# Řízení informační bezpečnosti

PV017

**Kamil Malinka**
(využity materiály Doc. Staudka a konzultace Prof. Matyáše)
Verze: podzim 2023

# Osnova

- Řízení informační bezpečnosti v organizaci: Management, role a odpovědnosti
- ISMS - Systém řízení informační bezpečnosti
- Projekt implementace ISMS

# Řízení informační bezpečnosti v organizaci: Management, role a odpovědnosti

Řízení informační bezpečnosti PV017

**Kamil Malinka**
(využity materiály Doc. Staudka a konzultace Prof. Matyáše)
Verze: podzim 2024

# Management organizace (z pohledu informační bezpečnosti)

- Správní rada - výkonný management + dozorčí rada
- Nejvyšší výkonný management (*Board of Directors*)
  - *Chief Executive Officer* (CEO), výkonný (generální) ředitel
  - *Chief Financial Officer* (CFO), finanční ředitel
  - *Chief Operating Officer* (COO), provozní/obchodní ředitel
- Střední výkonný management (*Board of Directors - 1*)
  - *Chief Information Officer* (CIO), ředitel odboru informačních technologií
  - ***Chief Information Security Officer*** (CISO), ředitel odboru (manažer) informační bezpečnosti,
  - Ředitelé dalších odborů, poboček, částí, … organizace
- Řídící výbor (informační bezpečnosti), příp. samostatný architekt informační bezpečnosti pokud není výbor ustavený
- Lokální správci (informační bezpečnosti)
- Administrátoři systémů
- Auditoři

# Zásady řízení informační bezpečnosti organizace 1/2

- **Informační bezpečnost se zavádí v rámci celé organizace**
  - Aktivity v oblasti informační bezpečnosti jsou plně integrované do procesů organizace
  - Aktivity týkající se fyzické a logické bezpečnosti mají být úzce koordinovány
  - Odpovědnost za informační bezpečnost a za její sledovatelnost má být promítnuta do všech činností organizace
- **Zavedení informační bezpečnosti vychází z výstupů procesů řízení rizik**
  - Určení, jak silné a jak nákladné zabezpečení je smysluplné
  - Založeno na ochotě organizace riskovat, tj. na určení akceptovatelných velikostí ztrát (finančních, konkurenčních výhod, odpovědnostních rizik, z provozních poruch, …)
- **Investiční strategie informační bezpečnosti je dána podnikatelskými cíli organizace**
  - Je nutná harmonizace podnikatelských a bezpečnostních požadavků

# Zásady řízení informační bezpečnosti organizace 2/2

- **Musí být zajištěna shoda s interními a externími požadavky**
  - Soulad s příslušnými povinnými právními a správními předpisy, jakož i se smluvními závazky a případnými dalšími vnějšími či vnitřními požadavky
- **Hodnocení výkonnosti informační bezpečnosti musí sledovat cíle podnikatelských činností**
  - Vč. cílů budoucích
  - Nelze hodnotit a zkoumat efektivitu a účinnost pouze bezpečnostních opatření, nutno provázat s měřením a hodnocením i podnikatelské výkonnosti
- **Musí se podporovat prostředí s pozitivním přístupem k informační bezpečnosti**
  - Lidské chování je jedním ze základních prvků podporujících dosažení odpovídající úrovně informační bezpečnosti
  - Takovou kulturu podpoří poskytování programů bezpečnostního vzdělávání, odborné přípravy a zvyšování povědomí v informační bezpečnosti

# Odpovědnosti řídícího výboru informační bezpečnosti

- Je ustanovený nejvyšším managementem organizace
- Jedná se o fórum členů napříč funkční strukturou organizace, (přirozeně dostatečně odměňovaných za vysokou odpovědnost)
- Informační bezpečnost má být koordinovaná představiteli různých částí organizace působících v relevantních rolích a pracovních funkcích
- Člen výboru pověřený péčí o celkovou architekturu informační bezpečnosti - **bezpečnostní architekt**
- Ve velkých organizacích může působit více manažerů informační bezpečnosti, CISO (v každé části organizace jeden), **řídící výbor informační bezpečnosti má však být unikátní**
- Zasedání 2x-4x ročně, vydávají se řádné zápisy z jednání
- Závěry zasedání výboru projednává výkonný management

# Řídící výbor - aktivity 1/2

- Např.
  - Stanovení cílů informační bezpečnosti v organizaci
  - Posuzování významu bezpečnostních incidentů
  - Zajišťování, že celá organizace si je vědoma způsobu/formy řešení informační bezpečnosti, pěstování bezpečnostního uvědomění

# Řídící výbor - aktivity 2/2

- Odsouhlasení specifických rolí a odpovědností napříč celou organizací z pohledu dosažení požadované úrovně informační bezpečnosti
- Odsouhlasení charakteristik metodologií a procesů  použitých pro implementaci politiky informační bezpečnosti
- Posuzování adekvátnosti opatření a koordinování  implementací opatření pro nové systému, výrobky a služby Kontrola, zda jsou v organizaci dostupné zdroje pro dosažení cílů
- Kontrola, zda je ISMS řádně integrovaný do procesů organizace
- Posuzování a schvalování BP, vymezení oblasti působení ISMS
- Odsouhlasení validnosti funkčnosti ISMS
- Odsouhlasení přidělení rolí a odpovědností stanovených v BP do rolí podle organizační struktuře organizace
- Postarání se o dostatečné zdroje pro vývoj, implementaci, provozování a udržování ISMS
- Sledování změn ve vystavení klíčových informačních aktiv organizace hlavním hrozbám, stanovování hladiny akceptovatelnosti rizika
- Kontrola plnění programu bezpečnostního uvědomění a chápání ISMS
- Kontrola účinnosti bezpečnostních opatření podle pravidelných zpráv podávaných výboru bezpečnostním manažerem
- Odsouhlasování hlavních iniciativ pro vylepšování informační bezpečnosti v organizaci
- Stanovení metrik vyhovění BP a jejich periodické kontrolování
- Postarání se o koordinaci implementací opatření napříč organizací
- Trvalé postarání se o to, že běží adekvátní kroky cílené na vylepšování ISMS
- Zajištění, že probíhá posuzování ISMS managementem
    - Pravidelně (alespoň 1x ročně)
    - Stanovuje minimální vstupy pro a výstupy z posouzení ISMS
    - Za vlastní získání vstupů a za sdělení výstupů všem relevantním osobám je odpovědný manažer informační bezpečnosti (CISO)

# Manažer informační bezpečnosti, CISO

- Máme tedy 3 role participující na realizaci ISMS + řídící výbor informační bezpečnosti
  - **CEO** - výkonný ředitel, role daná statutem organizace, má odpovědnost za veškeré výkony v organizaci, tedy i ze ISMS
  - **CISO** - správce informační bezpečnosti, role daná statutem organizace, má odpovědnost za zajišťování informační bezpečnosti, většinou ho ustanovuje řídicí výbor informační bezpečnosti, vedení organizace jmenuje řídicí výbor a požádá řídicí výbor o výběr CISO
  - **Šéf projektu ISMS** - osoba pověřená řízením vlastního projektu ISMS, role není standardem vázaná na roli CEO nebo na CISO, ideálně je šéf projektu ISMS manažer schopný vhledu do informační bezpečnosti
- Požadované znalosti CISO
  - Znalost pouhé generické informační bezpečnosti nestačí
  - Musí znát byznys procesy v organizaci (jejich rizika, …)
- Kam má být role CISO v organizaci zařazená?
  - Role v některém oddělení bez konfliktu zájmů – např. v bance odd. provozních rizik
  - V malých organizacích může být role CISO sdružená s šéfem IT
  - Ve velkých organizacích (zaměstnanců) samostatná role přímo podřízená CEO (ideál) nebo jinému oddělení (provozní, IT, …)
  - Nikdy někdo z odd. interního auditu - to je konflikt zájmů

# Pracovní náplň CISO

- Vyhovění legislativním, regulačním a smluvním požadavkům
- Řízení rizik
- Řízení lidských zdrojů
- Vztah s vrcholovým managementem
- Zlepšování ISMS
- Správa aktiv
- Styk s třetími stranami
- Oblast komunikace
- Zachování kontinuity činnosti
- Technická bezpečnost
- Správa dokumentů
- Správa bezpečnostních incidentů

