Politika informační bezpečnosti

PV 017 ◇ Bezpečnost IT

Jan Staudek
http://www.fi.muni.cz/usr/staudek/vyuka/

Verze : podzim 2019

Politika

- Politika – pravidla řídicí dosažení cílů určenými způsoby
  - ✓ *A policy is a deliberate system of principles to guide decisions and achieve rational outcomes.*

    A policy is a statement of intent, and is implemented as a procedure or protocol.
- Politika organizace
  - ✓ prohlášení o celkovém záměru a směru podnikání formálně vyjádřené vedením organizace
  - ✓ Organizace může mít řadu politik, jednu pro každou z oblastí činnosti, které jsou pro organizaci důležité.
    - Personální politika
    - Politika finančních toků, *Cash flow policy*
    - Politika působení v tržním prostředí
    - Sociální politika . . .
  - ✓ Některé politiky jsou navzájem nezávislé, jiné politiky mají hierarchický vztah nebo se doplňují

Typová struktura dokumentu politiky

- Shrnutí
  - ✓ 1 nebo 2 přehledové věty
- Úvod
  - ✓ stručné vysvětlení důvodů zavedení politiky
- Oblast
  - ✓ popisuje ty části nebo činnosti organizace, které jsou ovlivněny politikou.
  - ✓ případně se odkazují další politiky, které jsou danou politikou podporovány
- Cíle
  - ✓ podrobný popis záměru politiky

Typová struktura dokumentu politiky

- Pravidla, zásady
  - ✓ pravidla týkající se akcí a rozhodnutí k dosažení cílů.
  - ✓ pokud je užitečné identifikovat klíčové procesy související s tématem politiky a pak i pravidla pro provozování těchto procesů
- Odpovědnosti
  - ✓ kdo je odpovědný za opatření (procedury, protokoly, . . .), kterými se plní požadavky této politiky.
  - ✓ příp, i popis organizační struktury a odpovědností osob s určenými rolemi
- Klíčové výstupy
  - ✓ co pro podnikání dosažení výsledků politiky přinese
- Související politiky

Hierarchie bezpečnostních politik

- Pro oblasti bezpečnosti organizace mají být politiky organizovány hierarchicky
- na nejvyšší úrovni je bezpečnostní politika organizace
  - ✓ souhrn bezpečnostních zásad a předpisů, množina pravidel definujících správu a ochranu aktiv organizace
  - ✓ definuje způsob zabezpečení organizace jako celku
  - ✓ od fyzické ostrahy, přes ochranu soukromí, přes bezpečné plnění cílů činnosti organizace až po ochranu lidských práv
- bezpečnostní politika organizace je podporována řadou dalších specifických politik, mj. např.

  politikou informační bezpečnosti, zásady, pravidla zajištění InfSec

  politikou ISMS, zásady, pravidla chování ISMS

  politikou uchování kontinuity činnosti, Business Continuity Plan . . .

Politika informační bezpečnosti a politika ISMS

- Politka InfSec – co proti čemu chránit
  Politika ISMS – jak navrhovat, vyvíjet, provozovat a hodnotit procesy plnící politiku InfSec
- Politika InfSec bývá podporována řadou detailních politik na konkrétních aspekty informační bezpečnosti
  (řízení přístupu, e-mailu, čistého stolu,
  používání síťových služeb, . . .)
- ISO / IEC 27001 (standard ISMS) žádá, aby organizace měla jak politiku ISMS tak i politiku informační bezpečnosti.
  - ✓ konkrétní vztah mezi těmito politikami nestanovuje,
    politiku ISMS žádá ISO / IEC 27001, politiku InfSec ISO / IEC 27002
  - ✓ Obě mohou být vytvořeny jako doplňující se politiky,
    politika ISMS může být podřízena politice InfSec
    nebo politika InfSec může být podřízena politice ISMS.

