Financované Európskou úniou
NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI
ŽILINSKEJ UNIVERZITY V ŽILINE

# Bezpečnosť pri nadobúdaní, vývoji a údržbe IS a siete, komunikačná bezpečnosť

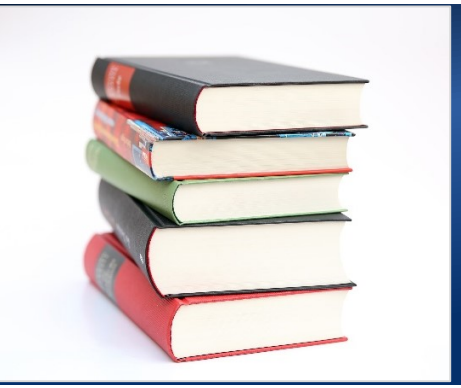
Technické opatrenia (Blok IV)

**Kurz: Manažér kybernetickej bezpečnosti vo verejnej správe**


Milan Kubina

**KC KYB UNIZA; https://kc.uniza.sk/**

milan.kubina@fri.uniza.sk



# Obsah

1. Princípy riadenia a správy informačných systémov
2. Princípy riadenia a správy počítačových sietí
3. Princípy riadenia a správy IT služieb
4. Nástroje, metódy a techniky navrhovania bezpečnostných systémov
5. Bezpečnosť pri nadobúdaní IS a PC sietí
6. Bezpečnosť pri vývoji IS a PC sietí
7. Bezpečnosť pri údržbe IS a PC sietí
8. Bezpečná komunikácia pri vývoji a údržbe IS a PC sietí
9. Podporné opatrenia

# Princípy riadenia a správy IS

- Riadenie a správa IS/IT
- Ciele riadenia IS/IT

# Riadenie a správa IS

- Princípy riadenia informačných systémov (IS) predstavujú základné pravidlá a odporúčania, ktoré organizácie používajú na efektívne
  - plánovanie,
  - prevádzku,
  - kontrolu a
  - rozvoj svojich IS a IT služieb.

- Riadenie a správa IS suvisí s IT governance (riadením IT) a manažmentom IS.
- Riadenie a správa IS nie je „len“ o technológiách, ale hlavne o **strategickom manažmente zdrojov** s cieľom efektívne využívať IS/IT služby pre podporu cieľov organizácie.
- Moderné prístupy vychádzajú z rámcov ako **COBIT, ITIL, IT4IT, ISO/IEC 20000** alebo **TOGAF**.

# Riadenie a správa IS  - ciele

- 1. **Zladenie IS so strategickými cieľmi organizácie**
  - IS musia podporovať biznis procesy, strategické priority a konkurencieschopnosť firmy.
  - Investície do IT by mali mať jasný prínos (ROI, efektívnosť, inovácie).
- 2. **Efektívne plánovanie a architektúra IS**
  - Vypracovanie informačnej stratégie a dlhodobého plánu rozvoja IS/IT.
  - Vytvorenie podnikovej architektúry (Enterprise Architecture – EA), ktorá zabezpečí kompatibilitu, štandardizáciu a flexibilitu systémov.
  - Minimalizácia duplicity dát a aplikácií.
- 3. **Riadenie kvality a dostupnosti informácií**
  - Zabezpečenie presných, úplných a aktuálnych dát.
  - Definovanie zodpovednosti za dáta (data governance).
  - Dostupnosť informácií v správnom čase, mieste a pre oprávnených používateľov.

# Riadenie a správa IS - ciele

- 4. **Bezpečnosť a ochrana dát**
  - Implementácia bezpečnostných politík (autentifikácia, autorizácia, šifrovanie, zálohovanie).
  - Ochrana pred stratou, zneužitím alebo neoprávneným prístupom.
  - Dodržiavanie legislatívy (napr. GDPR).
- 5. **Riadenie životného cyklu IS**
  - IS treba plánovať, budovať, prevádzkovať a modernizovať systematicky (analýza → návrh → implementácia → testovanie → prevádzka → údržba → vyradenie).
  - Priebežné hodnotenie výkonu a návratnosti.
- 6. **Kontrola nákladov a hodnota IS/IT**
  - Sledovanie celkových nákladov na vlastníctvo (TCO) a efektívnosť využitia IT.
  - Prioritizácia projektov podľa prínosu pre organizáciu.
  - Transparentné rozpočtovanie IS/IT.

# Riadenie a správa IS  - ciele

- 7. **Flexibilita a inovácie**
  - IS by mali byť schopné rýchlo reagovať na zmeny trhu a procesov.
  - Podpora digitalizácie, automatizácie, umelej inteligencie a inovácií.
- 8. **Riadenie rizík**
  - Identifikácia a hodnotenie rizík spojených s IS/IT (bezpečnostné incidenty, výpadky, technologické zastaranie).
  - Plány obnovy po havárii (Disaster Recovery, Business Continuity Planning).
- 9. **Zapojenie vrcholového manažmentu a IT governance**
  - Riadenie IS nie je len úlohou IT oddelenia, ale celej organizácie.
  - Vznik IT výborov alebo CIO/CTO funkcie pre strategické rozhodovanie.
- 10. **Orientácia na používateľa a podporu procesov**
  - IS majú zvyšovať produktivitu zamestnancov a zlepšovať zákaznícku skúsenosť.
  - Priebežné školenia a podpora používateľov.

# Princípy riadenia a správy PC sietí

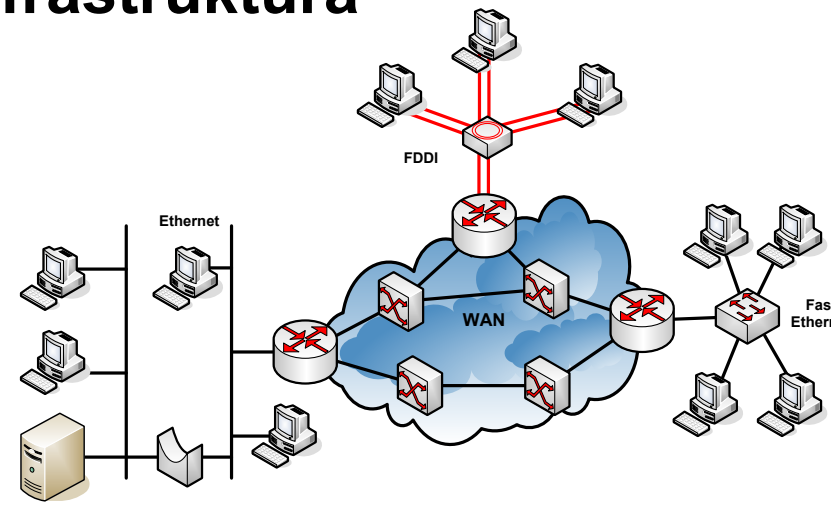
- Východiská
- Princípy
- FCAPS

# Prečo nás zaujíma sieť

- Voľná definícia pojmu „Komunikačná sieť (KS):

  *Súbor koncových staníc a sieťových uzlov prepojených komunikačnými linkami, ktoré umožňujú vzdialenú elektronickú komunikáciu medzi používateľmi alebo koncovými stanicami*

  - Poskytuje komunikačnú službu
- Pozícia komunikačnej siete dnes = **Sieť je kritická infraštruktúra**
  - Spája ľudí, dáta, aplikácie a cloud
    - „*all-is-connected*“, IoT, BYOD, IoE
  - V digitálnej ekonomike => Sieť je chrbtová kosť biznisu
  - Vstupná brána ku všetkým aktívam
    - *Assets (aktíva) v sieti: Dáta, servery, aplikácie, zariadenia*




- Výpadok alebo kompromitácia siete → okamžitý dopad na služby, výrobu, financie

# Prečo nás zaujíma sieť z pohľadu bezpečnosti

## Problém?

- Siete
  - Sami sú ako aj prepájajú aktíva (Assets)
  - Sú konvergované a komplexné (hlas, video, dáta, IoT, cloud)
  - Tvoria ich rôzne HW + SW komponenty
  - => Každý prvok potencionálne obsahuje zraniteľnosti (vulnerabilities)
- Útočníci cielia na tieto slabiny sietí
  - => vznikajú hrozby a riziká

## Pojmy

- Assets:
  - *Čokoľvek hodnotné v organizácii (dáta, servery, aplikácie, zariadenia, služby)*
- Vulnerabilities (zraniteľnosti)
  - *Slabiny v HW, SW, konfigurácii alebo procese, ktoré možno zneužiť*
- Hrozba (Threat / Hrozba)
  - *Potenciálna udalosť, ktorá môže zneužiť zraniteľnosť konkrétneho aktíva a spôsobiť škodu*
  - *Potenciálna nebezpečná udalosť*
- Riziko (Risk)
  - *Pravdepodobnosť, že hrozba zneužije zraniteľnosť aktíva*
  - *Vyjadruje pravdepodobnosť výskytu incidentu*

# Príklady kybernetických hrozieb

- Softvérové útoky
  - Malware, DoS/DDoS, exploitácia zraniteľností
- Softvérové chyby
  - Bugy, výpadky služieb, chybné skripty
- Sabotáž
  - Úmyselné poškodenie systémov oprávneným používateľom
- Ľudské chyby
  - Misconfigurations, slabé heslá, neúmyselné chyby
- Krádež
  - Odcudzenie HW alebo citlivých dát
- HW zlyhania
  - Poruchy zariadení, diskov, sieťových prvkov
- Prerušenie služieb
  - Výpadky elektriny, zlyhanie chladenia, požiarne systémy
- Prírodné katastrofy
  - Povodne, zemetrasenia, požiare, búrky



Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

# Prečo nás zaujíma sieť z pohľadu bezpečnosti

## Problém?

- Slabiny sieti a systémov
  - *Attack surface*
- Útočníci cieliaci na tieto slabiny sietí
  - => Vykonávajú kybernetický útok
- Ako?
  - Realizáciou vektoru útoku cez exploit
- **Cieľ bezpečnosti** = znížiť útočnú plochu potláčaním a protiopatreniami (mitigation)

## Pojmy

- Attack surface
  - *Celkový súčet zraniteľností v danom systéme, ktoré môže útočník využiť*
- Útok (Attack)
  - *Konanie, ktorým sa entita snaží obísť bezpečnostné služby a porušiť politiku*
  - *Môže byť zvonka/zvnútra, pasívny/aktívny*
- Attack vector
  - *Cesta alebo metóda, ktorou sa útočník snaží získať prístup*
  - *Spôsob realizácie útoku*
- Exploit
  - *Mechanizmus, ktorý využíva konkrétnu zraniteľnosť na kompromitáciu aktíva*
- Mitigácia (Mitigation / Zmiernenie)
  - *Opatrenie na zníženie závažnosti alebo pravdepodobnosti zneužitia zraniteľnosti*
  - *Často označované ako countermeasures (protiopatrenia)*

# Princípy riadenia PC sietí

- Princípy riadenia počítačových sietí (**network management**) zahŕňajú základné oblasti a postupy, ktoré umožňujú efektívne a bezpečné fungovanie siete.
- Riadenie PC sietí znamená
  - **monitorovať,**
  - **chrániť,**
  - **konfigurovať,**
  - **optimalizovať a**
  - **dokumentovať** sieť tak,
- aby bola **spoľahlivá, rýchla a bezpečná** pre všetkých používateľov.