# Příklady pracovní náplně CISO

- V oblasti vyhovění legislativním, regulačním a smluvním požadavkům
  - Vypracovává seznam zainteresovaných stran na informační bezpečnosti
  - Např. zaměstnanci, majitelé firmy, státní správa, regulační instituce, krizové služby (hasiči, policie, záchranka, …), klienti, media, dodavatelé, partneři, …
- Ve vztahu s vrcholovým managementem
  - Objasňuje přínosy zajištěním informační bezpečnosti
  - Navrhuje bezpečnostní cíle
  - Podává zprávu o měření účinnosti opatření
- V oblasti zachování kontinuity činnosti
  - Koordinuje proces analýzy dopadů katastrofických incidentů na byznys činnosti a tvorby plánu činnosti po takových incidentech
  - Koordinuje procvičování zaměstnanců a testování plánů

# Odpovědnosti za informační bezpečnost, generické role 1/3

- **Oddělení IT** mají odpovídat za
  - Za zajištění výkonu bezpečnostních opatření systémů, za které odpovídají
  - Bezpečnost serveroven, …
  - Spolupráce při identifikaci hrozeb, hodnocení rizik, řízení projektů, revizí, výkon zpravodajství
- **Lokální administrátoři/správci systémů** mají odpovídat za
  - Registrace a rušení uživatelů systémů, monitorování systémů, přípravu bezpečnostních postupů (procedur), průběh změnového řízení v definovaných mezích, zálohování dat, navrhování aplikační bezpečnosti, implementace vnitřních opatření, testování nouzových plánů a plánů reakcí na bezpečnostní incidenty

# Odpovědnosti za informační bezpečnost, generické role 2/3

- Typová klasifikace administrátorů/správců systémů:
  - **Správci systémů** mají odpovídat (na úrovni systému) za
    - Identifikaci hrozeb, hodnocení rizik, implementaci vybraných opatření, bezpečné konfigurování systémů, nastavování systému správy uživatelů (ID, hesla), nastavování monitorování bezpečnosti systémů, implementaci změnového řízení, nastavování všech nutných bezpečnostních procedur, udržování, aktualizování a testování plánů zachování činnosti organizace
  - **Správci sítí** mají odpovídat (na úrovni domény nebo samostatné sítě) za
    - Identifikaci hrozeb v mezích sítě, hodnocení rizik, implementaci vybraných síťových opatření (vč. firewallů), bezpečné (navrhování a) konfigurování sítí, implementaci změnového řízení, nastavování bezpečnostních procedur, udržování a testování plánů obnovy sítě

# Odpovědnosti za informační bezpečnost, generické role 3/3

- Typová klasifikace administrátorů/správců systémů:
  - **Správci areálů** mají odpovídat za
    - Identifikaci hrozeb, hodnocení rizik, implementaci vybraných fyzických opatření vč. kontrol hranic areálu, detekci a likvidaci požáru, veřejné služby (plyn, elektřina) a jejich zálohování, dodávky a expedice, nastavení bezpečnostních procedur, udržování a testování plánů udržování činnosti areálu
  - **Uživatelé IT** musí znát a dodržovat politiku informační bezpečnosti organizace
    - Politika čistého stolu, dodržování přihlašovacích pravidel, zálohování dat na noteboocích a PDA, oznamovací povinnost o bezpečnostních incidentech, …
  - **Třetí strany**
    - Mají odpovědnosti stanoveny ve smlouvě a mají znát relevantní bezpečnostní procedury a praktiky organizace (tedy někdo jim je musí předat!)

# ISMS - Systém řízení informační bezpečnosti

Řízení informační bezpečnosti PV017

**Kamil Malinka**
(využity materiály Doc. Staudka a konzultace Prof. Matyáše)
Verze: podzim 2024

# Systém řízení informační bezpečnosti

- Information Security Management System, ISMS,
  Systém řízení informační bezpečnosti
- Je součástí celkového systému řízení organizace:
  - Struktura organizace
  - Politiky,
  - Plánovací činnosti
  - Odpovědnosti
  - Praktiky
  - Procesy
  - Zdroje
- Je reprezentace - projev – jak organizace přistupuje k rizikům daným orientací na informační ekonomiku

# Systém řízení informační bezpečnosti

- Cíl řízení pomocí procesů ISMS:
  - Správně fungující **procesy podporující informační bezpečnost** (autentizace, řízení přístupu, zálohování, podpisování, …) v činnostech organizace, konkrétně jejich
    - Návrh
    - Implementace
    - Zavedení do provozu
    - Provozování
    - Monitorování
    - Přezkoumávání
    - Udržování
    - Zajišťování stanovené úrovně zaručitelnosti jejich kvality

# Systém řízení informační bezpečnosti, ISO 27001/ISO 27002

- Báze pro budování ISMS - standardy ISO 27001/ISO 27002
- ISO 27001 –
  - Říká jak navrhnout ISMS a co má ISMS dělat, neříká, která bezpečnostní opatření má podporovat
- ISO 27002 –
  - Kodex nejlepších praktik zajišťujících informační bezpečnost podporujících/zpřesňujících/dotvářejících detaily chování organizace řízené podle ISO 27001 – říká, která bezpečnostní opatření může/má zabezpečovaný systém obsahovat, neříká však už jak vybraná opatření prosazovat, k tomu navádí ISO 27001
- Splnění požadavků ISO 27001 lze potvrzovat **certifikací**, v současnosti drží certifikát splnění ISO 27001 tisíce ISMS

# Standard ISO 27001:2013 v roli specifikace ISMS

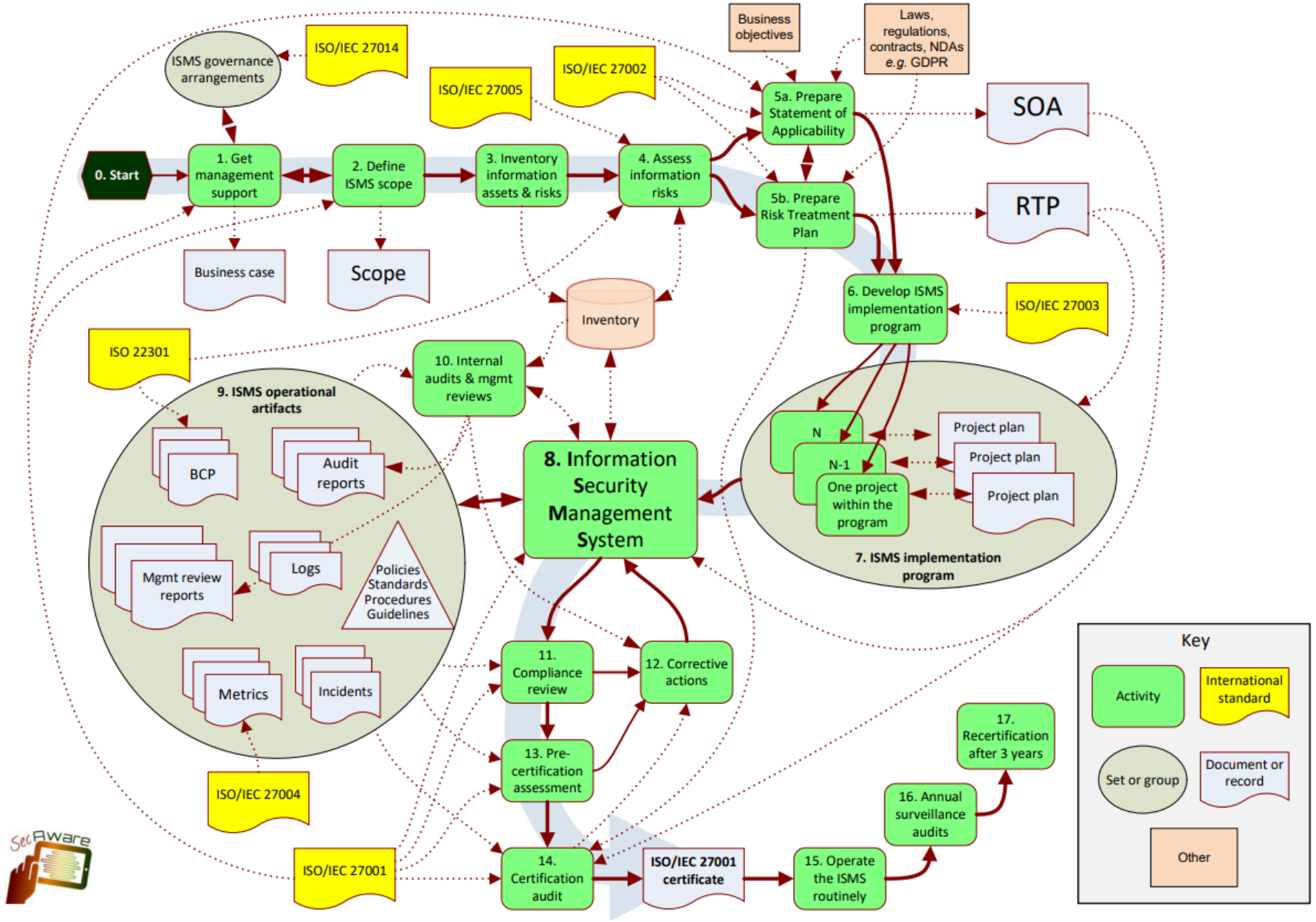
- Information Security Management Systems – Specification with Guidance for Use
  - Specifikace ISMS - jak musí být ISMS udělaný
- Standard specifikuje
  - Procesy ustanovení a řízení (správy, managementu) ISMS
  - Procesy zavádění a provozování ISMS
  - Procesy monitorování a přezkoumávání účinnosti ISMS
  - Procesy udržování a zdokonalování ISMS
  - Procesy správy dokumentové základny ISMS
  - Odpovědnost vedení organizace za projekt ISMS
  - Procesy přezkoumávání ISMS audity nezávislou třetí stranou
  - Procesy aktualizování ISMS
  - Cíle a principy vybraných bezpečnostních opatření (ilustrativní výčet uvádí ve svém Dodatku A, analogie ISO 27002)