Politika informační bezpečnosti (IT Security Policy)

- souhrn bezpečnostních zásad a předpisů pro ochranu informačních aktiv
- politika se běžně vyjadřuje neformálně, v přirozeném jazyce
  - ✓ standardizovaná hodnocení informační bezpečnosti budou IT systémy s neformálně vyjádřenou politikou informační bezpečnosti hodnotit jako systémy s nízkou úrovní záruky důvěryhodnosti politiky
- vyšší úroveň záruky za důvěryhodnost politiky poskytuje její semi-formální vyjádření
  - ✓ zvýšení úrovně důvěryhodnosti nelze dosáhnout použitím silnějších bezpečnostních mechanismů a/nebo bohatší škálou opatření
- vyjímečně lze použít i formální logicko–matematické jazyky pro vyjádření politiky (pro omezená prostředí a systémy)
  - ✓ pak lze dosáhnout až vysoké úrovně důvěryhodnosti

Politika informační bezpečnosti (IT Security Policy)

- má vyhovovat celkové bezpečnostní politice organizace
- definuje bezpečné používání IT v rámci organizace
- stanovuje koncepci informační bezpečnosti organizace v horizontu 5-10 let
- stanovuje co jsou citlivá informační aktiva, jejich klasifikaci a odpovědnosti za jejich stav
- stanovuje bezpečnostní infrastrukturu organizace
  - ✓ nutná je nezávislost výkonných a kontrolních rolí
- definuje třídu (sílu) útočníků, vůči kterým se informace organizace zabezpečují
- je nezávislá na konkrétně použitých IT

Bezpečnostní politika systému zpracování informací

- také bezpečnostní politika IS , systémová bezp. politika, . . .
- podle ISO/IEC 27000 – Plán zvládání rizik
  - ✓ detailní normy, pravidla, praktiky, předpisy konkrétně definující způsob správy, ochrany, distribuce citlivé informace a jiných IT zdrojů v oblasti vymezené systémem pro zpracování informací organizace
  - ✓ specifikace bezpečnostních opatření, způsobu jejich implementace a určení způsobů jejich použití zaručujících přiměřenou bezpečnost
  - ✓ musí splňovat politiku informační bezpečnosti organizace
  - ✓ musí respektovat konkrétně použité IT
  - ✓ určuje způsob zabezpečení informací v daném systému v horizontu 2–5 let, tj. definuje
    - konkrétní cíle – co se proti čemu chrání
    - konkrétní opatření
    - použité mechanismy pro implementaci opatření
    - obsahuje havarijní plán a plány činnosti po útocích

Tvorba politiky informační bezpečnosti

- Definice politik InfSec a ISMS je 1. krok při budování ISMS
  - ✓ Tvorba politiky je obvykle iterativní proces
  - ✓ finální verze politiky musí odrážet výsledek ohodnocení rizik daný obsahem prohlášení o aplikovatelnosti (specifikace vhodných opatření) – dokument vzniklý jak výsledek ohodnocení rizik
- politika je konceptuální dokument, který má
  - ✓ respektovat charakteristiky činností, lokalit a aktiv organizace a technologií použitých organizací pro zpracování informací
  - ✓ definovat systém stanovení cílů a strategií řízení organizace a rizik
  - ✓ ustanovit kontext, ve kterém bude působit
  - ✓ ustanovit kritéria pro evaluaci rizik a strukturu procesu hodocení rizik
- politika musí být
  - ✓ schválená vedením organizace
  - ✓ pravidelně přezkoumávaná (např. ročně) a aktualizovaná

Jednoduchý příklad politiky informační bezpečnosti

- Shrnutí
  - ✓ Politika činnosti organizace deklaruje, že veškerá informační aktiva obsažená v oblasti působnosti této politiky InfSec musí být být vždy chráněná proti kompromitaci, proti neautorizované změně jejich integrity a proti omezení jejich dostupnosti, a to bez ohledu na jejich formu, a na to zda jsou sdílená, sdělená nebo skladovaná

Jednoduchý příklad politiky informační bezpečnosti

- Úvod
  - ✓ Informace se mohou vyskytovat ve více formách:
    mohou být vytištěné nebo napsané na papíře,
    uložené v elektronické podobě, přenášené poštou nebo
    pomocí elektronických prostředků, zobrazené na filmy, nebo
    řečené v rozhovoru.
  - ✓ Informační bezpečností se rozumí ochrana informací před širokou
    škálou hrozeb s cílem zajištění kontinuity činnosti organizace,
    minimalizace podnikatelských rizik a
    maximalizace návratnosti investic a obchodních příležitostí

Jednoduchý příklad politiky informační bezpečnosti

- Oblast
  - ✓ Tato politika podporuje politiku bezpečnosti organizace
  - ✓ Vztahuje na celou organizaci