# Princípy riadenia PC sietí

- **Centralizované monitorovanie**
  - použitie nástrojov ako Zabbix, PRTG, Nagios.
- **Redundancia a vysoká dostupnosť**
  - záložné linky, failover protokoly (HSRP, VRRP).
- **Automatizácia a skriptovanie**
  - znižuje chybovosť pri správe siete.
- **Štandardizácia protokolov**
  - SNMP, Netconf, Syslog pre zber dát.
- **Proaktívny prístup**
  - problémy riešiť ešte predtým, než spôsobia výpadok.

# FCAPS

- F – Fault, C – Configuration, A – Accounting, P – Performance, S – Security

- Model **FCAPS** je medzinárodne uznávaný rámec (odporúčaný organizáciou **ISO/OSI**), ktorý opisuje hlavné oblasti **riadenia počítačových sietí**.

- Model **FCAPS** rozdeľuje správu siete do **piatich základných oblastí**, aby bola správa **prehľadná, systematická a úplná**.

- Používa sa ako **základ pri návrhu** sieťových monitorovacích a riadiacich systémov

# Riadenie chýb (Fault Management)

- Monitorovanie siete, aby sa čo najrýchlejšie zistili a odstránili poruchy (výpadky, poškodené linky, zlyhanie zariadení).
- Detekcia a hlásenie chýb (notifikácie, alarmy – SNMP traps).
- Lokalizácia problému a jeho odstránenie (napr. prepnutie na záložnú linku).
- Prevencia opakovaných zlyhaní (logy, analýza príčin).

# Riadenie konfigurácie (Configuration Management)

- Centrálna správa konfigurácií sieťových zariadení (routery, switche, firewally).
- Evidencia a dokumentácia zmien (verzovanie, zálohovanie konfigurácií).
- Automatizácia zmien (napr. Ansible, Netconf).
- Dodržiavanie štandardov a politiky nastavení.

# Riadenie účtovania / nákladov (Accounting Management)

- Meranie a evidencia využitia siete jednotlivými používateľmi alebo oddeleniami.
- Rozpočítanie nákladov alebo sledovanie spotreby (bandwidth accounting).
- Identifikácia neefektívneho využitia zdrojov.

# Riadenie výkonu (Performance Management)

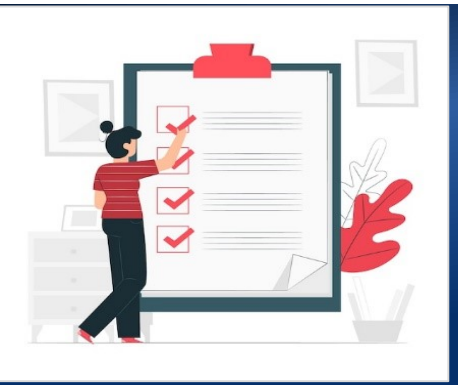
- Sledovanie využitia šírky pásma, latencie, strát paketov, jitteru.
- Optimalizácia výkonu siete – load balancing, QoS (Quality of Service).
- Kapacitné plánovanie (capacity planning) na budúci rast siete.
- Vyhodnocovanie metrík cez monitoring (napr. NetFlow, SNMP, Grafana)

# Riadenie bezpečnosti (Security Management)

- Riadenie prístupových práv (autentifikácia, autorizácia, AAA – RADIUS/TACACS+).
- Monitorovanie bezpečnostných incidentov (IDS/IPS, SIEM systémy).
- Správa firewallov, VPN, segmentácia siete (VLAN, ACL).
- Aktualizácia firmvéru a zabezpečenie proti útokom (patch management).

# Trendy 2025 v sieťovej bezpečnosti

- **AI Phishing a Generatívne útoky**
  - Deepfake hovory, AI-generované e-maily a malvér – útočníci používajú gen AI na sofistikované phishingové kampane
  - Zvýšené využitie AI na personalizované útoky zvyšuje úspešnosť o 20-30% (https://deepstrike.io/blog/top-cybersecurity-threats-2025 )
- **Quantum threats**
  - Ohrozenie asymetrických šifier (RSA, ECC) kvôli quantum computing – potreba prechodu na post-quantum kryptografiu
  - NIST odporúča migráciu, ako útoky na šifrovanie sa stávajú realitou do 2030
- **Supply chain útoky**
  - Kompromitácia dodávateľov a softvéru (napr. SolarWinds 2020, MOVEit 2023) – zameranie na third-party riziká
  - Rast o 15% v 2025, s dôrazom na edge devices a open-source knižnice
- **Cloud & remote work**
  - Rozplývanie perimetra – shift k SASE a Zero Trust pre hybridné prostredia
  - 72% organizácií hlási zvýšené riziká kvôli cloud migrácii a remote access (https://www.sentinelone.com/cybersecurity-101/cybersecurity/cyber-security-statistics/ )
- **Ďalšie kľúčové trendy**
  - **Ransomware evolution:** Sofistikovanejšie taktiky, vrátane double extortion a AI-assisted šírenia
  - **OT cyber threats:** Zvýšené útoky na operačné technológie (IoT, ICS) v kritických sektoroch
  - **Regulačné zmeny:** Prísnejšie normy (NIS2, DORA) nútia k compliance a resilience
  - **AI v obrane:** Použitie gen AI na automatizovanú detekciu a odpoveď na hrozby



# Kvíz

- Aké sú ciele riadenia a správy IS?
- Čo je to **FCAPS** ?
- Aké sú trendy v sieťovej bezpečnosti.

# Princípy riadenia a správy IT služieb

- ITSM
- ISO 20000
- ITIL v4
- IT4IT
- COBIT

# Predstava ideálneho IT sveta

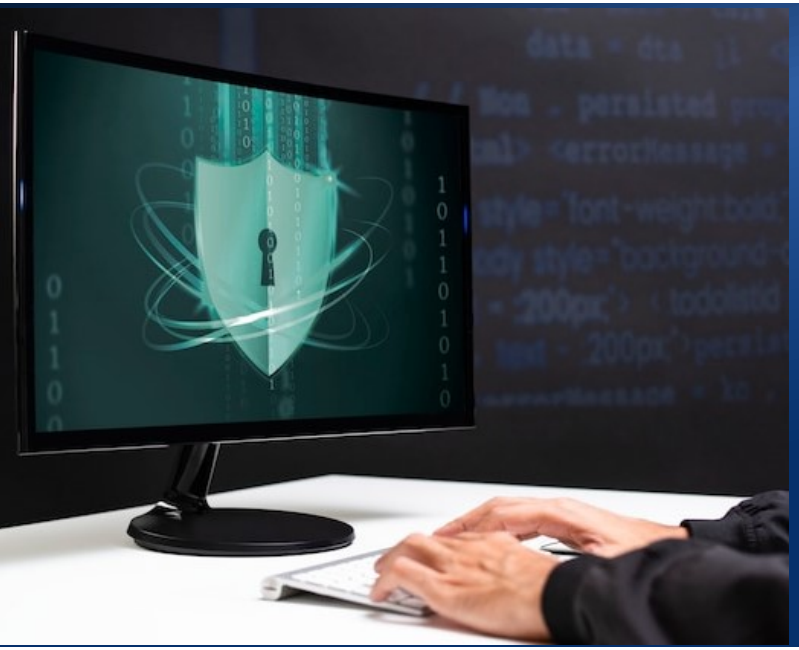
- IT infraštruktúra nikdy nezlyháva
- Všetky IT spolupracujú
- Vždy je k dispozícii aktuálna dokumentácia k IT
- Nové IT sú zavádzané bez problémov
- Užívatelia sú na nové IT vždy vyškolení
- Nikdy nemusíme opakovane riešiť rovnaké problémy
- Používatelia IT služieb sú vždy spokojní ☺



Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

# Prečo podniky investujú do IT?

- IT pomáhajú pri realizácii ich podnikateľských aktivít
- IT zabezpečujú fungovanie podnikových procesov
  - rýchlejšie
  - efektívnejšie
  - spoľahlivejšie
  - lacnejšie atď..
- IT umožňujú podnikom ponúkať nové služby (presun od výrobkov k službám).



# ITSM

# Čo je to služba?

- ITIL® definuje **službu**, a to ako nástroj k poskytovaniu hodnoty zákazníkovi, čiže zákazníkovi pomôže získať také výsledky/výstupy, ktoré potrebuje, ale bez toho, aby bol vlastníkom špecifických nákladov a rizík spojených s poskytnutím a dodávkou tejto služby.
- **PRÍKLAD:**
- **Výstup pre zákazníka**
  - Obchodník chce venovať viac času komunikáciou so zákazníkom
- **Realizovaný službou**
  - Služba napríklad vzdialeného prístupu, ktorý umožňuje spoľahlivý prístup do obchodného IS podniku z mobilných zariadení obchodníka, kt. tak môže promptne reagovať na otázky/požiadavky zákazníka.

# Čo je to IT služba?

- ITIL® definuje IT **službu,** ako špeciálny typ služby, založenej na využití informačných technológií.
- **IT Služba = explicitne definovaná a popísaná funkcionalita, poskytovaná IT, ktorá podporuje, alebo priamo umožňuje fungovanie niektorého biznis procesu / činnosti v podniku.**
- Príklady IT služieb:
  - zabezpečenie bezpečnosti IS/IT
  - prevádzka konkrétneho IS
  - školenia používateľov....
- **Nie je služba**
  - MS Outlook, Exchange server, CISCO router/switch a pod.
- **Je služba**
  - Služba elektronickej pošty s podporou (helpdeskom)

# Riadenie IT služieb v podniku.

*„Riadenie IT služieb existuje skoro tak dlho, ako prvý počítač.“*

- V priebehu času sa vyvinul z **technologicky** orientovaného riadenia na **riadenie IT služieb**.
- V porovnaní s minulými rokmi v popredí **nestojí technologický prístup, ale IT služby**, ktoré umožňujú využitie  IT pre služby v podnikových procesoch.
- Začiatky riadenia IT služieb v podniku začínajú v roku 1989, kedy bol vytvorený úrad - **Office for Government Commerce** (OGC) vo Veľkej Británii.
- Úrad považoval klasické metódy riadenia IT za
  - **nedostatočné**, pretože tie sa zaoberali výlučne riadením technológií a
  - **chýbalo spojenie** medzi IT a podporou podnikových procesov pomocou IT služieb.

# Riadenie IT služieb v podniku.

- *Prečo je nutné sa zaoberať  riadením IT služieb v podniku?*
- *Nestačí robiť len údržbu IT resp. riadiť a manažovať IT ako také? (servery, PC, tlačiarne, aplikácie....)*

*„Stručná odpoveď znie **NIE!“***

- Podnik musí:
  - **definovať a popísať IT služby**, ktoré následne úsek IT poskytuje zamestnancom podniku,
  - **určiť zamestnancov,** ktorí s týmito IT službami pracujú v kontexte ich každodenných činností,
  - **kontinuálne riadiť** tieto IT služby a to na operatívnej, taktickej a hlavne na strategickej úrovni podniku.

# Riadenie IT služieb v podniku.

- Moderné IT sú v dnešnej dobe pre podnik nevyhnuté ale nie **postačujúce!**
- Samotné IT nezabezpečia **tvorbu a fungovanie** IT služieb v podniku ale treba IT služby aj **aktívne riadiť**.

