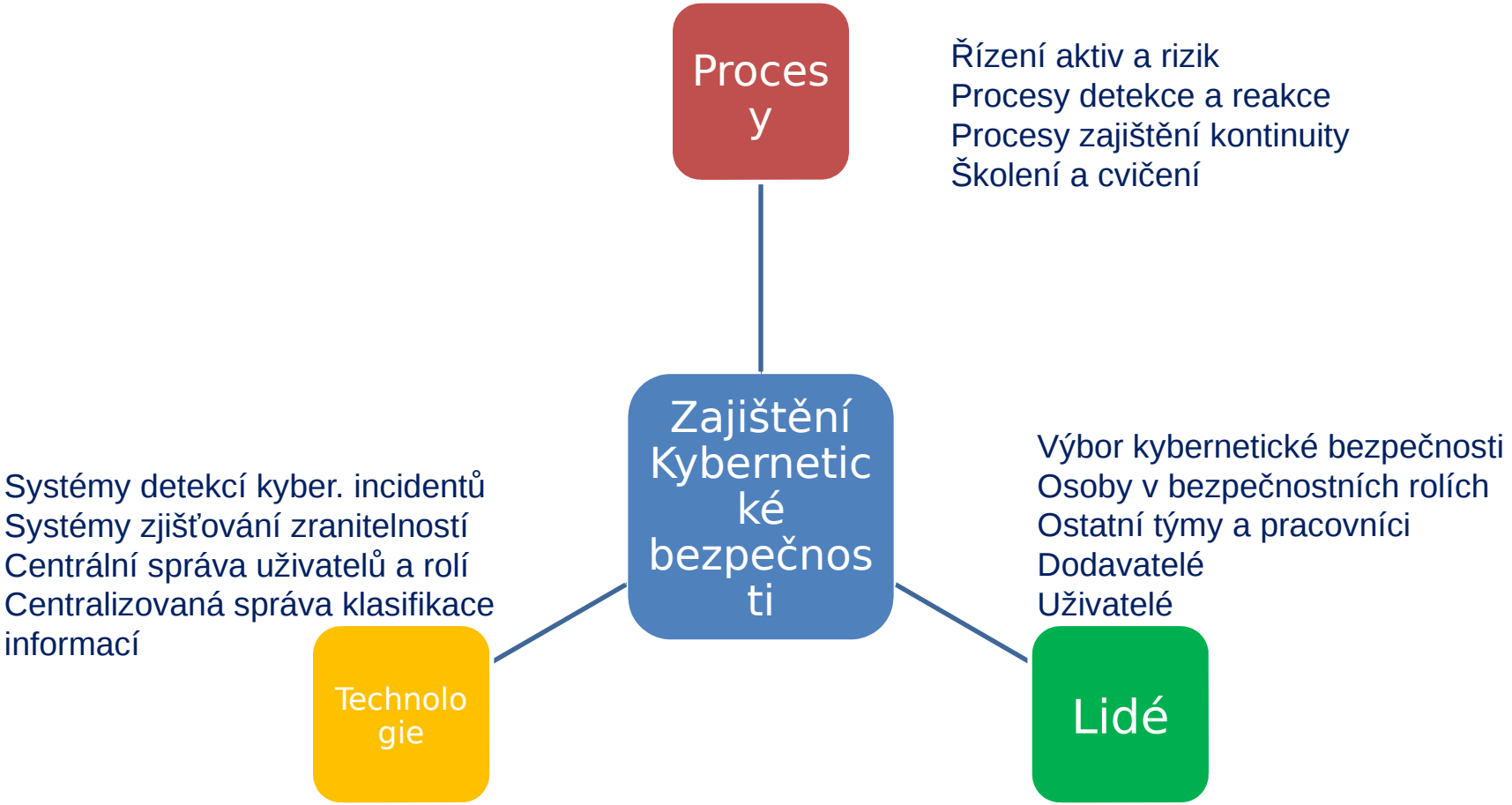
b. systémy dle ZoKB:

- Významné informační systémy
- Informační systémy kritické inf. infrastrukrtury
- Komunikační systémy kritické inf. infrastrukrtury

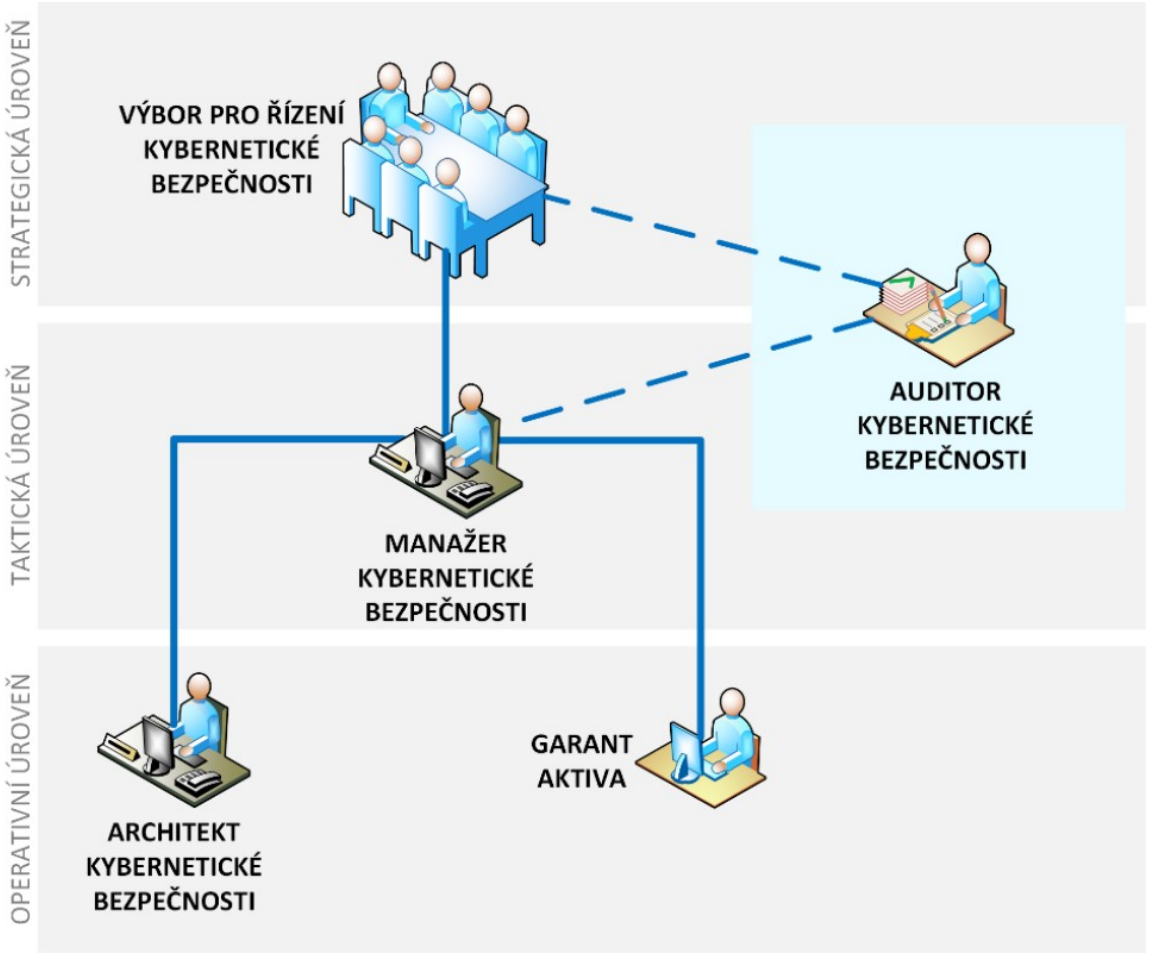
c. Specifikace