# Proč používat standard ISO 27001? Protože …

- Je specifikací dosud známých nejlepších řídicích praktik (nejlepších - mezinárodních, všeobecně akceptovaných) a současně je návodem k jejich použití
- Specifikuje ISMS netechnickou a nejurisdickou formou, nevázanou na konkrétní technologie
- Je systematický, řešení informační bezpečnosti pokrývá plně
- Jeho validnost je prokázána v mnoha konkrétních nasazení
- Produkt vybudovaný podle ISO 27001 lze externě certifikovat
- Úzce navazuje na standard ISO 9001, standard kvality podnikatelských procesů organizace

# Co je vlastně ISMS?

- Z definice standardem se jedná se o systém řízení, který je
  - Dokumentovaný, systematicky implementovaný a řízený
  - Trvale přezkoumávaný, auditovaný a kontrolovaný
  - Trvale vylepšovaný (aktualizovaný)
  - DŮVĚRYHODNÝ systém pro řízení informační bezpečnosti
- Důkazem důvěryhodnosti ISMS je jeho certifikace
  - Certifikaci provádí třetí, nezávislá certifikační instituce (autorita)
  - Certifikací ISMS se získává důkaz úplnosti a kvality ISMS
  - Pro podnikání je certifikace ceněná, nikoli však vždy nezbytná
  - Certifikace přispívá k dosažení maximální, dlouhodobě platné, hodnoty podnikatelských procesů
  - Vždy jde o finální etapu vývoje a zavedení ISMS




Implementation and Certification process 2022, ISO27k Implementation Forum. *https://www.iso27001security.com/*

# ISO 27001: 7 kapitol definovaných požadavků

- Kontext organizace – určení záměru a potřeb organizace, rozsahu ISMS a implementace a průběžné zlepšování
- Vůdčí role – závazek vedení organizace, stanovení politiky, určení rolí a odpovědností
- Plánování – opatření zaměřená na rizika (posouzení rizik a jejich ošetření) vč. seznamu nezbytných opatření, stanovení cílů bezpečnosti a plán jejich dosažení
- Podpora – jsou zaručeny dostatečné zdroje, kompetence a povědomí, informace jsou dokumentované a aktualizované
- Provozování – plánování a řízení provozu, průběžné posuzování a ošetření rizik
- Hodnocení výkonnosti – monitoring, audit, přezkoumání vedením
- Zlepšování – neshody a nápravná opatření, neustálé zlepšování

# Oblast působnosti ISMS

- Řízení informační bezpečnosti lze uplatňovat pouze v prostoru uvnitř vymezené oblasti *(scope)*
  - Požadavek přímo daný standardem
  - Oblastí nemusí nutně být celá organizace (obvykle vymezuje politika informační bezpečnosti)
  - Informace do oblasti vstupuje a oblast opouští pomocí určených nástrojů - kontrolovaně
  - V oblasti se musí nacházet úplná chráněná informace vč. všech souvisejících technických i netechnických procesů
- Definování hranic oblasti
  - Hranice jsou fyzicky nebo logicky definovatelné v pojmech organizace či její části, která se má chránit (data, sítě, geografické lokace, …)
  - Oblast musí být fyzicky/logicky vyčlenitelná od třetích stran a od jiných organizací působících v rámci větší skupiny
- ISMS v definované oblasti zajišťuje řízení informační bezpečnosti v kontextu podnikatelských procesů organizace (procesů činnosti)

# Kontext

- Externí kontext
  - Právní důsledky – např. předávání dat mezi US a EU
  - Geolokace – časté výskyty hurikánů, záplavové území, pravidelné demonstrace
  - Kulturní a sociální požadavky na služby
- Interní kontext
  - Centralizace některých služeb – v MUNI např. EDUROAM (CESNET -> UVT -> fakulty + FI jako výjimka)
  - Co mimobrněnské lokality (Telč)?

# Podpora od managementu/vedení organizace

- Úspěšná implementace ISMS absolutně závisí na reálné a nepředstírané podpoře vrcholovým managementem organizace
- Vrcholový management se musí průkazně zavázat, že na realizaci projektu ISMS zajistí ekonomické a personální zdroje
  - Požadavek přímo uvedený v ISO 27001, pro certifikaci povinný důkaz
  - Vrcholový management musí jasně stanovit úroveň preference projektu ISMS vůči ostatním projektům organizace
- Projekt ISMS je projektem změny řízení v organizaci
  - Nelze jej jen tak jednoduše transplantovat do existujících procesů a procedur podnikatelských projektů
  - Zavedení ISMS vyvolá řadu změnových řízení

# Výčtová ilustrace požadované dokumentace ISMS 1/5

- Vlastnosti a charakter ISMS na první pohled výrazně charakterizuje výčet požadované a doporučované **dokumentace ISMS**

# Výčtová ilustrace požadované dokumentace ISMS 2/5

1. Oblast působnosti ISMS
   - Často samostatný, krátký dokument obvykle vypracovaný hned na počátku zavádění ISMS
2. Politika Informační bezpečnosti, stanovení bezpečnostních cílů
   - Celková bezpečnostní politika, co proti čemu/komu se chrání
3. Metodologie ohodnocování a zvládání rizik
   - Typicky 4-5 stran, vypracovaných dřív, než se spustí ohodnocování rizik
   - Definice pravidel, jak provádět řízení rizik, škály, úroveň akceptovatelnosti rizika
   - Jak zvládat neakceptovatelná rizika (zvolit opatření, řešit pojištěním, zrušením rizikové aktivity, zvýšením úrovně akceptovatelnosti, …)

# Výčtová ilustrace požadované dokumentace ISMS 3/5

4. Prohlášení o aplikovatelnosti bezpečnostních opatření
   - Která opatření se zvolila a proč
5. Plán zvládání rizik
   - Kdo které opatření za kolik a v jakém čase implementuje
   - Dokument okamžitě schvalovaný vedením (dává „peníze“)
6. Zpráva o posouzení a ošetření rizik
   - Výsledek ohodnocení rizik
7. Definice rolí a odpovědností v oblasti informační bezpečnosti
   - Nejlepší metodou je popsat role a odpovědnosti přes všechny politiky a procedury
   - Co nejpřesněji! Ne „mělo by se provést“, ale „CISO každé pondělí v XX:YY udělá XYZ“
   - Role a odpovědnosti třetích stran se definují ve smlouvách

# Výčtová ilustrace požadované dokumentace ISMS 4/5

8. Soupis aktiv
9. Popis akceptovatelného používání aktiv
   - Nejlépe formou politiky, specifikací pravidel používání každého aktiva
10. Politika řízení přístupu
    - Schvalování přístupu k určitým informacím a systémům na aplikační (byznys) úrovni a na technické úrovni, může pokrývat logický i fyzický přístup
    - Lze vypracovat až po ohodnocení a zvládnutí rizik
11. Bezpečné provozní procedury správy IT
    - Pro změnové řízení, používání služeb třetích stran, zálohování, síťovou bezpečnost, zvládání škodlivého softwaru, likvidaci dat a zařízení, přenosy informací, monitorování
    - Lze vypracovat až po ohodnocení a zvládnutí rizik