*„Treba zabezpečiť dodávku kvalitných IT služieb podporujúcich podnikateľské ciele organizácie použitím nákladovo optimálnych prostriedkov“*

- Riešenie? použitie **metód/metodík** na tvorbu a riadenie IT služieb s cieľom poskytovať podnikom/zákazníkom **kvalitné IT služby**.



Financované Európskou úniou NextGenerationEU | PLÁN OBNOVY | MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY | KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

# ITSM.

- Disciplína, ktorá sa tejto oblasti venuje, sa volá **IT Service Management**, po slovensky „**riadenie služieb informačných technológií**“.
- ITSM je metóda/metodika riadenia IT služieb v podniku/pre podnik.
- ITSM sa zaoberá riadením **interakcie medzi ľuďmi, procesmi a technológiami (väčšinou informačnými ☺).**
- ITSM zahrňuje v sebe **stratégie**, **vývoj služby, implementáciu, podporu**...všetky procesy súvisiace s IT službou ☺



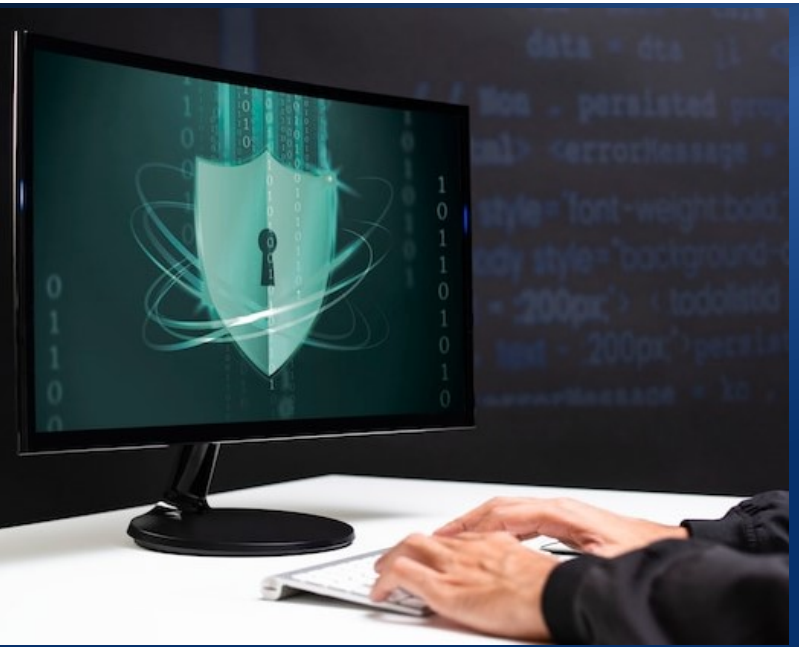
Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

# Definície ITSM

- ITIL® definuje ITSM **ako implementáciu a manažment kvality IT služieb,** ktoré podporujú potreby podniku.
  - Manažment IT služieb vykonávajú poskytovatelia IT služieb pomocou vhodnej zostavy ľudí, procesov a informačných technológií.
- **ITSM je súhrn najlepších skúseností z praxe vo verejnom a súkromnom sektore** a referenčných modelov procesov riadenia služieb informačných technológií.
- **ITSM predstavuje spôsob riadenia IT**, ich prevádzku a rozvoj, ktorý využíva princípy riadenia na báze služieb, čo znamená, že zahŕňa pohľad nie len poskytovateľov IT Služieb, ale aj zákazníkov IT služieb.

# Podstata riadenia IT služieb

- Podstatou Riadenia IT služieb je zmena IT oddelenia na **poskytovateľa IT služieb** s vlastnými internými a externými zákazníkmi.
- Každá činnosť IT oddelenia bude definovaná ako IT služba napr.:
  - podpora používateľov (helpdesk),
  - tlač a kopírovanie,
  - rozosielanie emailov,
  - ochrana a bezpečnosť IS atď.
- Parametre každej IT služby sú definované ako napr.:
  - vlastník IT služby,
  - zdroje pre fungovanie IT služby,
  - výstup IT služby,
  - čas poskytovania IT služby,
  - počet používateľov IT služby atď.



# ISO/IEC 20000

# ISO/IEC 20000-1:2018

- **ISO/IEC 20000** je medzinárodná norma pre **riadenie IT služieb (IT Service Management – ITSM)**.
- Je vnímaná ako „štandardizovaný brat“ ITILu
  - ITIL dáva odporúčania a „best practice“,
  - ISO 20000 stanovuje **formálne požiadavky**, ktoré možno certifikovať/auditovať.
- **Účelom** ISO 20000 je pomôcť organizáciám
  - **zaviesť,**
  - **prevádzkovať,**
  - **monitorovať a**
  - **neustále zlepšovať systém riadenia IT služieb**

# Hlavné časti normy ISO/IEC 20000-1:2018

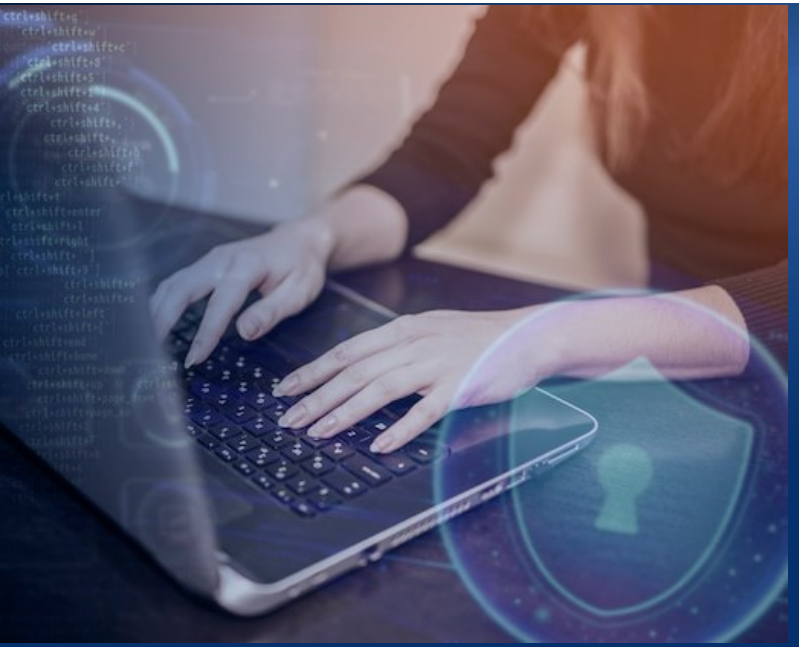
- **Kontext organizácie**
  - Pochopiť potreby zákazníkov, partnerov a interných zainteresovaných strán.
- **Vedenie (Leadership)**
  - Vrcholový manažment musí byť zapojený, definovať politiku, ciele a zodpovednosti.
- **Plánovanie**
  - Hodnotenie rizík a príležitostí, stanovenie merateľných cieľov pre riadenie služieb.
- **Podpora (Support)**
  - Ľudia, kompetencie, komunikácia, dokumentácia a znalosti potrebné na prevádzku SMS.
- **Prevádzka (Operation)**
  - Kľúčové procesy ITSM: riadenie incidentov, problémov, zmien, úrovne služieb, dodávateľov, kapacity, kontinuity, bezpečnosti informácií atď.
- **Hodnotenie výkonnosti (Performance Evaluation)**
  - Monitorovanie, meranie, interné audity, preskúmanie vedením.
- **Zlepšovanie (Improvement)**
  - Neustále zlepšovanie procesov a kvality poskytovaných služieb.

# Kľúčové princípy ISO/IEC 20000

- **Orientácia na zákazníka**
  - služby musia prinášať hodnotu a spĺňať dohodnuté SLA.
- **Integrovaný systém riadenia**
  - procesy musia byť zdokumentované a riadené ako celok.
- **Neustále zlepšovanie**
  - organizácia má pravidelne hodnotiť a zlepšovať svoje ITSM procesy.
- **Manažment rizík a bezpečnosť informácií**
  - zabudovaný do celého systému riadenia IT služby.

| Časť | Názov (skrátene) | Účel |
|---|---|---|
| ISO/IEC 20000-1 | *Service management system requirements* | Hlavná norma – definuje **požiadavky** na systém riadenia služieb (SMS). Podľa nej sa certifikuje organizácia. |
| ISO/IEC 20000-2 | *Guidance on the application of service management systems* | Poskytuje **návod**, ako implementovať požiadavky z časti 1 v praxi. |
| ISO/IEC 20000-3 | *Guidance on scope definition and applicability* | Pomáha stanoviť **rozsah SMS** a rozhodnúť, na ktoré služby a procesy sa bude norma vzťahovať. |
| ISO/IEC 20000-5 | *Exemplar implementation plan* | Vzorový **plán implementácie** SMS podľa časti 1. |
| ISO/IEC 20000-6 | *Requirements for bodies providing audit and certification of service management systems* | Požiadavky na **certifikačné orgány**, ktoré vykonávajú audity ISO 20000-1. |
| ISO/IEC 20000-10 | *Concepts and vocabulary* | Definuje **pojmy a terminológiu** používanú v oblasti riadenia IT služieb. |

| Časť normy | Povaha | Účel |
|---|---|---|
| **ISO/IEC 20000-1** | **POVINNÁ** | Požiadavky na systém riadenia služieb (SMS). Základ pre **certifikáciu organizácie**. |
| **ISO/IEC 20000-2** | Odporúčacia | Návod, ako implementovať požiadavky z časti 1 v praxi. |
| **ISO/IEC 20000-3** | Odporúčacia | Pomáha určiť **rozsah** SMS (čo bude zahrnuté v certifikácii). |
| **ISO/IEC 20000-5** | Odporúčacia | Ukážkový **implementačný plán** krok za krokom. |
| **ISO/IEC 20000-6** | Normatívna pre certifikačné orgány | Požiadavky na **audítorov a certifikačné spoločnosti**. |
| **ISO/IEC 20000-10** | Odporúčacia | Definuje **terminológiu a základné koncepty** ITSM. |



# ITIL

# ITIL

- ITIL poskytuje ucelený **súbor najlepších skúseností z praxe** (best practice) v celom rozsahu správy IT služieb.

- ITIL **pokrýva** jednotlivé oblasti riadenia IT služieb (ľudí, procesy, zdroje..).

- ITIL je najpoužívanejší a celosvetovo uznávaný **prístup k zabezpečeniu dodávky a podpory IT služieb** ako aj k **údržbe IT infraštruktúry**.

# FAKTY O ITILe

- ITIL nie je predpis ani norma
- ITIL je rámec (framework) ITSM **nie** metodika
- Podľa ITILu nie je možné auditovať systém riadenia IT služieb v podniku
- ITIL neobsahuje prevratné „múdrosti“
- ITIL reaguje oneskorene na požiadavky/zmeny trhu

# FAKTY O ITILe

- ITIL je vo vlastníctve britskej spoločnosti **AXELOS**
- AXELOS,  dohliada ešte na ďalšie celosvetovo používané manažérske rámce a metodiky, najznámejšie sú
  - metodika riadenia projektov PRINCE2® ,
  - metodika riadenia rizika M_o_R ®,
  - ....