- Garant primárního aktiva
- Garant podpůrného aktiva

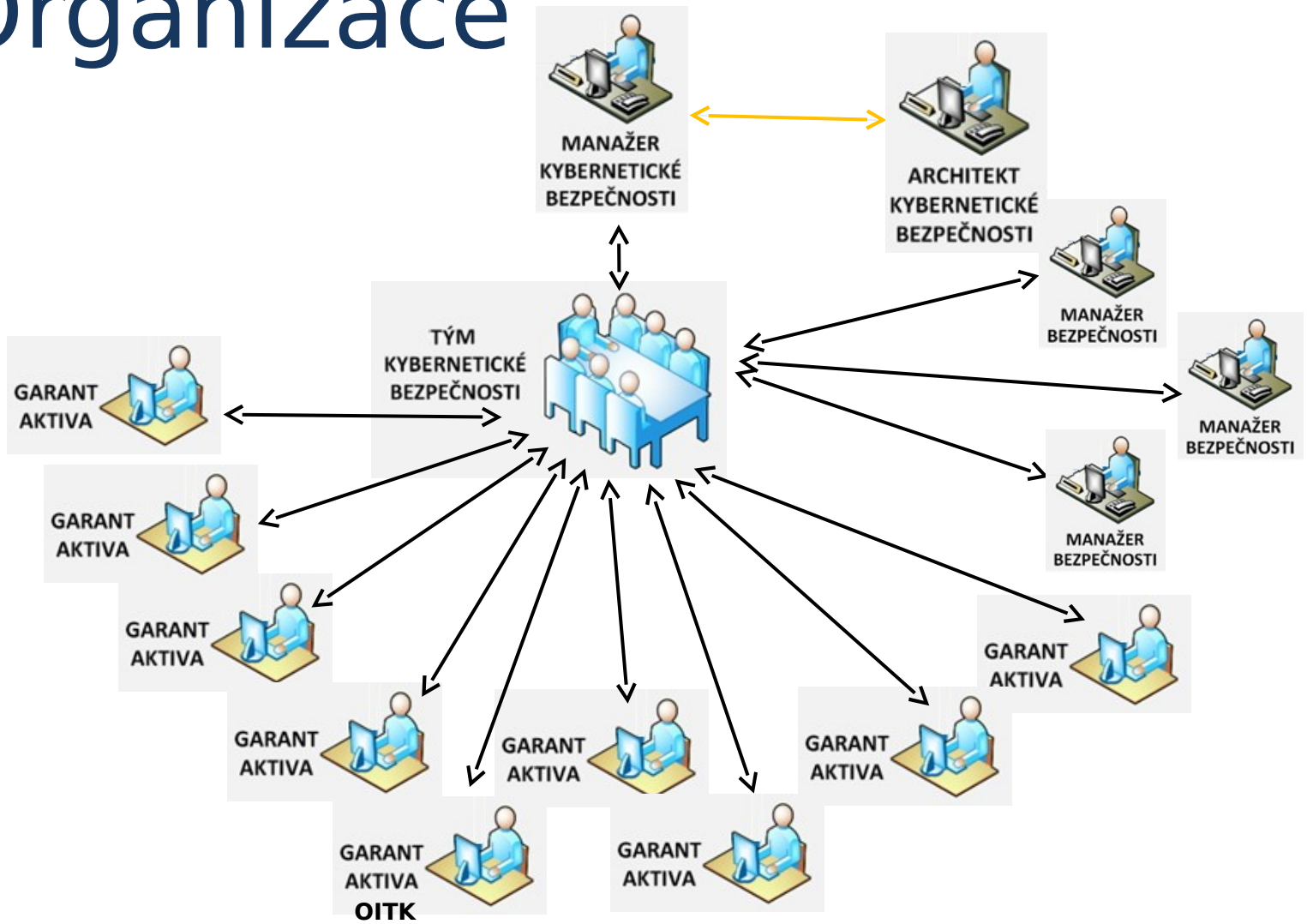
Týká se to všch



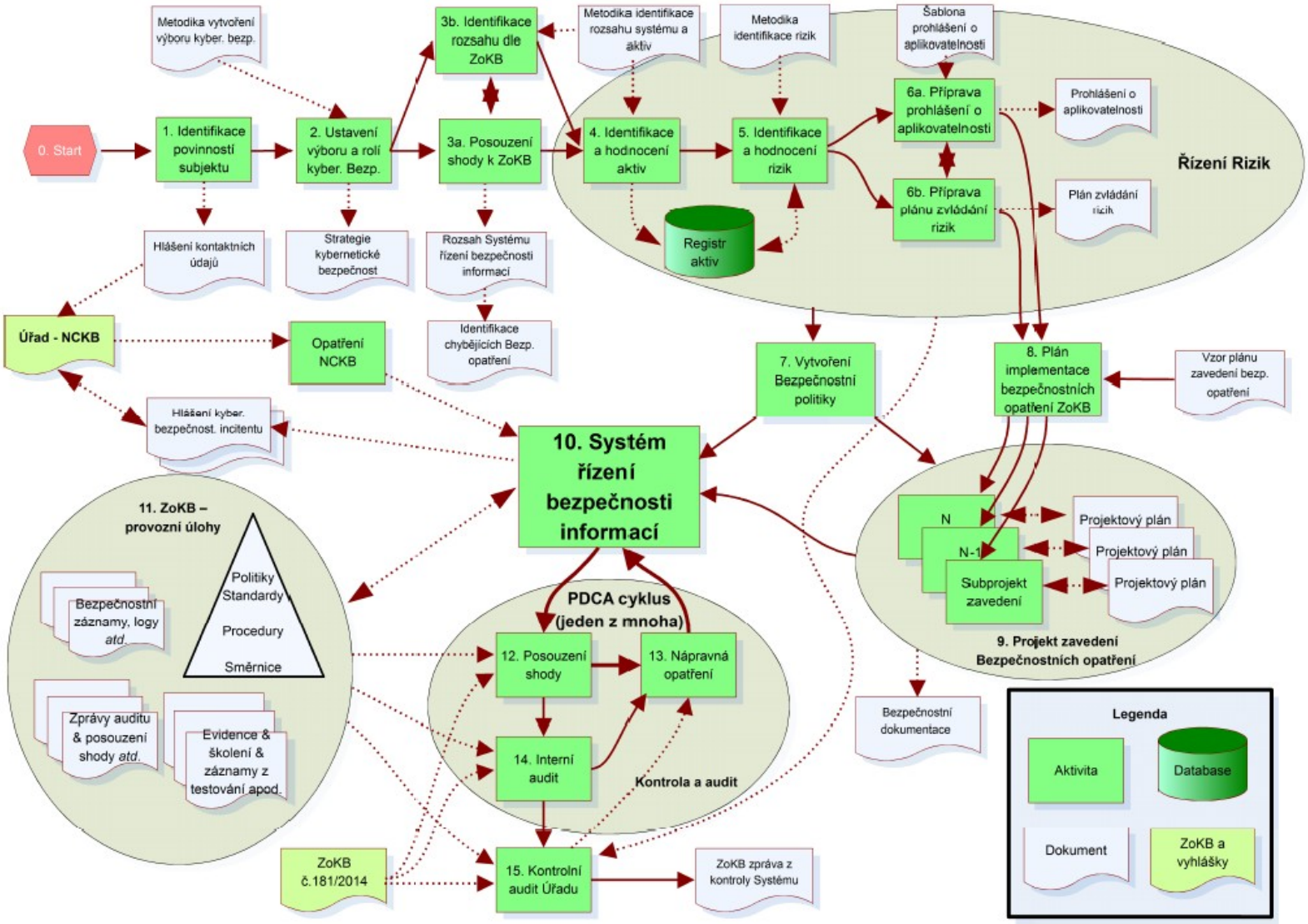
Organizace


STRATEGICKÁ ÚROVEŇ
TAKTICKÁ ÚROVEŇ
OPERATIVNÍ ÚROVEŇ
VÝBOR PRO ŘÍZENÍ KYBERNETICKÉ BEZPEČNOSTI
AUDITOR KYBERNETICKÉ BEZPEČNOSTI
MANAŽER KYBERNETICKÉ BEZPEČNOSTI
GARANT AKTIVA
ARCHITEKT KYBERNETICKÉ BEZPEČNOSTI