- Cíle
  - ✓ Zvládají se strategická a provozní rizika informační bezpečnosti tak, aby byla pro organizaci akceptovatelná
  - ✓ Chrání se důvěrnost informací o zákaznících, vyvíjených produktech a marketingových plánech
  - ✓ Zajišťuje se integrita protokolových záznamů o činnostech
  - ✓ Veřejné webové služby a služby vnitřních sítí vyhovují stanovenému standardu dostupnosti

Jednoduchý příklad politiky informační bezpečnosti

- Pravidla
  - ✓ Organizace toleruje informační rizika, která nemusí být tolerována v konzervativně řízených organizací, za předpokladu, že se jim rozumí, monitorují se a v případě potřeby se zvládají. Podrobnosti ohodnocování rizik a zvládání rizik se nacházejí v politice ISMS.
  - ✓ Všichni zaměstnanci jsou vědomí a odpovědní za informační bezpečnost v míře relevantní jejich pracovnímu zařazení
  - ✓ Zajišťuje se financování opatření informační bezpečnosti v provozních a projekčních procesech
  - ✓ Při celkovém řízení informačních systémů se bere do úvahy možnost podvodů zneužitím informačních systémů
  - ✓ Vydávají se zprávy o stavu informační bezpečnosti
  - ✓ Sledují se rizika informační bezpečnosti a pokud riziko není akceptovatelné, spouští se odpovídající akce cílené na zvýšení efektivnosti ochran (inovace opatření, inovace ISMS apod.)

Jednoduchý příklad politiky informační bezpečnosti

- ✓ Kritéria pro klasifikaci rizik a přijatelnost rizik stanovuje politika ISMS
- ✓ Netolerují se situace,
  které by mohly vést k rozporu s právem či s předpisy

□ Odpovědnosti

- ✓ Nejvyšší management je zodpovědný za to, že informační bezpečnost je dostatečně řešena v rámci celé organizace.
- ✓ Každý z nejvyšších manažerů je odpovědný za to, že mu podřízení lidé, chrání informace v souladu se standardy organizace.
- ✓ Šéf bezpečnosti radí vrcholovým manažerům, poskytuje odbornou podporu zaměstnancům organizace a zajišťuje vypracovávání zprávy o stavu informační bezpečnosti
- ✓ Každý zaměstnanec při plnění pracovních povinnosti relevantně odpovídá za informační bezpečnost

Jednoduchý příklad politiky informační bezpečnosti

- Klíčové výstupy
  - ✓ Incidenty v oblasti informační bezpečnosti nezpůsobí vážné a nečekané škody a/nebo nebudou vážným narušením služeb a podnikatelských aktivit.
  - ✓ Škody vzniklé podvody zneužitím informačních systémů budou v akceptovatelných mezích.
  - ✓ Zákazníci nebudou nepříznivě ovlivněni obavami o informační bezpečnost

Jednoduchý příklad politiky informační bezpečnosti

- Související politiky
  - ✓ Politika systému řízení informační bezpečnosti (ISMS)
  - ✓ Politika řízení přístupu
  - ✓ Politika čistého stolu a displeje
  - ✓ Politika používání neautorizovaného software
  - ✓ Politika v oblasti získávání souborů software buď prostřednictvím externích sítí nebo přímo z těchto sítí
  - ✓ Politika zálohování
  - ✓ Politika výměny informací mezi organizacemi
  - ✓ Politika možného využívání elektronických komunikačních zařízení
  - ✓ Politika využívání síťových služeb

Jednoduchý příklad politiky informační bezpečnosti

- ✓ Politika používání mobilní výpočetní techniky a komunikace
- ✓ Politika práce z domova
- ✓ Politika používání kryptografických opatření
- ✓ Politika souladu
- ✓ Politika licencování softwaru
- ✓ Politika likvidace software
- ✓ Politika ochrany osobních údajů a soukromí

Tvorba politiky informační bezpečnosti, iniciální dokument

- Deklarace politiky informační bezpečnosti
  - ✓ Maximální rozsah – 2 až 3 strany A4
  - ✓ Odpovědi na klíčové otázky – Pro koho ? Kde ? Co ? Proč ?
  - ✓ Deklaruje vrcholový management, podepisuje „šéf" organizace
- Pro koho bude politika informační bezpečnosti závazná ?
  - ✓ odpovědnost za politiku (za každou revizi) má vrcholový management, musí existovat důkaz, že tomu tak je – zápisy z vedení, . . .
  - ✓ vrcholový management / řídicí výbor musí zvážit a vymezit dopad politiky na konkrétní okruhy zaměstnanců, zákazníků, dodavatelů, . . . vč. přínosů/negativ pro byznys, . . .
  - ✓ vytvářená politika má být maximálně srozumitelná, úplná (samostatně použitelný dokument) a evidentní (nezpochybnitelná), aby se v průběhu implementace nemusely opakovaně odsouhlasovat všechny dílčí alternativy politiky