# Výčtová ilustrace požadované dokumentace ISMS 5/5

12. Principy bezpečného systémového inženýrství
    - Jak zabudovat bezpečnostní techniky do všech úrovní - ladění, testování, akceptace, živý provoz, techniky autentizace, řízení relací
13. Bezpečnostní politika pro dodavatele
    - Jak lustrovat potenciálního dodavatele, jak udělat ohodnocení rizik dodavatele, která bezpečnostní opatření dát do smlouvy a jak dozorovat jejich plnění, jak lze měnit smlouvu, jak ukončit přístupy po vypršení smlouvy, …
14. Procedura reakce na incidenty
    - Jak jsou zaznamenávány, klasifikovány a zvládány bezpečnostní události a incidenty, zranitelnosti
15. Legislativní, regulační a smluvní požadavky
    - Dělat co nejdříve, má vliv na hodně zbývajících dokumentů a prací

# Výčtová ilustrace požadovaných protokolů ISMS 1/2

- Plnění programu školení a zvyšování kvalifikace
  - Zajišťuje personální oddělení
- Výsledky měření a monitorování
  - Definice každého opatření by měla obsahovat **KPI** (*key performance indicators*), které je potřeba měřit a monitorovat
- Program vnitřních auditů
  - Roční plán vnitřních auditů
  - Kdo bude auditor, metoda auditu, kritéria hodnocení
- Výsledky vnitřních auditů
  - Auditní zprávy, zprávy o výsledcích auditů

# Výčtová ilustrace požadovaných protokolů ISMS 2/2

- Výsledky a závěry oponentur
  - Zápisy z jednání managementu
- Výsledky opravných akcí
- Záznamy (logy) uživatelských aktivit, výjimečných stavů a bezpečnostních událostí

# Výčtová ilustrace doporučované dokumentace ISMS 1/2

- Procedura správy dokumentů
- Nástroje pro správu protokolů
- Procedura interního auditu
- Procedura opravné akce
- Politika *Bring your own device* (BYOD)
- Politika práce ze vzdáleného pracoviště a z mobilních zařízení
- Politika klasifikace informací
- Politika hesel
- Politika likvidace a destrukce
- Politika čistého stolu/obrazovky
- Politika změnového řízení

# Výčtová ilustrace doporučované dokumentace ISMS 2/2

- Politika zálohování
- Politika přenosu informací
- Analýza dopadů činnosti na informační bezpečnost
- Plán procvičování a testování
- Plán údržby
- Plán oponentur
- Strategie zachování kontinuity činnosti

# Projekt implementace ISMS

Řízení informační bezpečnosti PV017

**Kamil Malinka**
(využity materiály Doc. Staudka a konzultace Prof. Matyáše)
Verze: podzim 2024

# Úvodní kroky, dobrý začátek - půl je hotovo

- Zredukujte v zadání vše, co vypadá potenciálně složité, náročné na čas či zdroje, obtížné, … na to, o čem je každý přesvědčen, že je realizovatelné v rámci určeného času a přidělených zdrojů
  - Projekt musí mít přidělené dostatečné ekonomické a personální zdroje
  - Na realizaci ISMS musí být dost času i v případě, že se věci nebudou vyvíjet dobře - **musí existovat časová rezerva**
  - Každý zaměstnanec musí znát rizika vyžadující zavedení ISMS a akceptovat opatření, která se použijí pro jejich minimalizaci
- Většina lidí nemá ráda změny, nerada pracuje s neznámem **ISMS přináší změny, a tudíž něco (mnoho) nového do pracovních zvyklostí :-((**
  - Je potřeba počítat, že alespoň hrstka lidí bude projekt podkopávat

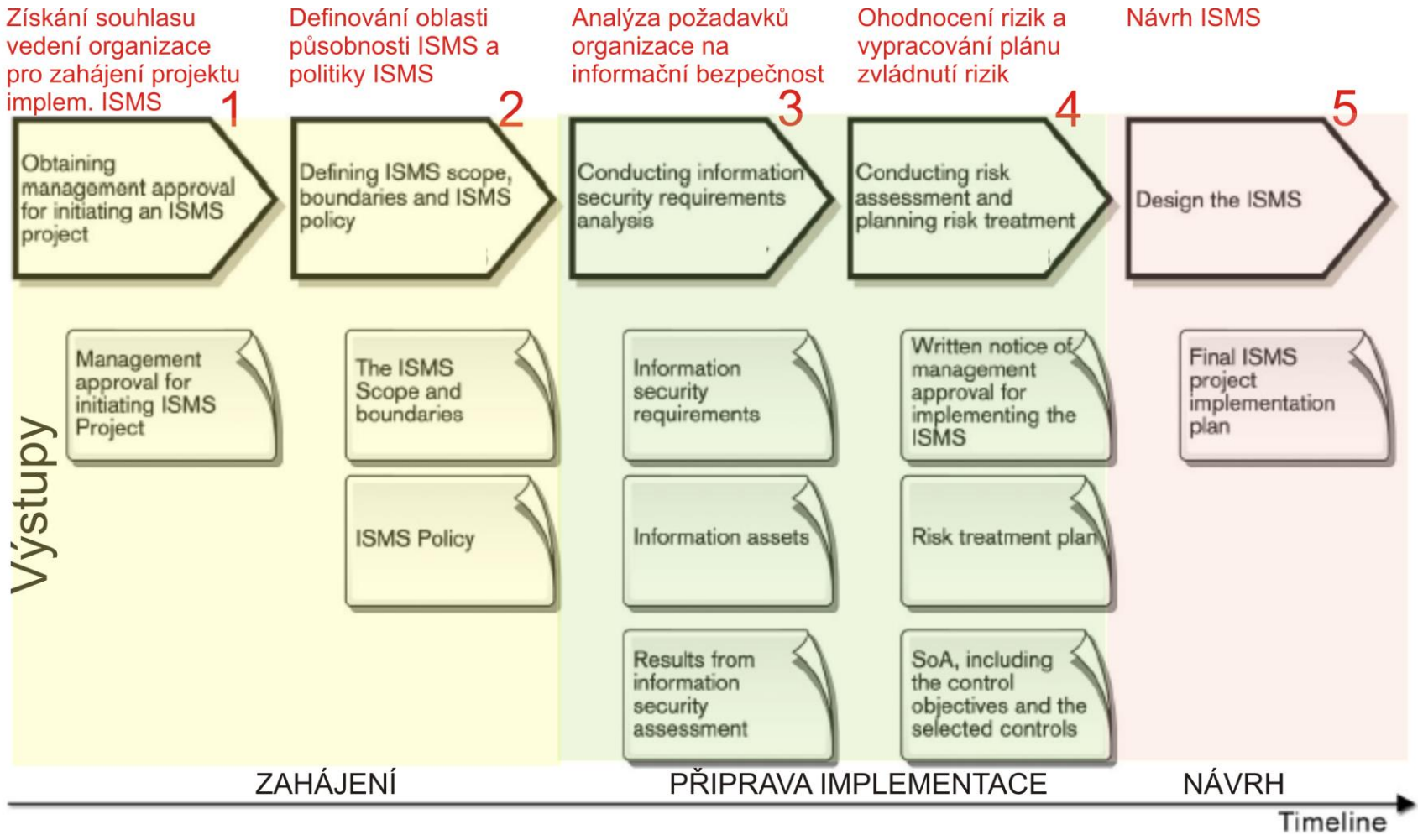
# Projekt zavedení, implementace ISMS

- ISO/IEC 27003 : 2010 Information technology — Security techniques — Information security management system implementation guidance

- Návod k implementaci ISMS
  - Jak zahájit, naplánovat a definovat **projekt** zavádění ISMS

- Co je to projekt  - obecná charakteristika
  - Jedinečná soustava činností směřujících k předem stanovenému a jasně definovanému cíli,
  - Která má určený začátek a konec,
  - Která vyžaduje spolupráci různých profesí, váže jejich kapacity a jejich úsilí a
  - Využívá (případně spotřebovává) pro
    - Vytvoření cílových výstupů
    - Informace
    - Materiál
    - Peníze
    - Schopnosti a dovednosti zúčastněných lidí

# Fáze projektu implementace ISMS



# Dílčí kroky fází projektu implementace ISMS

1. **Získání souhlasu vedení organizace pro zahájení implem. ISMS**
    1. Objasnění priorit organizace pro projekt ISMS
    2. Předběžná definice oblasti působnosti ISMS
    3. Vytvoření zakázky a plánu projektu implementace ISMS pro odsouhlasení vedením organizace
2. **Definování oblasti působnosti ISMS a politiky ISMS**
    1. Definování oblasti a hranic inf. bezpečnosti v organizaci
    2. Definování oblasti a hranic informačních a komunikačních technologií (ICT)
    3. Definování fyzické oblasti a hranic
    4. Integrace všech oblastí a hranic do oblasti a hranic ISMS
    5. Vývoj politiky ISMS a získání souhlasu od vedení