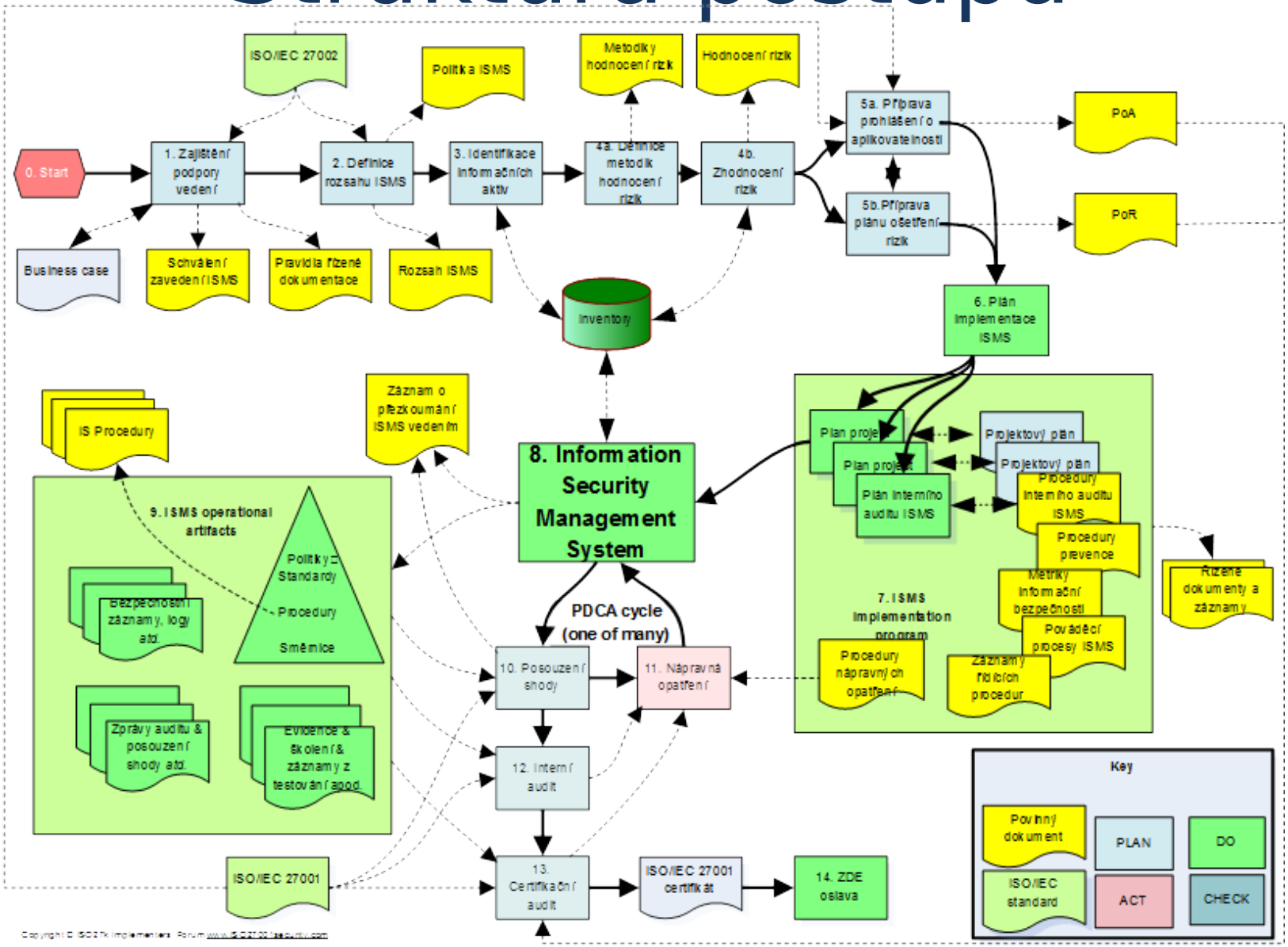
Organizace


MANAŽER KYBERNETICKÉ BEZPEČNOSTI
ARCHITEKT KYBERNETICKÉ BEZPEČNOSTI
TÝM KYBERNETICKÉ BEZPEČNOSTI
MANAŽER BEZPEČNOSTI
MANAŽER BEZPEČNOSTI
MANAŽER BEZPEČNOSTI
GARANT AKTIVA
GARANT AKTIVA
GARANT AKTIVA
GARANT AKTIVA
GARANT AKTIVA
GARANT AKTIVA
GARANT AKTIVA
GARANT AKTIVA
GARANT AKTIVA
OITK

Struktura postupu



Struktura postupu



Postup zavedení

- 1. DOKUMENTACE ZAVÁDĚNÍ SYSTÉMU
- 2. IDENTIFIKACE SUBJEKTU
- 3. URČENÍ VÝBORU A BEZPEČNOSTNÍCH ROLÍ
- 4. STRATEGIE KYBERNETICKÉ BEZPEČNOSTI
- 5. IDENTIFIKACE ROZSAHU ŘÍZENÍ SYSTÉMU BEZPEČNOSTI INFORMACÍ

Postup zavedení