# VLASTNOSTI ITIL

- **Procesné riadenie -** procesne orientovaný prístup k riadeniu IT služieb,
  - proces je riadený, monitorovaný, meraný, vyhodnocovaný a neustále vylepšovaný (PDCA).
- **Zákaznícky orientovaný prístup -** procesy navrhnuté vzhľadom na potreby zákazníka.
- **Jednoznačná terminológia** - odstraňuje nedorozumenia/slovník.
- **Platformová nezávislosť -** je možné ITIL použiť aj mimo IT, v akomkoľvek podniku, na akýchkoľvek no IT službách.
- **Public Domain -** hocikto môže implementovať vo vlastnej organizácii.

# Životný cyklus IT služby

- Podľa ITIL® vychádza popis každej IT služby
  - zo stratégie (**Service strategy**), ktorá definuje dôvody jej existencie;
  - následne sa služba ako taká navrhne (**Service design**) a zrealizuje;
  - následne sa nasadí do prevádzky (**Service transition**);
  - na každodennej báze sa prevádzkuje (**Service operation**);
  - vo všetkých fázach životného cyklu služby potom prichádza ku neustálemu zlepšovaniu (**Continual service improvement**) všetkých aspektov služby.
- V ITIL® celkom úmyselne chýba fáza vývoja IT služby (**Service development**), lebo na životný cyklus služby tu nazeráme najmä z pohľadu zákazníka/užívateľa.

# ITIL 4

- **Information Technology Infrastructure Library, verzia 4** je najnovší rámec pre **riadenie IT služieb (IT Service Management – ITSM)**.
- Pomáha organizáciám
  - navrhovať,
  - poskytovať,
  - prevádzkovať,
  - neustále zlepšovať IT služby,
- aby prinášali hodnotu zákazníkom a aj biznisu.

# 7 riadiacich princípov ITIL 4

1. Zamerajte sa na hodnotu (**Focus on value**) – všetko, čo robíte, musí prinášať hodnotu zákazníkovi alebo firme.
2. Začnite tam, kde ste (**Start where you are**) – využite existujúce riešenia, nebudujte zbytočne od nuly.
3. Postupujte iteratívne so spätnou väzbou (**Progress iteratively with feedback**) – robte zmeny po menších krokoch a priebežne získavajte odozvu.
4. Spolupracujte a buďte transparentní (**Collaborate and promote visibility**) – komunikujte a zdieľajte informácie naprieč tímami.
5. Myslite a pracujte holisticky (**Think and work holistically**) – vnímajte služby a procesy ako prepojený celok.
6. Udržujte jednoduchosť a praktickosť (**Keep it simple and practical**) – nevytvárajte zbytočnú zložitosť.
7. Optimalizujte a automatizujte (**Optimize and automate**) – zlepšujte procesy a využívajte automatizáciu tam, kde sa to oplatí.

# Systém tvorby hodnoty služby (Service Value System – SVS)

- SVS ukazuje, ako organizácia premieňa dopyt a príležitosti **na hodnotu** pre zákazníkov.

- Hlavné časti SVS:
  - Riadiace princípy (Guiding principles)
  - Riadenie (Governance)
  - Reťazec tvorby hodnoty (Service Value Chain)
  - Praktiky (Practices) – modernizované procesy ITIL
  - Neustále zlepšovanie (Continual Improvement)

# Service Value Chain (reťazec tvorby hodnoty)

- Šesť hlavných aktivít pri tvorbe a poskytovaní služby:

1. Plan – plánovanie cieľov a stratégie IT služieb.
2. Improve – neustále zlepšovanie všetkého, čo organizácia robí.
3. Engage – komunikácia so zákazníkmi a partnermi.
4. Design & Transition – návrh a zavádzanie nových alebo zmenených služieb.
5. Obtain/Build – získanie zdrojov a vývoj komponentov.
6. Deliver & Support – prevádzka, podpora a poskytovanie služieb používateľom.

# Praktiky ITIL 4

- ITIL 4 používa pojem **praktiky** (namiesto starých „procesov“).
- Celkovo existuje 34 praktík, rozdelených na:
  - Všeobecné manažérske (General Management) – napr. riadenie zmien, riadenie rizík, neustále zlepšovanie.
  - Servisné (Service Management) – napr. riadenie incidentov, riadenie problémov, service desk, riadenie úrovne služieb (SLA).
  - Technické (Technical Management) – napr. deployment management, správa infraštruktúry a platforiem.

# Praktiky ITIL 4 /General Management/

- Continual Improvement
  - Neustále hodnotenie a zlepšovanie procesov, služieb a technológií.
- Information Security Management
  - Ochrana informácií a systémov pred hrozbami, zabezpečenie dôvernosti, integrity a dostupnosti dát.
- Project Management
  - Plánovanie, riadenie a dodávanie projektov v súlade s cieľmi organizácie.
- Risk Management
  - Identifikácia, hodnotenie a riadenie rizík spojených s IT službami a technológiami.
- Supplier Management
  - Správa vzťahov s dodávateľmi a sledovanie ich výkonu.

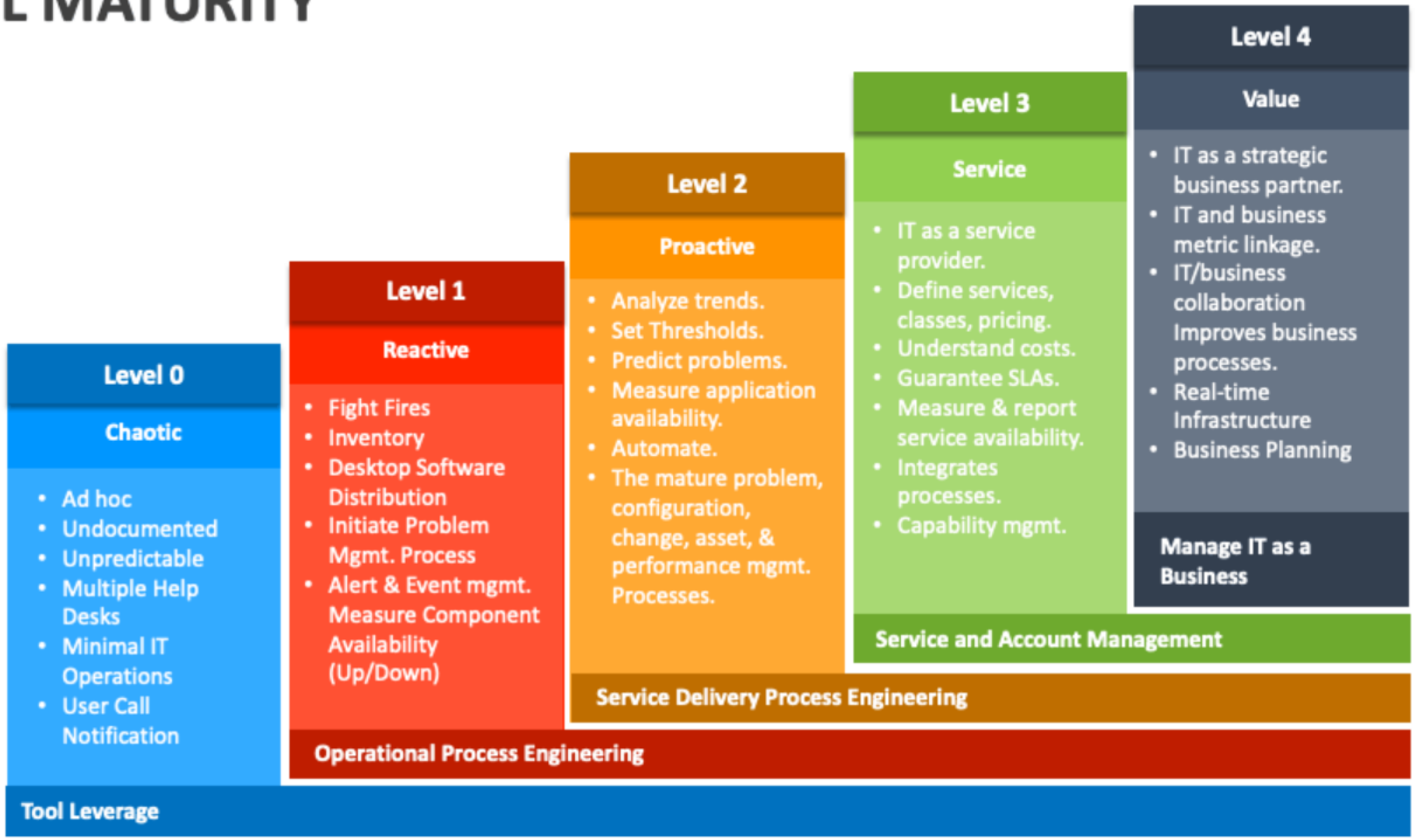
# Praktiky ITIL 4 /Service Management/

- Incident Management
  - Riešenie nečakaných chýb a prerušení služieb tak, aby sa čo najrýchlejšie obnovila bežná prevádzka.
- IT Asset Management
  - Evidencia a správa hardvéru, softvéru a licencií počas celého životného cyklu
- Service Desk
  - Hlavný kontaktný bod medzi používateľmi a IT (zákaznícka podpora, riešenie požiadaviek a eskalácia problémov).
- IT Service Continuity Management
  - Plánovanie obnovy a fungovania služieb pri havárii alebo výpadku (Disaster Recovery).
- Monitoring and Event Management
  - Sledovanie IT prostredia a včasné reagovanie na upozornenia a udalosti.

# Praktiky ITIL 4 /Technical Management/

- Deployment Management
  - Nasadzovanie nových verzií aplikácií a služieb do prevádzky bezpečným a riadeným spôsobom.
- Infrastructure & Platform Management
  - Prevádzka a údržba fyzickej aj cloudovej infraštruktúry a platforiem.
- Software Development & Management
  - Riadenie životného cyklu vývoja softvéru a jeho zlepšovanie.

# ITIL MATURITY




Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

# IT4IT

# IT4IT™

- Moderný rámec pre **riadenie IT ako biznisu,** vytvorila ho organizácia **The Open Group**
- Zameriava sa na **end-to-end hodnotový reťazec IT**
- Poskytuje **referenčný model** pre správu celého životného cyklu IT služieb a riešení.
- IT4IT je **„mapa“** pre riadenie IT ako podnikania (od stratégie až po podporu).
  - **IT = služba pre biznis**, ale IT samotné má aj **vlastné procesy, dáta a hodnotový reťazec**, ktoré treba riadiť systematicky.
  - IT4IT opisuje, **ako má byť IT riadené ako „továreň na služby“**: od plánovania až po prevádzku.
- Definuje **4 hodnotové prúdy** a **dátový referenčný model** pre integrovaný IT manažment.
  - Nerieši detailné procesné postupy (ako ITIL), ale skôr **architektúru IT manažmentu a dátové modely**.