# Dílčí kroky fází projektu implementace ISMS

3. **Analýza požadavků organizace na informační bezpečnost**
    1. Definování požadavků organizace na inf. bezpečnost
    2. Identifikace aktiv v oblasti působnosti ISMS
    3. Ohodnocení informační bezpečnosti
4. **Ohodnocení rizik a vypracování plánu zvládnutí rizik**
    1. Ohodnocení rizik
    2. Výběr cílů opatření a opatření - **Prohlášení o aplikovatelnosti**
    3. Získání souhlasu vedení organizace s implementací a provozováním ISMS, vypracování **plánu zvládnutí rizik**

# Dílčí kroky fází projektu implementace ISMS

5. **Návrh ISMS**
    1. Návrh informační bezpečnosti v organizaci
    2. Návrh fyzické a ICT bezpečnosti
    3. Návrh informační bezpečnosti specifické pro ISMS
    4. Vytvoření finálního plánu projektu ISMS

# Plán návrhu a implementace ISMS

- Projekt vždy zaměstnává skupinu lidí a ovlivňuje jiné skupiny lidí.
- Projekt je vždy spojen s rizikem neúspěchu, poněvadž je jedinečný a nikdy zcela přesně nevíme, co nás v průběhu jeho realizace čeká nebo zaskočí.
- Abychom však mohli projekt řídit k úspěchu, musíme mít nějaký scénář či osnovu - tímto jsou **plány projektu**
- Příklady plánovaných úkolů
  - Určení způsobu řízení projektu (waterfall, agilní přístup)
  - Určení způsobu zajištění integrace různých řídících systémů
  - Identifikace klíčových odpovědností
  - Identifikace požadovaných zdrojů v průběhu životního cyklu projektu
  - Rozhodnutí o využívání konzultantů
  - …

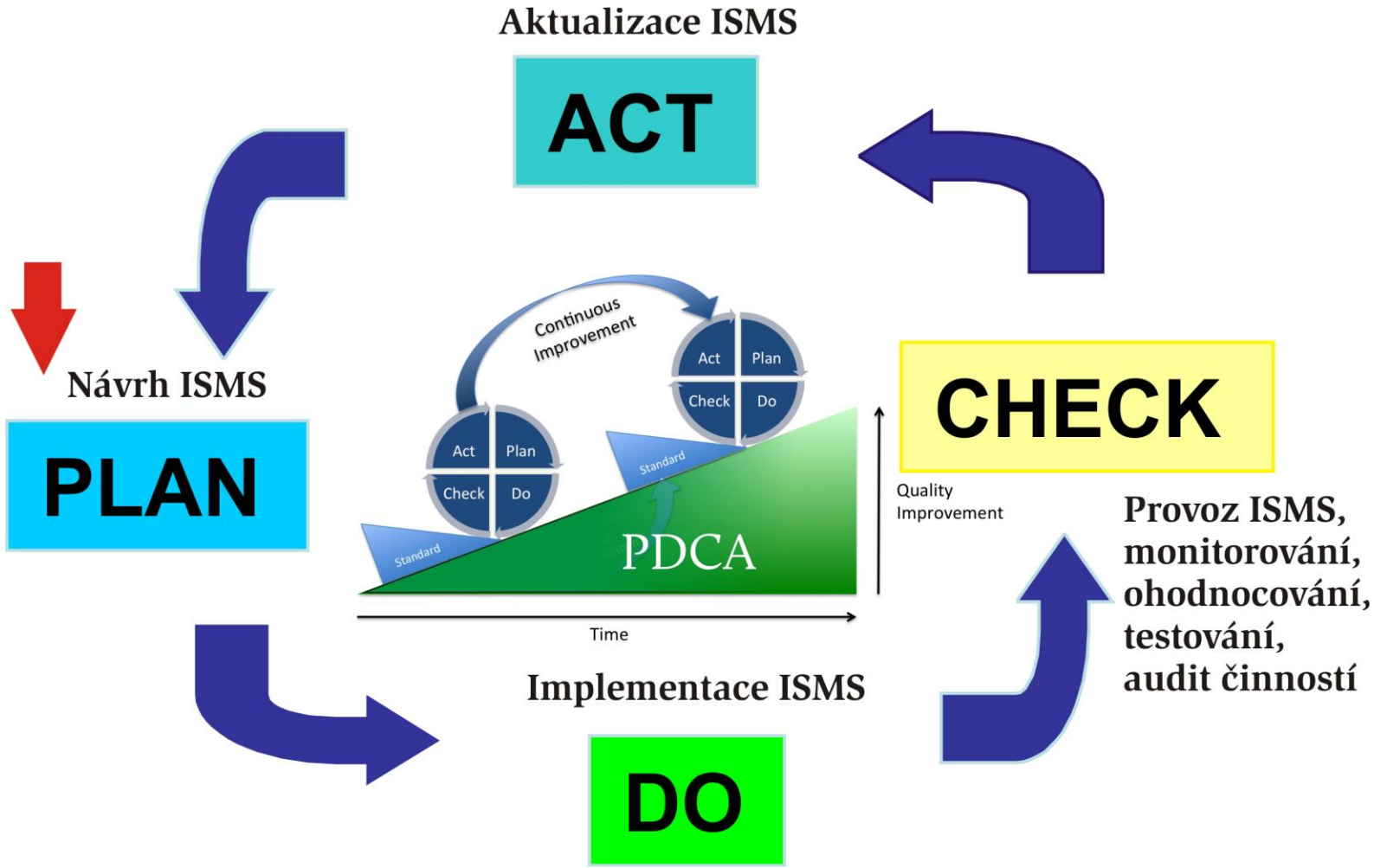
# Plán návrhu a implementace ISMS

- Úspěch projektu tedy znamená splnění cíle ve třech dimenzích:
  - **Věcně** (CO, JAK, a V JAKÉ KVALITĚ se má udělat)
  - **Časově** (KDY má být co provedeno - etapy/fáze, kroky, úkony)
  - **Nákladově** (ZA KOLIK se to má udělat, nejprve ve spotřebované práci a pak v penězích)
- Tento trojimperativ projektu v podstatě odpovídá tomu, jak bývá vymezena smlouva o dílo
  - *Každá smlouva o dílo musí obsahovat:*
    - *specifikaci plnění (CO A JAK, V JAKÉ KVALITĚ),*
    - *termíny (KDY) a*
    - *cenu (ZA KOLIK),*
    - *aby to smlouva o dílo byla*

# Metody řízení realizačního projektu

- Standard ISO/IEC 27001 původně direktivně předpisoval použít pro projekt implementace ISMS procesní přístup podle metodologie PDCA
  - **PDCA**, *Plan-Do-Check-Act*, plánuj, udělej, zkontroluj, jednej
  - Také Demingův cyklus nebo PDCA cyklus - metoda postupného zlepšování například kvality výrobků, služeb, procesů, aplikací, dat, probíhající formou opakovaného provádění čtyř zmíněných činností. Detaily viz např. *http://mostechinformationsite.blogspot.cz/2014/10/pdca-cycle-of-quality-management-basic.html*
- Další aplikovatelné metody řízení
  - COBIT, *http://www.isaca.org/cobit/pages/default.aspx*
  - ITIL, *https://managementmania.com/cs/information- technology-infrastructure-library*

# Model PDCA je široce uplatňovaný v podnikání, v řízení kvality, … tedy i pro ISMS



# PDCA – fáze 1/3

- PLAN (zřízení ISMS)
  - Definice oblasti ISMS
  - Definice politiky informační bezpečnosti
  - Definice systematického přístupu k ohodnocování rizik
  - Vypracování procedur řešících ohodnocení rizik a provedení ohodnocení rizik cíl - v kontextu politiky a oblasti ISMS identifikovat důležitá informační aktiva a rizika, kterým jsou tato aktiva vystavena
  - Identifikace a vyhodnocení možností jak zvládat rizika
  - Výběr cílů ochran a implementovatelných opatření pro každou možnost
  - Vypracování Prohlášení o aplikovatelnosti vybraných opatření (pokryté bezpečnostní cíle a vlastnosti vybraných opatření)