Tvorba politiky informační bezpečnosti, iniciální dokument

- Kde bude oblast působnosti politiky informační bezpečnosti ?
  - ✓ Nutno přesně vymezit podle org. řádu / geograficky / funkčně / . . .
  - ✓ špatně se prosazuje ITSP v oblasti, která nepodléhá jednotnému řízení
  - ✓ mnohdy nestačí jednostranné vymezení např. na bázi organizační struktury či geografické lokality, do oblasti musí být zahrnuty všechny související kritické funkce
- Co politika informační bezpečnosti chrání ?
  - ✓ specifikace informačních aktiv pokrytých politikou
  - ✓ specifikace relevantních rysů bezpečnosti chráněných aktiv (důvěrnost, integrita, dostupnost, . . .)
  - ✓ stanovení kritérií pro akceptování rizik a identifikace úrovně akceptovatelného rizika

Tvorba politiky informační bezpečnosti, iniciální dokument

- Proč se politika informační bezpečnosti zavádí ?
  - ✓ srozumitelné vyjádření podstaty hrozeb pro organizaci
  - ✓ srozumitelné vyjádření výše škod způsobených narušením bezpečnosti informací (ve finančních i nefinančních pojmech)
  - ✓ ilustrační příklady důsledků incidentů podporující zavedení ISMS

Deklarace politiky informační bezpečnosti, šablona – příklad

- ✓ Vedení organizace . . . . . provozující činnost v oblasti . . . . . ,
  umístěné v . . . . . , se rozhodlo
  chránit důvěrnost, integritu a dostupnost všech svých
  relevantních fyzických a elektronických informatických aktiv
- ✓ Cílem ochran je udržení dobrého stavu konkurenčních výhod,
  hotovostních toků, ziskovosti, vyhovění zákonným a
  smluvním omezením a zachování dobré pověsti organizace.
- ✓ Cíle ochran, požadavky na informace a na bezpečnost informací
  budou vyhovovat cílům organizace v oblasti . . . stanovených
  politikou informační bezpečnosti a jako zmocňovací mechanismus
  pro sdílení informací v elektronických operacích, pro e-komerci a
  pro redukci rizik vázaných na zpracování informací na akceptovatelnou
  úroveň se použije systém řízení informační bezpečnosti (ISMS).
- ✓ Zaměstnanci organizace činí v oblasti . . . jsou povinni plnit požadavky
  bezpečnostní politiky a ISMS, který tuto politiku implementuje.
  Totéž platí pro třetí strany definované v ISMS.
- ✓ Tato politika bude přezkoumávaná alespoň jednou ročně.
- ✓ Odpovědností za bezúečnostní politiku a ISMS je pověřen odbor . . . .

Tvorba politiky informační bezpečnosti

- Tak jak jsou následně získávané dílčí výsledky z hodnocení rizik, deklarace politiky informační bezpečnosti se může rozšiřovat a upřesňovat
- Formulování politiky informační bezpečnosti
  - ✓ Typová šablona politiky informační bezpečnosti pro ISMS je součásti studijních podkladů pro tento předmět

Tvorba politiky informační bezpečnosti

- Politika informační bezpečnosti má pokrývat/obsahovat:
  - ✓ prohlášení, že vedení organizace bude podporovat ISMS a periodicky přezkoumávat politiku informační bezpečnosti
  - ✓ nástin přístupu k řízení rizik (určení metodiky),
  - ✓ kritéra evaluace (vyhodnocení) rizik,
  - ✓ strukturu procesu ohodnocení rizik a
  - ✓ kdo bude za ohodnocení rizik odpovědný
  - ✓ stručnou identifikaci požadavků na soubory opatření zajišťujících vyhovění politice, např.
    - plán(y) reakcí na incidenty,
    - plán zachování činností,
    - plán zálohování dat,
    - plán ochran před viry,
    - politika řízení přístupu,
    - zpravodajství o bezpečnostních incidentech, . . .

pokrač.