# Štyri hodnotové prúdy (Value Streams)

- **Strategy to Portfolio (S2P)**
  - Premena biznisových požiadaviek na IT stratégiu, plánovanie portfólia služieb a investícií.

| Dátový objekt | Popis |
|---|---|
| Strategy | Strategické ciele IT, smerovanie investícií a služieb. |
| Policy | Pravidlá a štandardy pre IT služby a ich správu. |
| Portfolio Backlog | Zoznam nápadov, iniciatív a investičných požiadaviek. |
| Service Portfolio | Kompletný súpis všetkých IT služieb (plánované, aktívne aj vyradené). |
| Project / Investment | Finančné a projektové dáta o pripravovaných službách. |

# Štyri hodnotové prúdy (Value Streams)

- **Requirement to Deploy (R2D)**
  - Premena požiadaviek na technické riešenia, vývoj, testovanie a nasadzovanie.

| Dátový objekt | Popis |
|---|---|
| Requirement | Požiadavky na službu alebo produkt. |
| Solution Blueprint | Návrh riešenia (architektúra, dizajn). |
| Build Package | Balíček vyvíjaného riešenia pripravený na testovanie/nasadenie. |
| Release | Schválený a pripravený balíček na nasadenie do produkcie. |
| Test Report | Výsledky testovania riešenia. |

# Štyri hodnotové prúdy (Value Streams)

- **Request to Fulfill (R2F)**
  - Riešenie požiadaviek používateľov, katalóg služieb, samoobslužné objednávky, riadenie prístupov.

| Dátový objekt | Popis |
|---|---|
| Service Catalog | Zoznam služieb, ktoré si môže používateľ objednať. |
| Subscription | Záznam o tom, že používateľ/služba má objednanú konkrétnu IT službu. |
| Request | Konkrétna požiadavka používateľa (napr. nový účet, prístup, notebook). |
| Entitlement | Práva a oprávnenia používateľov k službám a zdrojom. |
| Chargeback/Showback | Dáta o nákladoch na službu, ktoré možno fakturovať alebo zobrazovať. |

# Štyri hodnotové prúdy (Value Streams)

- **Detect to Correct (D2C)**
  - Monitorovanie, detekcia problémov, incidentov a ich odstránenie, zlepšovanie prevádzky.

| Dátový objekt | Popis |
|---|---|
| Event | Upozornenie z monitoringu alebo systému. |
| Incident | Záznam o poruche alebo prerušení služby. |
| Problem | Záznam o základnej príčine opakujúcich sa incidentov. |
| Change | Požiadavka na zmenu infraštruktúry alebo služby. |
| Configuration Item (CI) | Konfiguračná položka – komponent služby (server, aplikácia, databáza). |
| Known Error | Dokumentovaná chyba s workaroundom alebo riešením. |
| Defect | Chyba vo vývoji/softvéri identifikovaná počas testov alebo prevádzky. |

# Referenčný dátový model

- IT4IT kladie veľký dôraz na **informácie a ich toky** medzi procesmi.
- **Definuje dátové** objekty (napr. Service Portfolio, Requirements, Release, Incident) a vzťahy medzi nimi.
- IT4IT opisuje **IT ako hodnotový reťazec** a tvrdí, že **dáta sú „chrbtovou kosťou“ riadenia IT**.
- IT4IT  pomáha **automatizovať a integrovať** rôzne IT nástroje (napr. Jira, ServiceNow, DevOps, CMDB, monitoring) do jedného uceleného ekosystému.

# COBIT

# COBIT

- **COBIT** (Control Objectives for Information and Related Technology) je **rámec pre riadenie a správu IT** vytvorený organizáciou **ISACA**.
- Je určený pre manažérov, audítorov a lídrov IT, ktorí chcú mať **pod kontrolou IT procesy, riziká a súlad s biznis cieľmi a reguláciami**.
- Cieľom COBITu je poskytnúť **štandardizovaný rámec** pre **riadenie IT** (IT Governance = strategická úroveň) a zabezpečiť, že IT podporuje biznis ciele.
- COBIT slúži najmä na:
  - riadenie IT portfólia a investícií,
  - interné a externé audity IT,
  - zosúladenie s legislatívou,
  - podpora bezpečnosti a riadenia rizík.

- **Aktuálna verzia: COBIT 2019** (predtým COBIT 5)

# Kľúčové princípy COBIT

- **Zameranie na hodnotu pre stakeholderov**
  - IT musí prinášať hodnotu a podporovať biznis ciele.
- **Pokrytie celého podniku od konca po koniec**
  - nielen IT oddelenie, ale celý podnikový IT ekosystém.
- **Integrovaný rámec riadenia**
  - zosúlaďuje sa s inými štandardmi (ISO 20000, ITIL, TOGAF, NIST…).
- **Prispôsobenie podľa potrieb**
  - rámec je modulárny, prispôsobuje sa veľkosti a odvetviu firmy.
- **Rozdelenie medzi správu (Governance) a riadenie (Management)**
  - jasne rozlišuje strategické rozhodovanie a operačné riadenie.



Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

# Riadenie vs. manažment podľa COBIT

- **Governance (správa):**
  - nastavuje smerovanie a pravidlá IT,
  - rozhoduje o prioritách a rizikách,
  - hodnotí, či IT prináša očakávanú hodnotu.

- **Management (riadenie):**
  - zabezpečuje plánovanie, prevádzku a implementáciu riešení podľa pravidiel governance.

# Štruktúra COBIT (Core Model)

- COBIT používa **„Core Model“**, ktorý je rozdelený do **domén**, každá doména obsahuje **procesy/praktiky (40)** s cieľmi a metrikami.

| Doména | Skratka | Obsah |
|---|---|---|
| Evaluate, Direct and Monitor | EDM | Strategické riadenie IT (hodnota, riziká, súlad s reguláciami). |
| Align, Plan and Organize | APO | Plánovanie IT stratégie, architektúry, investícií, vzťahy so stakeholdermi. |
| Build, Acquire and Implement | BAI | Vývoj a nasadenie riešení, riadenie zmien, riadenie projektov. |
| Deliver, Service and Support | DSS | Prevádzka IT služieb, podpora používateľov, riešenie incidentov, bezpečnosť. |
| Monitor, Evaluate and Assess | MEA | Monitoring, interné audity, dodržiavanie súladu, meranie výkonnosti. |

# COBIT procesy EDM

| Kód | Názov procesu | Stručná charakteristika |
|---|---|---|
| EDM01 | Ensure Governance Framework Setting and Maintenance | Definovanie a udržiavanie rámca správy IT, zásad a zodpovedností. |
| EDM02 | Ensure Benefits Delivery | Dohľad, že IT prináša hodnotu a očakávané prínosy. |
| EDM03 | Ensure Risk Optimization | Strategické riadenie a akceptácia rizík spojených s IT. |
| EDM04 | Ensure Resource Optimization | Efektívne využívanie ľudí, financií, infraštruktúry a dát. |
| EDM05 | Ensure Stakeholder Transparency | Poskytovanie správnych informácií stakeholderom o IT výkone a rizikách. |

# COBIT procesy APO

| Kód | Názov procesu | Stručná charakteristika |
|---|---|---|
| APO01 | Manage the IT Management Framework | Riadenie celého IT manažment systému, politík a štandardov. |
| APO02 | Manage Strategy | Definovanie IT stratégie v súlade s biznis cieľmi. |
| APO03 | Manage Enterprise Architecture | Plánovanie a udržiavanie podnikovej a IT architektúry. |
| APO04 | Manage Innovation | Podpora inovácií, hľadanie nových IT riešení pre biznis. |
| APO05 | Manage Portfolio | Riadenie portfólia IT investícií, projektov a služieb. |
| APO06 | Manage Budget and Costs | Plánovanie a sledovanie nákladov na IT. |
| APO07 | Manage Human Resources | Riadenie IT zručností, kapacít a kariérneho rozvoja. |
| APO08 | Manage Relationships | Budovanie a udržiavanie vzťahov s internými aj externými stakeholdermi. |
| APO09 | Manage Service Agreements | Definovanie a správa SLA/OLA a dohôd o úrovni služieb. |
| APO10 | Manage Vendors | Správa dodávateľov, zmlúv a ich výkonnosti. |
| APO11 | Manage Quality | Zavedenie a udržiavanie systému kvality v IT. |
| APO12 | Manage Risk | Identifikácia a riadenie rizík spojených s IT. |
| APO13 | Manage Security | Definovanie stratégie a riadenie informačnej bezpečnosti. |

# COBIT procesy BAI

| Kód | Názov procesu | Stručná charakteristika |
|---|---|---|
| BAI01 | Manage Programs and Projects | Plánovanie a riadenie IT projektov a programov. |
| BAI02 | Manage Requirements Definition | Zhromažďovanie a spracovanie požiadaviek na IT riešenia. |
| BAI03 | Manage Solutions Identification and Build | Návrh a vývoj nových riešení alebo služieb. |
| BAI04 | Manage Availability and Capacity | Plánovanie dostupnosti a kapacity systémov. |
| BAI05 | Manage Organizational Change Enablement | Podpora zmeny procesov a kultúry pri zavádzaní nových IT riešení. |
| BAI06 | Manage Changes | Riadenie zmien v IT prostredí (change management). |
| BAI07 | Manage Change Acceptance and Transitioning | Nasadzovanie nových služieb do produkcie. |
| BAI08 | Manage Knowledge | Riadenie znalostí a dokumentácie o IT riešeniach. |
| BAI09 | Manage Assets | Evidencia a správa IT majetku počas celého životného cyklu. |
| BAI10 | Manage Configuration | Udržiavanie presných informácií o IT komponentoch (CMDB). |

# COBIT procesy APO

| Kód | Názov procesu | Stručná charakteristika |
|---|---|---|
| DSS01 | Manage Operations | Riadenie každodennej prevádzky IT služieb. |
| DSS02 | Manage Service Requests and Incidents | Spracovanie požiadaviek používateľov a riešenie incidentov. |
| DSS03 | Manage Problems | Identifikácia a odstraňovanie hlavných príčin opakujúcich sa problémov. |
| DSS04 | Manage Continuity | Riadenie IT kontinuity a plánovanie obnovy po havárii (DRP/BCP). |
| DSS05 | Manage Security Services | Prevádzka a podpora bezpečnostných služieb (napr. monitoring hrozieb). |
| DSS06 | Manage Business Process Controls | IT podpora a kontrola biznis procesov podľa compliance požiadaviek. |

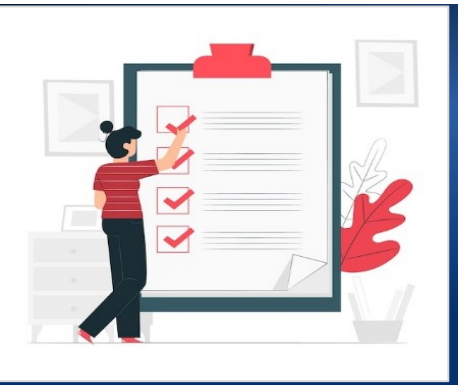
# COBIT procesy MEA

| Kód | Názov procesu | Stručná charakteristika |
|---|---|---|
| MEA01 | Monitor, Evaluate and Assess Performance and Conformance | Sledovanie výkonnosti IT a súladu s politikami a štandardmi. |
| MEA02 | Monitor, Evaluate and Assess the System of Internal Control | Hodnotenie interných kontrol IT prostredia. |
| MEA03 | Monitor, Evaluate and Assess Compliance with External Requirements | Posúdenie zhody s externými reguláciami a legislatívou. |