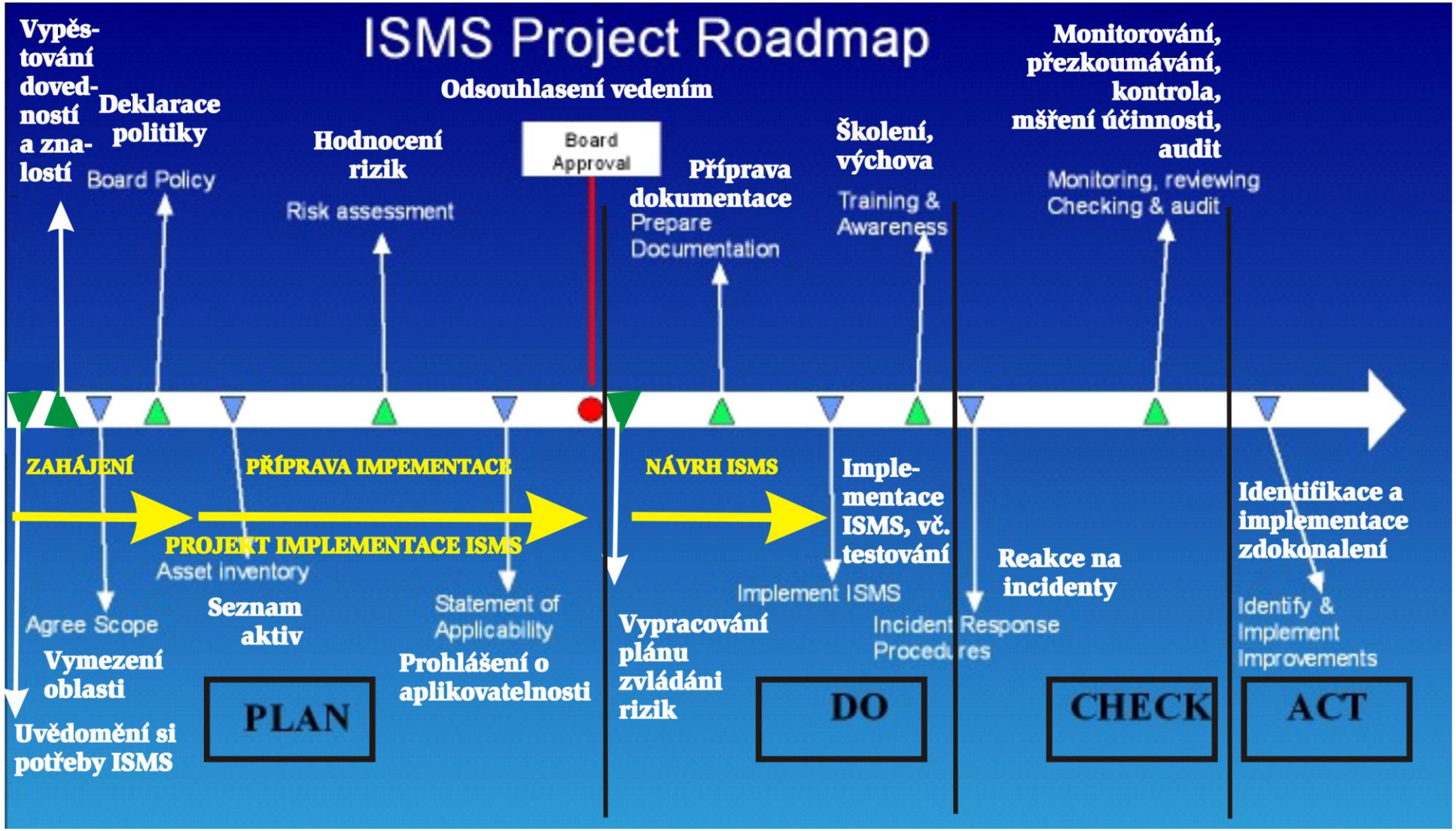
# PDCA – fáze 2/3

- DO (implementace ISMS)
  - Formulace plánu zvládání rizik, vytvoření jeho dokumentace
    - Systémová, detailní, bezpečnostní politika
    - Definice procesů a procedur plnících bezpečnostní opatření
  - Implementace všech opatření určených v plánu zvládání rizik
  - Implementace procedur (opatření) umožňujících promptní detekci bezpečnostních incidentů a reakce na ně
  - Zaškolení relevantních zaměstnanců, definice programu systematické výchovy k bezpečnostnímu uvědomění
  - Zajištění zdrojů a operací pro výkon činností ISMS

# PDCA – fáze 3/3

- CHECK (sledování a posuzování výkonů provozovaného ISMS)
  - Monitorování, ohodnocování, testování, audit činností řízených ISMS
  - Vytváření důkazů, shromažďování výsledků monitorování, …
  - Posuzování a tam, kde to jde i měření výkonů procesů proti bezpečnostní politice, cílům a praktickým zkušenostem
  - Generování zpráv pro posouzení managementem
  - Měření účinnosti systému řízení a opatření, která jej implementují
- ACT (údržba a vylepšení ISMS)
  - Provedení oprav a změn na základě výsledků posouzení managementem
  - Identifikace, dokumentace a implementace vylepšení ISMS

# Cestovní mapa PDCA cyklu ISMS



# Role dokumentace ISMS

Řízení informační bezpečnosti PV017

**Kamil Malinka**

(využity materiály Doc. Staudka a konzultace Prof. Matyáše)

Verze: podzim 2024

# Role dokumentace ISMS

- Procesy v organizaci opakovatelné, odolné vůči ztrátě znalostí např. po výpovědi některého zaměstnance, musí být dokumentované
  - Opakovatelné procesy jsou pak konzistentnější a více předvídatelné
- Účinnost každého systému řízení závisí na patřičné, korektní dokumentaci jeho procesů a na archivu záznamů demonstrujících jeho nedostatky
- ISO 27001 požaduje dostupnost dokumentace
  - Jak každého bezpečnostního opatření ISMS, tak i relevantního ISMS
- Dobře fungující ISMS je plně dokumentovaný

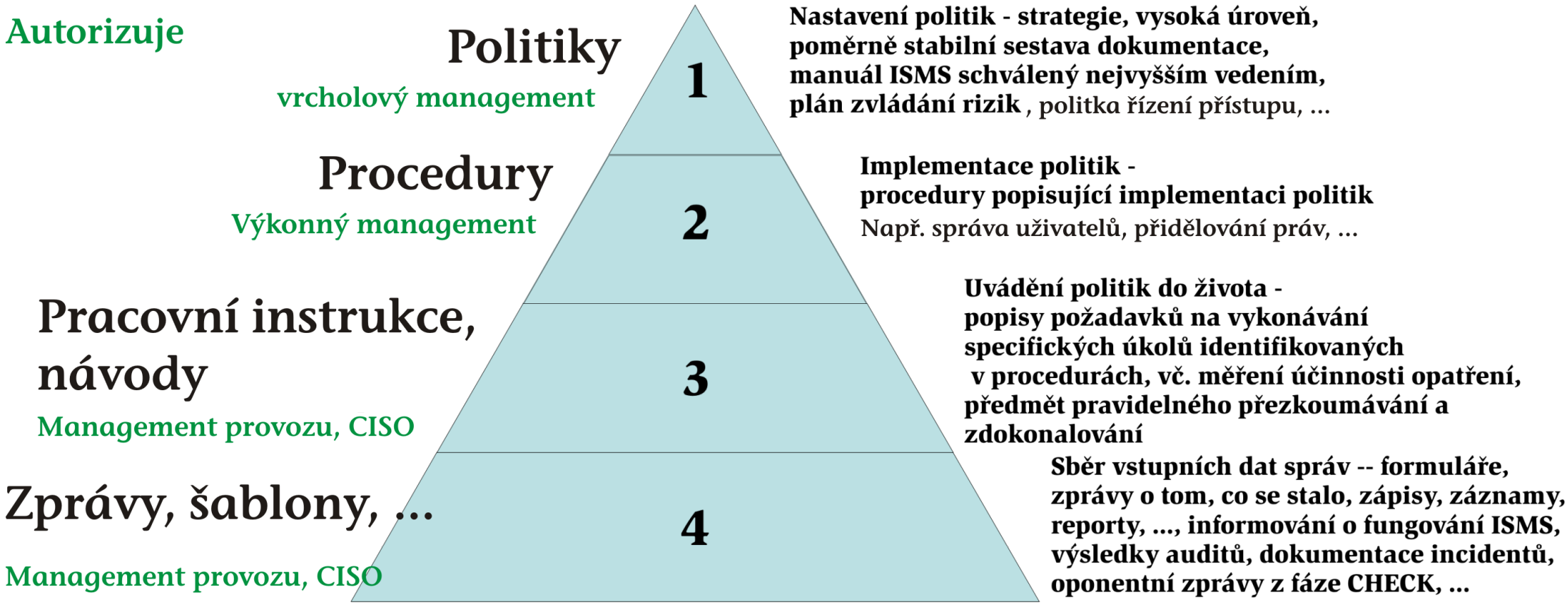
# Role dokumentace ISMS

- Tvorba dokumentace ISMS je **časově nejnáročnější** část projektu
- Dokumentace ISMS musí být
  - Úplná, vyčerpávající
  - V souladu s požadavky standardu ISO 27001
  - Ve formě odpovídající firemnímu stylu a kultuře
- Dokumentace musí být dostupná a použitelná