Tvorba politiky informační bezpečnosti

pokrač

- ✓ srozumitelnou deklaraci toho, že požadavky na informace a bezpečnost informací budou vyhovovat cílům organizace a že relevantní ISMS bude předmětem trvalého vylepšování
- ✓ jasné vyjádření, že všichni zaměstnanci budou podrobováni školení a trénování v bezpečnostním uvědomění a specialisté budou absolvovat specializovaná školení
- ✓ ideálně by ITSP měla deklarovat vyhovění standardu ISO/IEC 27002 (tj. prohlášení, že se uplatňují standardní opatření),
- ✓ případně by ITSP měla deklarovat cíl získat certifikátu ISO/IEC 27001 (tj. certifikátu, že se uplatňují validní procesy ISMS)

Tvorba politiky informační bezpečnosti

- Náklady na budování politiky InfSec
  - ✓ Vedení organizace má požadovat doložení návrhu politiky
    - odhadem ceny vybudování ISMS a zdrojů pro vybudování ISMS
    - hodnocením a kvantifikací potenciálních zisků
    - návrhem plánu implementace a odpovědnosti za implementaci
- Monitorování postupu budování politiky InfSec
  - ✓ Klíčové okamžiky pro přezkoumání postupu tvorby politiky jsou
    - vypracování návrhu Prohlášení o aplikovatelnosti (specifikace vhodných opatření) v rámci ohodnocování rizik
    - implementace iniciální sestavy procedur aplikujících opatření identifikovaná v Prohlášení o aplikovatelnosti
    - provedení prvního auditu ISMS
    - následně pak ročně, v termínech pravidelného přezkoumávání ISMS, určených v politice informační bezpečnosti

XXX tipů pro tvorbu politiky informační bezpečnosti

- Detailní výklad tipů viz dodatek k této přednášce
- Bezpečnostní politika je nejefektivnější,
  když si ji organizace napíše sama
- Politika informační bezpečnosti by měla být klíčovým
  faktorem při všech rozhodnutích o činnosti organizace,
  není pravda, že ovlivňuje činnost pouze IT oddělení
- Zaměstnanci musí být školení pro dodržování bezpečnostní
  politiky
- Bezpečnostní politika nebude organizaci chránit před všemi
  možnými hrozbami.
- Účinná bezpečnostní politika je
  bezpečnostní politika, která se trvale aktualizuje a reviduje

XXX tipů pro tvorbu politiky informační bezpečnosti

- Bezpečnostní politika má zahrnovat sledování výkonu.
- Co nemůžete obhájit / dokázat u soudu,
  není ani spolehlivé ani užitečné pro bezpečnost.
- Všichni musí dodržovat bezpečnostní politiky nebo
  čelit důsledkům
- Zaměstnanci potřebují uvolnění.
- Bezpečnostní politika je předmětem k diskusi.
- Účinnost a přijatelnost bezpečnosti
  jsou dva neoddělitelné faktory.
- Bezpečnostní politika musí být jasná, čtivá, srozumitelná
- Předpisy a dosažení souladu s nimi jsou nutné zla
- Když jste na pochybách, konzultujte standardy

Vybrané bezpečnostní zásady

- *Separation of duty* – separace odpovědností
  - ✓ kontrolu (audit) správnosti provedení akce X nesmí provádět osoba současně pověřená exekutivním výkonem (provedením) akce X
- *Dual control* – dublování autorizace
  - ✓ zpřístupňování a konfigurování systémů vysoce citlivých z hlediska bezpečnosti není povolené provádět jediné osobě individuálně (princip – ,,musí u toho být alespoň dva'')
- Mechanismy dublování autorizace
  - ✓ dělení kryptografických klíčů na části a přidělení jednotlivých částí osobám pověřeným relevantními rolemi
  - ✓ přidělení iniciálních hodnot kryptografických klíčů osobám pověřeným relevantními rolemi a vypočítání aktuální hodnoty klíče pomocí XOR jejich hodnot
  - ✓ vyžadování současné autentizace více osob, . . .