# Záver COBIT

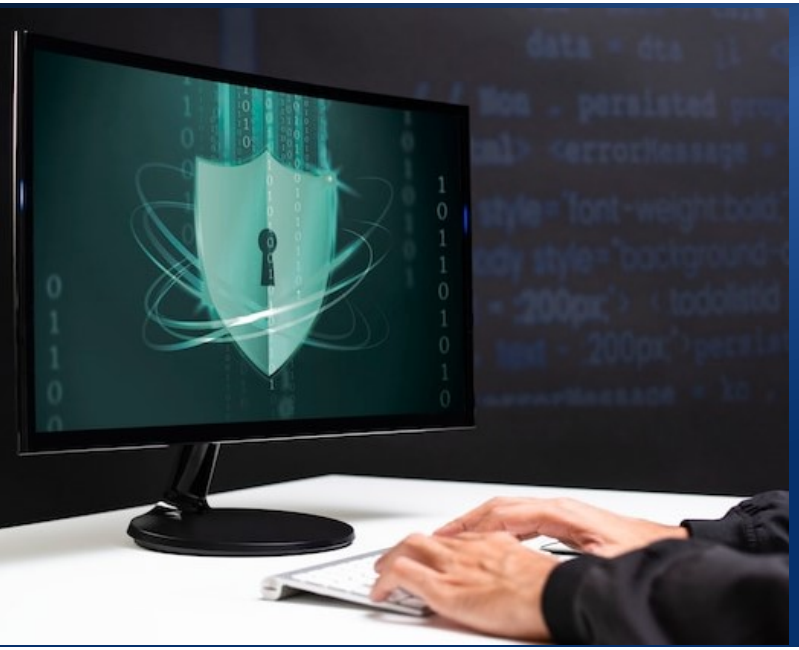
- COBIT je často „**meta-rámec**“ – pomáha zosúladiť a riadiť viacero iných štandardov.

| Rámec | Zameranie |
|---|---|
| COBIT | Riadenie a správa IT na strategickej úrovni |
| ITIL 4 | Prevádzka a poskytovanie IT služieb (ITSM) |
| ISO/IEC 20000 | Certifikovateľné požiadavky na ITSM |
| TOGAF | Podniková architektúra |
| NIST/ISO 27001 | Bezpečnosť a riadenie informačných rizík |



# Kvíz

- Na čo slúži ISO20000
- Čo je ITIL
- Čo je IT4IT
- Čo je COBIT



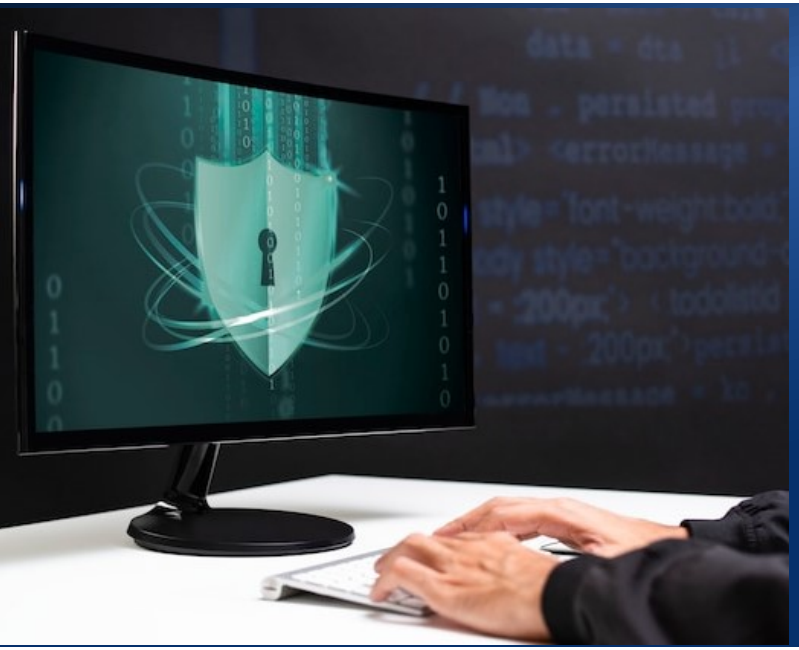
# Bezpečnosť pri nadobúdaní IS a PC sietí

# Bezpečnosť pri nadobúdaní IS

- Bezpečnostné požiadavky v zmluvách – už pri výbere dodávateľa musia byť definované požiadavky na bezpečnosť (napr. šifrovanie, prístupové práva, audit).
- Posudzovanie rizík – pred nasadením systému/siete treba identifikovať a vyhodnotiť riziká (technické aj organizačné).
- Kontrola dodávateľov – preveriť reputáciu, certifikácie, skúsenosti a schopnosť dodržiavať bezpečnostné štandardy.
- Licencie a právne aspekty – zabezpečiť, že používanie softvéru je legálne a zmluvne kryté (napr. GDPR, ochrana duševného vlastníctva...).
- Legislatíva napr.
  - zákon č. 343/2015 Z. z. o verejnom obstarávaní
  - zákon č. 69/2018 Z. z. o KB + vyhlášky
  - zákon č. 95/2019 Z. z. o ITVS + vyhlášky

# SLA

- SLA (Service Level Agreement – dohoda o úrovni poskytovaných služieb) pri nadobúdaní informačného systému je kľúčový dokument, ktorý definuje **parametre prevádzky, údržby a bezpečnosti systému** po jeho dodaní.
- Ak má byť dôraz na **kybernetickú bezpečnosť**, SLA musí byť rozšírená o špecifické bezpečnostné požiadavky, metriky a sankcie.
- Bezpečnostné požiadavky v SLA (Cybersecurity Clauses):
  - Prístupové práva - Silná autentifikácia (MFA), princíp minimálnych oprávnení (least privilege)
  - Aktualizácie a patchovanie - Kritické bezpečnostné záplaty do 24 h od vydania, ostatné podľa dohody.
  - Šifrovanie - Povinné šifrovanie dát v pokoj
  - Zálohovanie a obnova - Denné zálohy, test obnovy minimálne 1× ročne.
  - Monitoring a logovanie -Logovanie prístupov (min. 1 rok archivácia logov).
  - atď.



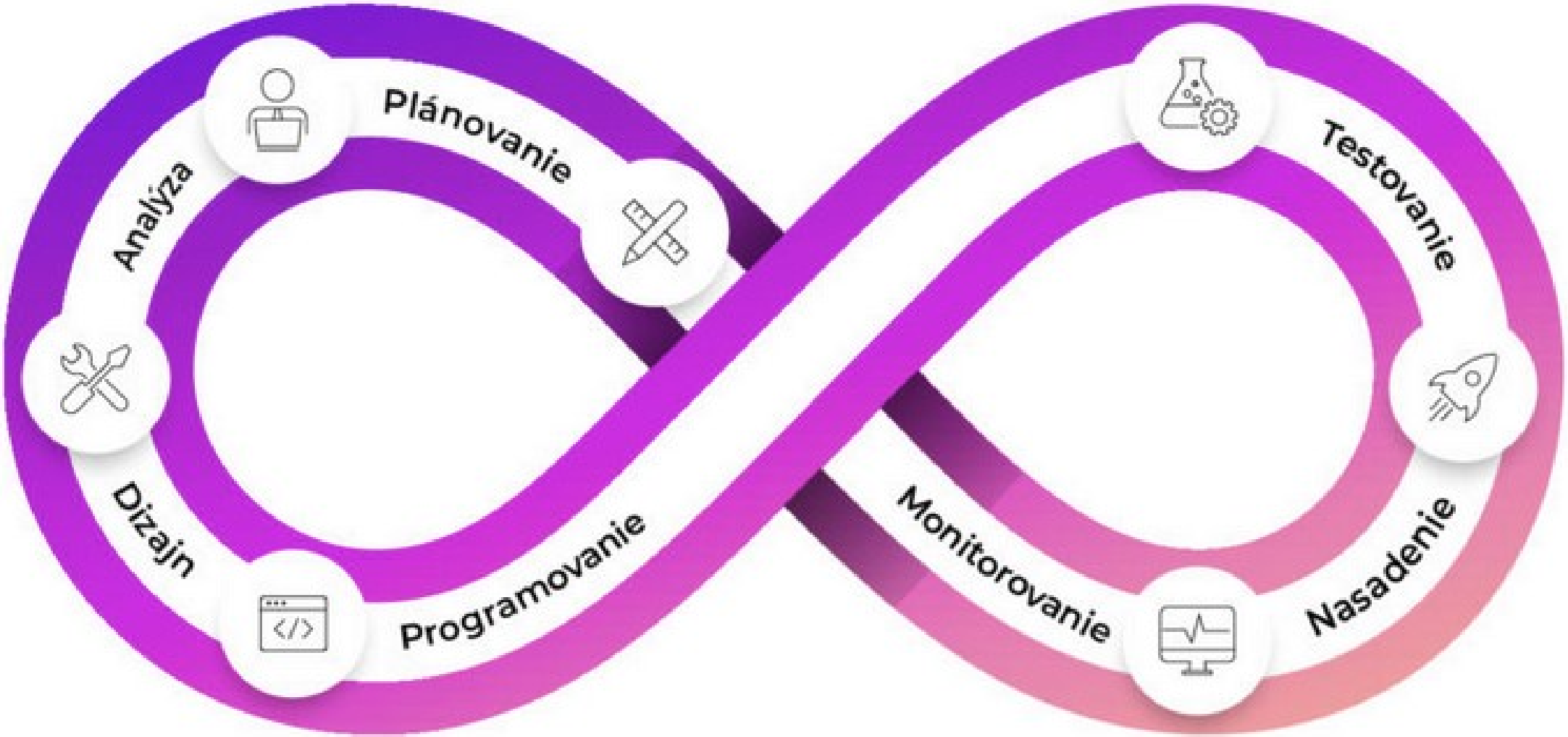
# Bezpečnosť pri vývoji IS a PC sietí

# Bezpečnosť pri vývoji IS

- Bezpečný životný cyklus vývoja (SDLC) – bezpečnosť má byť integrovaná do každej fázy vývoja (analýza, návrh, implementácia, testovanie, nasadenie).
- Bezpečnostné požiadavky v špecifikáciách – už pri návrhu treba počítať s autentifikáciou, autorizáciou, ochranou dát, logovaním.
- Bezpečné programovanie – používať zásady ako validácia vstupov, ochrana pred SQL injection, XSS, buffer overflow.
- Testovanie a audit – pravidelné penetračné testy, code review, statická a dynamická analýza kódu.
- Ochrana zdrojového kódu –systém pre verzionovanie s kontrolou prístupu, šifrovanie citlivých komponentov.

# SDLC = System Development Life Cycle

- SDLC **metodický rámec** pre projekty vývoja IS.
- SDLC predstavuje **procesný/fázový prístup** projektu vývoja IS.
- SDLC je definovaný ako **séria krokov**, ktoré sa dodržiavajú pri vývoji akéhokoľvek IS/SW s cieľom splniť alebo prekročiť stanovené očakávania / požiadavky zákazníkov.
- Poskytuje zákazníkom prehľad o vývoji;
  - sleduje všetky úlohy a termíny a ich plnenie;
  - pomáha držať sa vopred stanoveného rozpočtu;
  - pomáha dodržať všetky požiadavky zákazníkov.