# Požadavky na dokumentaci ISMS

- Organizace musí mít systém řízení dokumentace určující
  - Jak se informace distribuují, zpřístupňují, získávají a používají
  - Jak musí být informace uchovávané a chráněné, vč. udržení čitelnosti
  - Změnové řízení v dokumentaci
  - Pravidla skladování a likvidace dokumentace
  - Způsob identifikace a správy dokumentů chráněných autorskými právy
  - Způsob identifikace a zacházení s informacemi podle jejich klasifikační úrovně z hlediska důvěrnosti
  - Způsob zacházení s informacemi personalistického charakteru
- Jsou dostupné systémy pro řízení dokumentových základen ISMS obsahující předpřipravené šablony, …
  - *http://www.itgovernance.co.uk/shop/p-1462-iso-27001-iso27001-Isms-documentation-toolkit.aspx*
  - *http://advisera.com/27001academy/iso-27001-documentation-toolkit/*

# 4-vrstvá struktura dokumentové základny ISMS



# 4-vrstvá struktura dokumentové základny ISMS

- 1. vrstva - **Politiky**
  - Nastavení politik - strategické poměrně řídce měněné dokumenty na vysoké úrovni abstrakce, stanovení principů
  - Dokumenty autorizované nejvyšším managementem
    autorizace = demonstrace odpovědnosti nejvyššího vedení za politiky
  - Příklady dokumentů 1. úrovně
    - vymezení zabezpečované oblasti,
    - politika informační bezpečnosti,
    - plán řešení procesů PDCA při vývoji ISMS
    - výsledek hodnocení rizik,
    - prohlášení o aplikovatelnosti,
    - plán zvládání rizik,
    - manuál ISMS
    - …

# 4-vrstvá struktura dokumentové základny ISMS

- 2. vrstva - **Procedury**
  - Popis procedur pro implementaci politik,  nastavení podnikatelských požadavků, procedur a procesů
  - Dokumenty autorizované výkonným managementem, konkrétně těmi, kteří jsou odpovědní za prosazování politik v konkrétních oblastech podnikání, a CSO (Chief Security Officer), správcem bezpečnosti, vždy však po projednání s řídicím výborem informační bezpečnosti
  - Příklad: politika řízení přístupu si vyžádá procedury:
    - Správa uživatelů (*User Management*): zřizování účtů, …
    - Přidělování přístupových práv
    - …
  - Procedury se mohou měnit v průběhu roku tak, aby reagovaly na konkrétní podnikatelské podmínky a požadavky, změny se smí však odehrávat pouze v mezích stanovených politikami schválenými nejvyšším managementem

# 4-vrstvá struktura dokumentové základny ISMS

- 3. vrstva - **Pracovní instrukce**
  - Uplatňování politik při konkrétních činnostech organizace, instrukce pro provádění konkrétních úkolů zaměstnanci, vč. měření účinnosti opatření, v organizaci, v jednotlivých odděleních
  - Dokumenty typu smlouva s uživatelem, popis práce, apod. (např. jak postupovat při uzavírání dohody se vzdáleně pracujícím zaměstnancem)
  - Jsou vytvářené vlastníky podnikatelských aktiv/procesů, autorizované jejich přímými nadřízenými a správcem informační bezpečnosti, CISO (Chief Information Security Officer)
  - Jsou pravidelně přezkoumávané a vylepšované, mění se poměrně často, tak jak se mění pracovní metody (ISMS se průběžně vylepšuje), případně tak jak se identifikují rizika (preventivní akce) nebo selhávají opatření (opravné akce)
  - Změny v pracovních instrukcích se smí však odehrávat pouze v mezích stanovených procedurami, které implementují

# 4-vrstvá struktura dokumentové základny ISMS

- 4. vrstva - **Zprávy**
  - Zprávy o tom, co se stalo, jak ISMS běžel
  - Zápisy, logy, záznamy o incidentech, …
  - Výsledky auditů z fáze CHECK,
  - Formuláře, šablony pro tyto dokumenty

# Jak vytvářet dokumentaci ISMS?

- Metoda pokusů a omylů, první tvorba, pouze vlastními silami
  - Typicky potřebná doba: 14 – 19 měsíců
    - Porozumění požadavkům: 1 měsíc
    - Plánování: 1 měsíc
    - Vypracování politiky informační bezpečnosti: 1 měsíc
    - Vypracování prohlášení o aplikovatelnost: 2 měsíce
    - Vypracování procedur: 4 - 6 měsíců
    - Vypracování pracovních instrukcí: 5 - 9 měsíců
  - Kritika
    - Velká časová náročnost, absence znalosti nejlepších postupů
    - Projekt pravděpodobně selže díky nezkušenému vedení

# Jak vytvářet dokumentaci ISMS?

- Externí spolupráce, dokumenty vypracují externí konzultanti
    - Typicky potřebná doba: 10 – 14 měsíců
    - Porozumění požadavkům: 1 týden
    - Plánování: 1 týden
    - Vypracování politiky informační bezpečnosti: 1 měsíc
    - Vypracování prohlášení o aplikovatelnost: 2 měsíce
    - Vypracování procedur: 3 - 5 měsíců
    - Vypracování pracovních instrukcí: 4 - 6 měsíců
  - Přínosy
    - Rychlé řešení, dostupnost znalosti nejlepších postupů
    - Projekt pravděpodobně neselže díky zkušenému vedení
  - Kritika
    - Vysoké náklady
    - Obtížně řešitelné průběžné vylepšování ISMS (Cyklus PDCA)

# Jak vytvářet dokumentaci ISMS?

- Použití návodů a dokumentového nástroje připraveného třetí stranou
  - Řešení vlastními silami podle prototypů
  - Příklady prototypů: www.itgovernance.co.uk
  - Typicky potřebná doba: 4 – 7 měsíců
    - Porozumění požadavkům: 1 týden
    - Plánování: 1 týden
    - Vypracování politiky informační bezpečnosti: 2 - 4 týdny
    - Vypracování prohlášení o aplikovatelnost: 2 měsíce
    - Vypracování procedur: 1 - 2 měsíce
    - Vypracování pracovních instrukcí: 2 - 4 měsíce
  - Přínosy
    - Rychlé řešení, dostupnost znalosti nejlepších postupů
    - Nákladově efektivní řešení
    - Projekt pravděpodobně neselže díky postupu podle norem
    - Snadněji řešitelné průběžné vylepšování ISMS (Cyklus PDCA)

# Testování

- Proč se testuje ISMS ?
  - Fungují procedury řízení tak jak bylo zamýšleno ?
  - Fungují bezpečnostní opatření tak jak bylo zamýšleno ?
- Typy testů
  - Důkladný audit (interním nebo externím) auditorem, zkoumají se dokumentované procedury a demonstruje se jejich činnost
  - „Papírové“ testování, logické testování opatření a procedur na základě znalosti zranitelností, konstrukcí opatření, projevů hrozeb, …
  - Reálné testování, penetrační testy, testy ztráty energie, …
  - Rozsáhlé scénářově orientované testy - testy plánu zachování činnosti,
- Během roku se má testovat každý rys, vlastnost, … ISMS

# Audit

- 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

# 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 bezpečnosti 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

# Co dělat pro úspěšnost/prospěšnost auditu ISMS

- Dokumentace je úplná, pokrývá celý ISMS a je dostupná auditorům
- Jsou dostupné všechny zprávy z interních auditů a z provedených testů
- Všichni zaměstnanci musí být instruování, že vůči auditorům musí být maximálně otevření a vstřícní vč. ochotu k demonstracím činnosti
- Auditorům je nutné zpřístupnit i oblast vyššího managementu – vedení firmy
- Auditovaná strana musí být připravena diskuse s auditory
  - Zastrašování/dehonestace auditorů je cestou do pekel
  - Pomocnou ruku auditoři vesměs hodnotí pozitivně