- 6. ASSESMENT
- 7. REVIZE METODICKÉ ZÁKLADNY
- 8.1. IDENTIFIKACE AKTIV
- 8.2. HODNOCENÍ AKTIV
- 9. ANALÝZA RIZIK
- 9.1. ANALÝZA DOPADŮ
- 10. BEZPEČNOSTNÍ POLITIKA
- 11. PLÁN IMPLEMENTACE OPATŘENÍ ZOKB
- 11.1. ŘÍZENÍ KONTINUITY ČINNOSTI - DISASTER RECOVERY PLAN
- 11.2. PLÁN ZVLÁDÁNÍ RIZIK

Postup zavedení

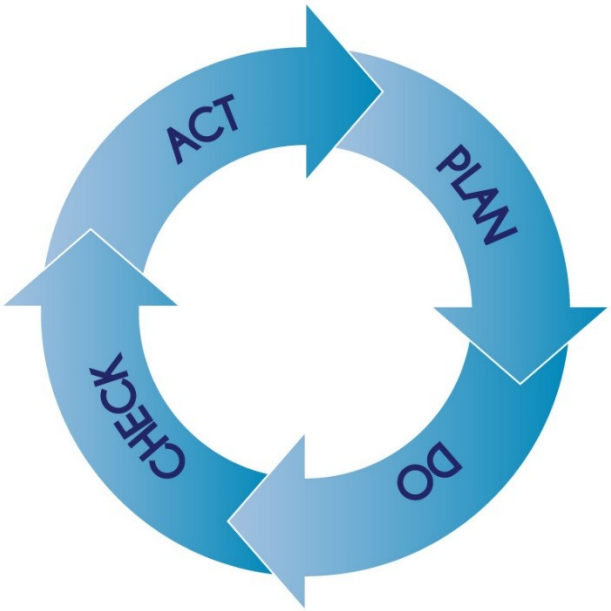
- 12. PRACOVNÍ POSTUPY, ŘÍDÍCÍ DOKUMENTACE
- 12.1. ŘÍZENÍ DOKUMENTACE
- 12.2. ŘÍZENÍ KOMUNIKACE
- 12.3. ŘÍZENÍ DODAVATELŮ
- 12.4. ŘÍZENÍ BEZPEČNOSTNÍCH INCIDENTŮ A UDÁLOSTÍ
- 12.5. PŘEZKOUMÁNÍ SYSTÉMU ŘÍZENÍ BEZPEČNOSTI INFORMACÍ
- 12.6. PROVÁDĚNÍ INTERNÍCH AUDITŮ