Mechanismy odpovědnosti/auditu (*accounting*, *audit*)

- bezpečný systém obvykle obsahuje protokolovací podsystém, který zaznamenává všechny události, které nějakou formou souvisí s bezpečností
- Protokolový záznam musí být odolný proti falšování/porušení neutorizovaným činitelem běžícím v systému
  - ✓ příklad zajištění:

    vypočítávání a doplňování MAC záznamů pomocí klíčů uchovávaných v nějakém zabezpečeném systému
- Součástí bezpečnostní politiky systému musí být předpis o formě vyhodnocování protokolovaných záznamů o událostech, které nějakou formou souvisí s bezpečností

Management/správa bezpečnosti

- Požadavek na správné (bezpečné) provozování systému požaduje kontinuální provádění správy (řízení) bezpečnosti
- Mezi řídicí úkony z hlediska bezpečnosti mj. patří
  - ✓ zajišťování inovací systému doplňováním nových funkcí
  - ✓ bezchybné detekování dosud neidentifikovaných zranitelností systému
- Důležitou komponentou nepřetržité správy je auditní činnost zabezpečovaná rolemi nezávislými na exekutivě bezpečnosti a na navrhovatelích bezpečnostního řešení
  - ✓ typická náplň činnosti kontrolního útvaru
  - ✓ kontrolní útvar si může ponechat odpovědnost a výkon auditu zajišťovat outsourcingem

Kategorizace forem správy bezpečnosti

- Správa chyb a závad
  - ✓ idnetifikace chyb a závad v aplikačním systému a ve způsobu jeho používání (vč. např. penetračního testování – testování průniků)
- Řízení konfigurace a změnové řízení
  - ✓ administrativa změn v aplikačním systému
- Řízení auditu a protokolování událostí souvisejících s bezpečností
  - ✓ audit objasníme na následujících průsvitkách podrobněji
- Řízení výkonu
  - ✓ monitorování a hodnocení zpracovávatelského/komunikačního výkonu
- Řízení bezpečnostního programu
  - ✓ řízení provozu systému podle definovaných procedur

Účel bezpečnostního auditu

- Hlavní cíle auditu
  - ✓ kontrola, zda byly bezpečnostní procedury definované správně
  - ✓ detekce neošetřených ,,bezpečnostních děr'', zranitelností nepokrytých adekvátními bezpečnostními opatřeními
- Další smysl auditu
  - ✓ audit procedur po narušení bezpečností s cílem zjištění jak k porušení došlo a kdo je za porušení odpovědný
- Role a nezávislost auditora
  - ✓ audit provádí role plně nezávislá na bezpečnostní exekutivě
  - ✓ žádný auditor nesmí současně pracovat jako bezpečnostní správce či bezpečnostní manažer, architekt apod. (separace odpovědností)
- Procedury / postupy auditu se definují jakou součást procedur správy a provozu systému
  - ✓ auditor musí být schopný audit vykonat bez spoléhání se na radu ,,jak audit dělat'' od monitorovaných entit

Politiky a systém řízení informační bezpečnosti

- Většina organizací vytváří
  politiku informační bezpečnosti
  podle standardu ISO/IEC 27002
  - ✓ Politika správy informační bezpečnosti založená na řízení rizik
  - ✓ Použití standardu ISO/IEC 27002 byly věnované vesměs všechny dosavadní přednášky