# Zamyšlení na závěr

# Jak poznat okamžik, kdy podnik potřebuje roli CISO (nebo ji oddělit od šéfa IT)?

- https://www.linkedin.com/pulse/when-should-startups-hire-ciso-prasanna-venkat-6yzke/

**When Should Startups Hire For Security ?**

prasanna@cyberquotient.in

CYBER QUOTIENT

| Funding Stage | Hire or Outsource? | Whom ? | Deliverables | Dependency / Most interacted Peering Teams |
|---|---|---|---|---|
| **Pre-Seed Stage** | Outsource | • vCISO | • High Level Architecture Review<br>• Threat Modelling | • Engineering Team<br>• Product Team |
| **Seed Stage** | Outsource / Hire | • vCISO<br>• AppSec Engineer<br>• IT / IT Security<br>• Cloud Security Engineer | • Product Security<br>• Infrastructure<br>• Cloud | • Engineering<br>• IT<br>• DevOps |
| **Growth Stage / Series B and C** | Hire | • CISO / Dir of Security / Head of Security<br>• Cloud Security<br>• AppSec Engineer<br>• IT Security Engineer | • Governance Risk & Compliance (GRC)<br>• Product Security<br>• MobileApp Security<br>• Infrastructure / Cloud | • IT<br>• Engineering<br>• Cloud / DevOps<br>• Legal / Compliance |
| **Late-Stage / Series D and Beyond** | Hire | • CISO / Dir of Security /<br>• DevSecOps Manager / Engineer<br>• Product Security Lead<br>• IT Security Engineer | • Governance Risk & Compliance (GRC)<br>• Product Security<br>• Mobile App Security<br>• Infrastructure / Cloud | • IT<br>• Engineering<br>• Cloud / DevOps<br>• Legal / Compliance |
| **IPO (Initial Public Offering)** | Hire | • CISO / Dir of Security /<br>• DevSecOps Manager / Engineer<br>• Product Security Lead<br>• IT Security Engineer | • GRC<br>• Product Security<br>• Mobile App Security<br>• Infrastructure / Cloud | • Legal / Compliance<br>• IT<br>• Engineering<br>• Cloud / DevOps |

https://cyberquotient.in

# Ukázkové otázky písemky

# Ukázkové otázky písemky

- Otevřené otázky:
  - Vysvětlete následující pojmy: aktivum
  - Jaké atributy se obvykle vyskytují v modelu útočníka?
- Testové otázky:
  - Mezi de facto standardy nepatří:
    a) ISO 9001
    b) ISO 27k
    c) RFC
    d) COBIT
    e) OWASP

# Dodatek

# Co je pracovní náplní CISO 1/9

- V oblasti vyhovění legislativním, regulačním a smluvním požadavkům
  - Vypracovává seznam zainteresovaných stran na informační bezpečnosti
  - Např. zaměstnanci, majitelé firmy, státní správa, regulační instituce, krizové služby (hasiči, policie, záchranka, …), klienti, media, dodavatelé, partneři, …
  - Vypracovává seznam požadavků zainteresovaných stran na ITSec
  - Udržuje kontakt úřady a speciálními zájmovými skupinami
  - Koordinuje veškeré činnosti související s ochranou osobní dat

# Co je pracovní náplní CISO 2/9

- V oblasti řízení rizik
  - Učí zaměstnance jak dělat ohodnocování rizik
  - Koordinuje všechny procesy ohodnocování rizik
  - Navrhuje výběr opatření
  - Navrhuje časové limity implementací opatření
  - Provádí iniciální posouzení rizik
  - Identifikuje změny rizik a zajišťuje odpovídající reakce
  - Zajišťuje, že vrcholový management a řídicí výbor odsouhlasuje rizika a přístup organizace k řízení rizik, plán zvládání rizik a  nutnou úroveň záruky za bezpečnost

# Co je pracovní náplní CISO 3/9

- V oblasti řízení lidských zdrojů
  - Ověřuje uchazeče o zaměstnání s hlediska informační bezpečnosti
  - Vypracovává plán školení v oblasti informační bezpečnosti
  - Průběžně je činný v oblasti zvyšování bezpečnostního uvědomění
  - Navrhuje disciplinární řízení se zaměstnanci narušujícími informační bezpečnost
  - Podílí se na výběrovém řízení zaměstnanců

# Co je pracovní náplní CISO 4/9

- Ve vztahu s vrcholovým managementem
  - Objasňuje přínosy zajištěním informační bezpečnosti
  - Navrhuje bezpečnostní cíle
  - Podává zprávu o měření účinnosti opatření
  - Navrhuje akce opravující a vylepšující opatření
  - Navrhuje objem nákladů a zdrojů potřebných na zajištění informační bezpečnosti
  - Sděluje důležité požadavky zainteresovaných stran na ITSec
  - Upozorňuje na hlavní rizika
  - Podává zprávu o implementaci opatření
  - Radí vrcholovému managementu ve všech bezpečnostních problémech
  - Spolupracuje na identifikaci cílů ITSec

# Co je pracovní náplní CISO 5/9

- Ve vztahu s vrcholovým managementem
  - Instruuje řídicí výbor o aktuálních hrozbách, zranitelnostech a o adekvátních krocích k jejich eliminaci
  - Sděluje výsledky měření efektivnosti zajištění ITSec
  - Navrhuje vylepšení a opravy zajištění ITSec
  - Navrhuje rozpočet pro zajištění ITSec
  - Odpovídá za provedení opravných akcí
  - Ověřuje, že opravné akce nebudou nekonformní
  - S řídicím výborem spoluvytváří BP, určuje její cíle a strategie a stanovuje oblast působení
  - Informuje řídicí výbor o postupu implementace ISMS, o incidentech, o problémech a bezpečnostních záležitostech a aktuálních hrozbách

# Co je pracovní náplní CISO 6/9

- V oblasti zlepšování ISMS
  - Zaručuje, že se provedou všechny opravné akce
  - Ověřuje, zda opravné akce nezpůsobí nesoulad, nekonformnost
- V oblasti správy aktiv
  - Udržuje evidenci všech důležitých informačních aktiv
  - Bezpečně likviduje dále nepoužitelná média a zřízení
- V oblasti styku se třetími stranami
  - Ohodnocuje rizika outsourcovaných aktivit
  - Kontroluje vhodnost kandidátů na outsourcující partnery
  - Definuje položky, které musí obsahovat smlouva s konkrétním partnerem

# Co je pracovní náplní CISO 7/9

- V oblasti komunikací
  - Definuje akceptovatelné a neakceptovatelné komunikační kanály
  - Připravuje komunikační zařízení použitá při katastrofách
- V oblasti zachování kontinuity činnosti
  - Koordinuje proces analýzy dopadů katastrofických incidentů na byznys činnosti a tvorby plánu činnosti po takových incidentech
  - Koordinuje procvičování zaměstnanců a testování plánů
  - Po incidentu oponuje plán obnovy

# Co je pracovní náplní CISO 8/9

- V oblasti technické bezpečnosti
  - Odsouhlasuje vhodné metody pro ochranu v mobilních zařízeních, v sítích a v komunikačních kanálech
  - Navrhuje metody autentizace, politiku hesel, metody šifrování, …
  - Definuje požadované bezpečnostní vlastnosti online služeb
  - Definuje principy bezpečného vývoje informačních systémů
  - Analyzuje záznamy o činnostech uživatelů a odhaluje podezřelé chování
- V oblasti správy dokumentů
  - Navrhuje pracovní verze hlavních dokumentů v oblasti ITSec: Politika ITSec, politika klasifikace aktiv, politika řízení přístupu, metody řízení rizik, prohlášení o aplikovatelnosti, plán zvládání rizik
  - Odpovídá za oponování a aktualizování těchto dokumentů

# Co je pracovní náplní CISO 9/9

- V oblasti správy bezpečnostních incidentů
  - Přijímá zprávy o bezpečnostních událostech a incidentech
  - Koordinuje reakce na bezpečnostní incidenty, vypracovává zprávy o bezpečnostních incidentech, a řídí reakce na ně
  - Připravuje důkazy pro právní řízení po incidentech
  - Analyzuje incidenty vč. prokázání jejich příčin s cílem prevence jejich opakování - určení adekvátních opravných a/nebo preventivních akcí
  - Spolupracuje na plánu zachování činnosti po incidentech
  - Školí a testuje v oblasti zachování činnosti po incidentech
  - Navrhuje korekce plánu zachování činnosti po incidentech