- 13. PROHLÁŠENÍ O APLIKOVATELNOSTI

Principy opatření

- Jedná se o systematický soubor vnitřně provázaných aplikovaných postupů a opatření, které jsou
  - plánovány
  - řízeny
  - vyhodnocovány

- a to kontinuálně !!!



Organizační opatření

- Systém řízení bezpečnosti informací (ISMS)
- Řízení rizik
- Bezpečnostní politika
- Organizační bezpečnost
- Stanovení bezpečnostních požadavků pro dodavatele
- Řízení aktiv
- Bezpečnost lidských zdrojů
- Řízení provozu a komunikací
- Řízení přístupu a bezpečné chování uživatelů
- Akvizice, vývoj a údržba
- Zvládání kybernetických bezpečnostních událostí a incidentů
- Řízení kontinuity činností
- Kontrola a audit

Technická opatření

- Fyzická bezpečnost
- Nástroj pro ochranu integrity komunikačních sítí
- Nástroj pro ověřování identity uživatelů
- Nástroj pro řízení přístupových oprávnění
- Nástroj pro ochranu před škodlivým kódem
- Nástroj pro zaznamenávání činností kritické informační infrastruktury a významných informačních systémů, jejich uživatelů a administrátorů
- Nástroj pro detekci kybernetických bezpečnostních událostí
- Nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí
- Aplikační bezpečnost
- Kryptografické prostředky
- Nástroje pro zajišťování vysoké úrovně dostupnosti
- Bezpečnost průmyslových a řídicích systémů

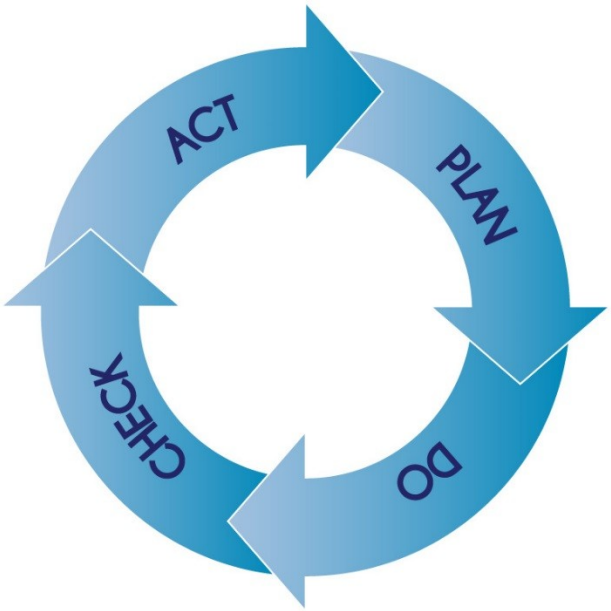
Kontrola a audit

- **Kontrola – audity:**
  - interní – interní audity
    - cílem je najít 100% reálný stav, aby neshody mohly být vyřešeny interně
    - v případě neplnění sjednání nápravy
  - externí
    - cílem je najít shodu s požadavky normy (ZoKB, jiného předpisu)

- **Kontroluje se:**
  - prováděcí dokumentace
  - provádění předepsaných činností v praxi,
  - soulad popisu v dokumentaci a prováděných činností.

Principy neustálého zlepšování

- Kontinuální opakování všech klíčových parametrických aplikací a kontrol



Dotazy

Děkuji za pozornost

Lukáš Vondráček

ELAT s.r.o

vondracek@elat.cz

http://www.elat.cz