Analýza
Plánovanie
Dizajn
Programovanie
Testovanie
Monitorovanie
Nasadenie

# SDLC - Plánovanie

- Pomáha jasne definovať**:**
  - **rozsah,**
  - **ciele,**
  - **účel** nového IS,
  - vypočítať **náklady** na vývoj nového IS,
  - **stanoviť harmonogram** projektu vývoja IS,
  - **vytvoriť projektový tím** pre vývoj IS.
- Poukazuje na **hlavné riziká** a potenciálne problémy, ktoré sa môžu počas procesu vývoja softvéru vyskytnúť.

# SDLC - Plánovanie

- Plánovanie znamená špecifikáciu:
  - časových termínov a
  - postupnosť krkov/činností,
  - ľudských zdrojov a rolí/funkcií,
  - finančných zdrojov,
  - materiálnych zdrojov ,
  - metodík, ktoré budú použité v jednotlivých fázach vývoja IS,
  - check pointy v rámci projektu
  - ....



Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

# SDLC - analýza

- Fáza, v ktorej je **detailne** analyzovaný riešený problém a následne sú špecifikované požiadavky klienta na vývoj IS.
- **Požiadavka** je nejaká potreba zainteresovanej strany (zákazníka)
  - Funkčná požiadavka špecifikuje funkčný aspekt softvéru, definuje nejakú funkciu systému alebo podsystému ako napr. výpočet penále za omeškanú platbu....
  - Nefunkčná požiadavka definuje očakávané charakteristiky IS, ako sú napríklad bezpečnosť, spoľahlivosť, dostupnosť...

# SDLC - analýza

- Všetky požiadavky sú spísané v dokumente = **špecifikácia softvérových požiadaviek** (SRS document = Software Requirements Specification)

- **Špecifikácia** z pohľadu AIS je technickým dokumentom s analyzovanými požiadavkami, kde sú popísané najmä
  - vlastnosti a
  - správanie sa IS

- Požiadavky sú prevedené do technického jazyka pre tím vývojárov IS.

# SDLC - návrh

- **Návrh** – vypracovať čo najpresnejšiu, najrobustnejšiu, najúčinnejšiu a nákladovo najvýhodnejšiu architektúru IS
- Pozostáva z 2 prístupov k návrhu:
  - **logický** – časť fázy návrhu, v ktorej sú všetky funkčné vlastnosti IS popísané nezávisle od konkrétnej realizácie/technológie.
  - **fyzický** – časť fázy návrhu, v ktorej je logický návrh transformovaný do technologicky špecifického návrhu.

- Táto fáza je dokumentovaná v **špecifikácii konštrukčného dokumentu** (DDS = Detailed Design Specification ).

- Fáza návrhu zahŕňa vývoj prototypu resp. predprodukčnej verzie IS
- Zákazníci podávajú spätnú väzbu a vývojári ju používajú na vylepšenie IS.

# SDLC - návrh

Počas tejto fázy sa načrtnú aspekty:

- **Architektúry IS** (dizajn**,** šablóny štandardy)
- **Používateľského rozhrania** – definuje spôsoby, akými zákazníci interagujú s IS a ako IS reaguje na ich vstupy
- **Platformy** (Apple, Android, Windows, Linux ..)
- **Programovania** –programovací jazyk, metódy riešenia problémov a vykonávania úloh v aplikácii
- **Zabezpečenia** –opatrenia na zabezpečenie resp. bezpečnosť IS...
- **Požiadavky na komunikáciu**
- **Požiadavky na databázy**
- **....**

# SDLC - programovanie

- Vývojový tím mení špecifikácie produktu a obchodné požiadavky na kód, ktorý vytvára produkt = **PROGRAMOVANIE/VÝVOJ.**
- Táto fáza je dokumentovaná ako dokument zdrojového kódu (SCD = *source code documentation*).
- Táto fáza je tiež najdlhšou a jednou z najdôležitejších fáz životného cyklu vývoja IS.
- Samotný vývoj môže trvať pomerne dlho, preto je dôležité mať stanovený časový plán a míľniky, aby vývojári IS pochopili očakávania a aby sa mohol sledovať pokrok v tejto fáze.

# SDLC - testovanie

- Vyvinutý IS je odoslaný na testovanie, kde sa na IS vykonávajú rôzne typy testovania a hľadajú sa chyby.
- Proces testovania môže tiež pomôcť odstrániť chyby a závažné problémy s používateľským prostredím ako aj problémy so zabezpečením.
- Typy (možné) testovania, ktoré treba v tejto fáze vykonať:
  - testovanie výkonu
  - funkčné testovanie
  - testovanie bezpečnosti
  - integračné testy
  - akceptačné testy
  - .....

# SDLC - nasadenie

- **Nasadenie resp. implementácia** – fáza, v ktorej je IS/riešenie realizované u zákazníka.

- IS je v tejto fáze naďalej testovaný (existuje rozsah opráv chýb, ktoré neboli zistené počas testovacej fázy).
  - existuje tu priestor na aktualizáciu IS pomocou novších verzií a najnovších bezpečnostných záplat a technológií.

# SDLC - monitorovanie

- **Monitorovanie resp. údržba** – finálna fáza, kedy je systém systematicky udržiavaný a zlepšovaný ☺.

- Vo fáze údržby môžu používatelia nájsť chyby a omyly, ktoré boli prehliadnuté v predchádzajúcej fázach.
  - V niektorých prípadoch môžu viesť k návratu k prvej fáze životného cyklu vývoja softvéru.

# SSDLC – security SDLC

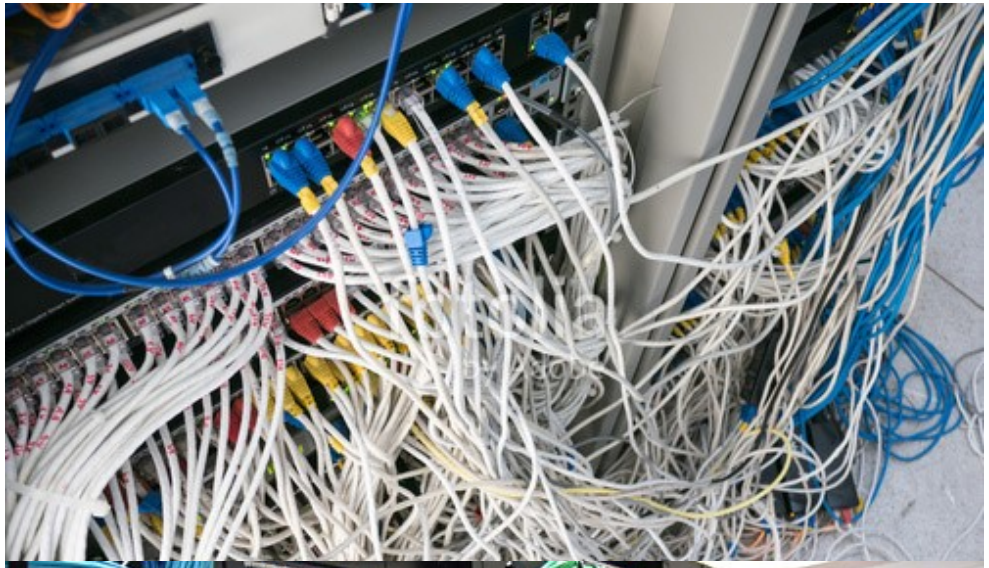
- **Security SDLC** je **rozšírená verzia klasického SDLC**, ktorá má za cieľ zahrnúť bezpečnosť **do každého kroku vývoja softvéru/IS**, nie len na konci ☺.
- Ide o proces vývoja softvéru, kde sa bezpečnostné požiadavky, analýzy, testy a kontroly implementujú už od prvotného plánovania až po údržbu.
  - Cieľ: **minimalizovať zraniteľnosti** a zabezpečiť, že aplikácia/IS spĺňa bezpečnostné štandardy a predpisy.
- Výhody SSDLC:
  - Prevencia drahých bezpečnostných chýb už v raných fázach
  - Vyššia dôveryhodnosť finálneho produktu
  - Splnenie regulačných a právnych požiadaviek
  - Lepšia ochrana dát a reputácie organizácie.

# Bezpečnosť pri vývoji PC sietí

- Budovanie počítačových sietí už dávno nie je iba o prepájaní zariadení. Moderné siete musia byť **odolné voči kybernetickým hrozbám**, poskytovať **spoľahlivý prístup k službám** a zároveň chrániť **citlivé údaje**.
- Bezpečnosť pri **vývoji a budovaní počítačových sietí** znamená, že už v **návrhu architektúry, implementácii a prevádzke** sa berú do úvahy riziká a opatrenia, ktoré chránia dáta, zariadenia aj používateľov pred útokmi a zlyhaním.
- Pri vývoji novej siete je dobré aplikovať rámce a odporúčania ako napr.:
  - **ISO/IEC 27033** (Sieťová bezpečnosť).
  - **NIST SP 800-115** (Testing and Vulnerability Assessment).
  - **Zero Trust Architecture** – žiadne implicitné dôverovanie sieťovým zónam.
- Pri návrhu je preto potrebné uplatňovať princíp **„security by design“** – bezpečnosť sa rieši už v prvotnej fáze plánovania a nie až dodatočne.

# Prečo potrebujeme plánovať bezpečnostnú architektúru

- Ad-hoc riešenia → chaos
  - Slabá odolnosť, ťažká správa, vyššie riziko incidentov
  - Príklad: WannaCry 2017 – nesegmentovaná sieť viedla k globálnemu výpadku
- Systematický dizajn → konzistentnosť
  - Predvídateľnosť správania / reakcie na útok
  - Auditovateľnosť pre regulácie (NIS2)
  - Jednoduchšia správa siete
- Plánovanie = základ pre:
  - **Bezpečnosť** – minimalizácia rizík (napr. segmentácia proti šíreniu)
  - **Škálovateľnosť** – pripravenosť na rast, rozšírenie
  - **Spoľahlivosť siete** – stabilná prevádzka, stabilita služieb
- Frameworky a metodiky pomáhajú
  - Určiť priority
  - Zjednotiť prístup (NIST CSF, SABSA, TOGAF)



# Architektúry sieťovej bezpečnosti ako stavebný princíp

- Architektúra ≠ produkt
  - Plán a princíp budovania bezpečnosti
  - Nejde o konkrétne zariadenie (napr. firewall, IDS), ale o **koncept, plán a princípy**
  - Určuje ***čo, kde a ako***
  - Výsledok ➔ Konzistentný a odolný dizajn siete namiesto ad-hoc riešení
- **Tradičné modely sieťovej bezpečnosti**
  - Perimeter-based security
  - Defense in Depth (Viacvrstvová obrana)
- **Moderné modely**
  - **Zero Trust Architecture (ZTA)**
  - **SASE (Secure Access Service Edge)**
  - **Iné**

## Odkiaľ začať? Urči postup nasadenia

# Top-down vs. bottom-up prístup k implementácií

## Top-down (zhora nadol)

- Vychádza z biznis požiadaviek, procesov a regulácií
- Strategický a systematický prístup
  - Od cieľov po technológie
    - Biznis ciele → analýza aktív → analýza rizík → návrh bezpečnostných zón a politík → výber technológií
- Výhody
  - Zhoda s podnikovými prioritami, komplexný pohľad
  - Konzistentnosť naprieč celou organizáciou
- Nevýhody
  - Časovo náročné, vyžaduje manažérsku podporu

## Bottom-up (zdola nahor)

- Iniciované technickými tímami (admins)
  - Začína od **konkrétnych technických riešení** (FW, IDS, ACL)
  - Postupne sa ad-hoc rozširuje
- Reaktívny prístup v praxi
  - Incident → kúpa technológie
    - Orientované na rýchle riešenia („kúpme firewall, lebo bol incident“)
- Výhody
  - Rýchla implementácia, technická presnosť
- Nevýhody
  - Riziko nesúladu s biznis potrebami, riziko nekonzistencie a slabých miest

**Best practice => kombinácia**

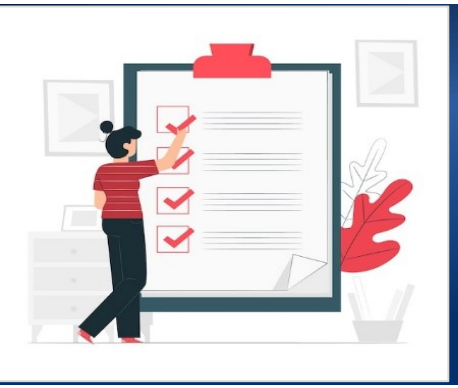
- **Top-Down**: strategické projekty, enterprise architektúra, compliance
- **Bottom-Up**: rýchle reakcie na incidenty, pilotné projekty.