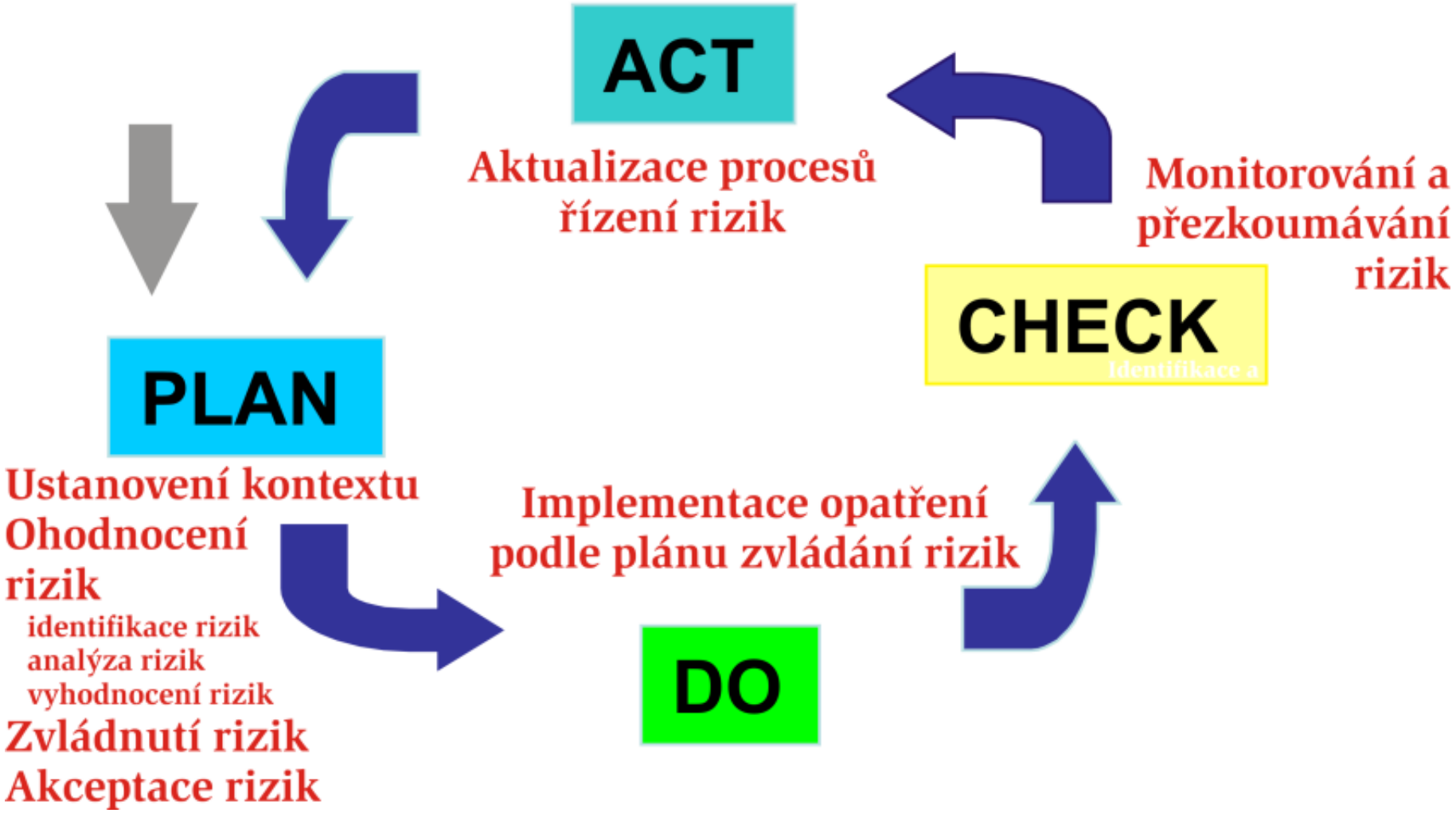
Politiky a systém řízení informační bezpečnosti

- Důvěryhodná bezpečnostní politika zpracování informací je základní kámen systému řízení informační bezpečnosti (*Information Security Management System*, ISMS).
- Cílem ISMS je zajistit trvalou aktuálnost politiky informační bezpečnosti a trvalou úroveň zabezpečení informací
  - ✓ Politika ISMS je buďto nadřazena politice informační bezpečnosti nebo je její přímou součástí
  - ✓ Standard definující ustavení, zavádění, provozování, monitorování, udržování a zlepšování ISMS v organizaci – ISO/IEC 27001
  - ✓ Použití standardu ISO/IEC 27001 bude věnovaná následující přednáška

Politiky a systém řízení informační bezpečnosti

- Základní ideje ISMS:
  - ✓ Bázová idea: Model *Plan-Do-Check-Act*, PDCA – cyklický proces:
  - ✓ Plan (zavedení ISMS, projekt a detailní návrh ISMS) $\mapsto$
    $\mapsto$ Do (implementace ISMS) $\mapsto$
    $\mapsto$ Check (sledování, monitorování, měření efektivnosti ISMS) $\mapsto$
    $\mapsto$ Act (definice vylepšení ISMS) $\mapsto$
    $\mapsto$ Plan . . .
  - ✓ podpora pochopení požadavků na informační bezpečnost organizace a potřeb pro stanovení politiky a cílů informační bezpečnosti
  - ✓ zavedení a provozování opatření pro řízení informační bezpečnosti v kontextu s řízením celkových rizik činností organizace
  - ✓ monitorování a přezkoumání výkonnosti a účinnosti ISMS
  - ✓ neustálé zlepšování založené na objektivním měření.

Příklad – začlenění procesů řízení rizik cyklu PDCA ISMS



Politika dle zákona o kybernetické bezpečnosti

- Struktura politiky informační bezpečnosti dle zákona o kybernetické bezpečnosti
  viz dodatek k této přednášce