# Risk-based prístup – hodnotenie rizík

- **Rizikovo-orientovaný prístup** = základ plánovania bezpečnostnej architektúry
  - Top-down či bottom-up – v oboch prípadoch potrebujeme systematicky hodnotiť riziká
    - => to určí priority

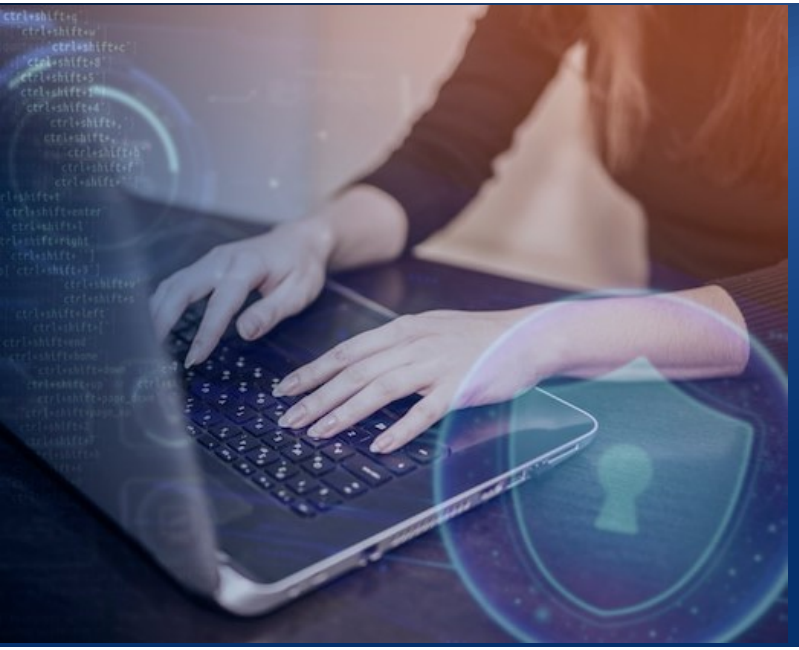
- Kľúčové kroky hodnotenia rizík
  - **Identifikácia aktív** (asset inventory)
    - Čo chránime?
      - Dáta, systémy, služby, servery
  - **Identifikácia hrozieb a zraniteľností**
    - Čo ich ohrozuje? (phishing, misconfig).
  - **Odhad pravdepodobnosti a dopadu** (risk matrix)
    - Aké je riziko?
    - Riziko = dopad × pravdepodobnosť
  - **Prioritizácia rizík** (high impact/high likelihood)
    - Podľa rizika a biznis dopadov
  - **Mitigácia - výber a implementácia kontrol**
    - Ako znížiť riziko?
      - FW, IDS/IPS, segmentácia, zálohy
  - **Kontinuálne monitorovanie a revízia**

- **Výhody**
  - Efektívne využitie zdrojov
    - Fokus na najväčšie hrozby
  - Prispôsobenie sa špecifickým potrebám
    - Napr. úradov, školám
  - Lepšia komunikácia s manažmentom
  - Podpora súladu (ISO 27001, NIST CSF)



# Kvíz

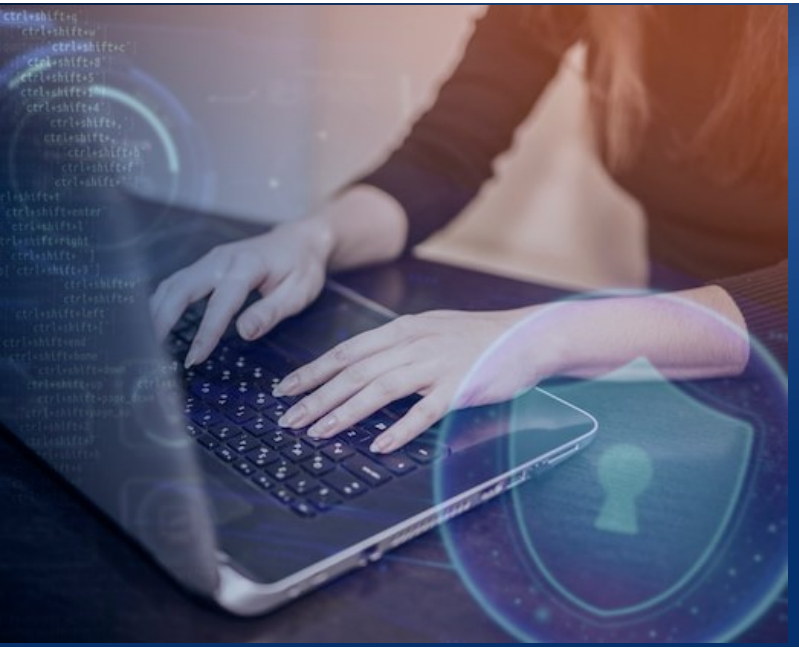
- Špecifikuj SLA z pohľadu KB
- Vymenuj SDLC fázy



# Bezpečnosť pri údržbe IS a PC sietí

# Bezpečnosť pri údržbe IS a PC sietí

- Patch management – pravidelné aktualizácie a opravy zraniteľností.
- Kontrola zmien (Change Management) – každá zmena musí byť schválená, zdokumentovaná a otestovaná.
- Monitorovanie a logovanie – zaznamenávať udalosti (neúspešné prihlásenia, zmeny v systéme, prístup k citlivým dátam).
- Incident management – postupy, ako riešiť bezpečnostné incidenty, aby sa minimalizoval dopad.
- Zálohovanie a obnova – pravidelné zálohy, testovanie obnovy a zabezpečenie proti neoprávnenému prístupu.
- Vyraďovanie systémov – pri ukončení životného cyklu treba bezpečne zlikvidovať alebo anonymizovať dáta.
- Dobrá SLA ☺



# Bezpečná komunikácia pri vývoji IS a PC sietí

# Základné princípy bezpečnej komunikácie

- 1. **Dôvernosť (Confidentiality)**
- Dáta musia byť chránené pred neoprávneným prístupom.
- Praktické opatrenia:
  - Šifrovanie dát pri prenose (TLS/HTTPS, VPN, IPSec).
  - Silná autentifikácia používateľov (heslá, MFA, certifikáty).
  - Oddelenie interných a verejných sietí (firewall, VLAN).
- 2. **Integrita (Integrity)**
- Dáta nesmú byť zmenené alebo poškodené počas prenosu.
- Praktické opatrenia:
  - Digitálne podpisy a hash funkcie (SHA-256, SHA-3).
  - Používanie protokolov s kontrolou integrity (TLS MAC, IPsec AH).
  - Ochrana pred útokmi typu Man-in-the-Middle (MITM).

# Základných princípy bezpečnej komunikácie

- 3. **Autentifikácia a autorizácia**
- Autentifikácia – overenie identity komunikujúcich strán (napr. serverový certifikát, používateľské meno + heslo + MFA).
- Autorizácia – udelenie prístupových práv iba oprávneným používateľom.
  - Praktické opatrenia: PKI infraštruktúra, OAuth2, Kerberos.
- 4. **Dostupnosť (Availability)**
- Služby a dáta musia byť dostupné oprávneným používateľom.
- Praktické opatrenia:
  - Ochrana pred DDoS útokmi.
  - Zálohy a redundancia sietí a serverov.
  - SLA pre dostupnosť (monitoring, reakčný čas).

# Základných princípy bezpečnej komunikácie

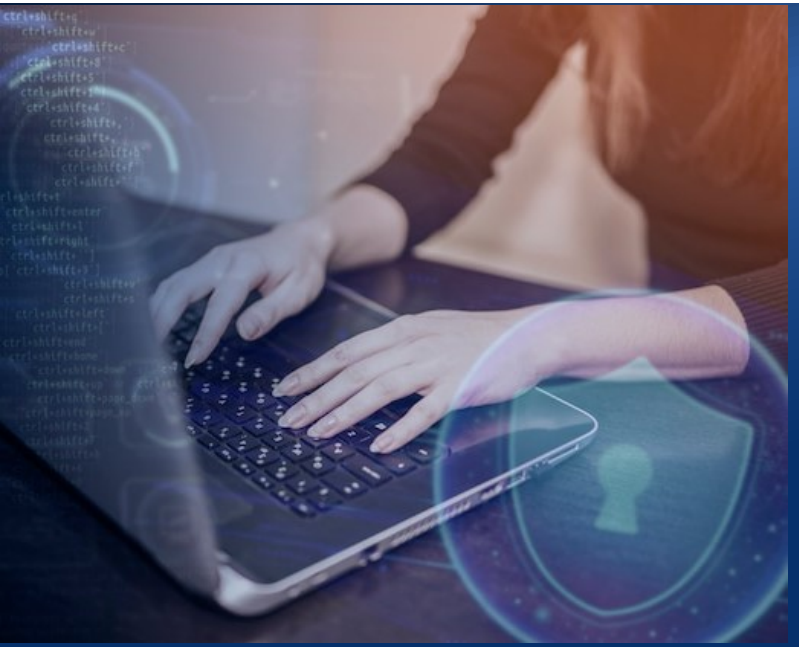
- 5. **Nepopierateľnosť (Non-repudiation)**
- Odosielateľ nemôže poprieť, že správu odoslal, a prijímateľ nemôže poprieť prijatie.
  - Praktické opatrenia: Digitálne podpisy (PKI), časové pečiatky.
- 6. **Minimalizácia expozície**
- Poskytovať von iba toľko informácií, koľko je nevyhnutné.
- Praktické opatrenia:
  - Segmentácia siete (DMZ, VLAN).
  - Odstránenie nepotrebných služieb a portov.
  - Používanie NAT a firewallov.
- 9. **Riadenie rizík a testovanie**
  - Pravidelné penetračné testy a bezpečnostné audity.
  - Patch management – rýchle aktualizovanie softvéru a zariadení.
  - Plány obnovy po incidente (Incident Response Plan).

# Základných princípy bezpečnej komunikácie

- 7. **Ochrana proti útokom a monitorovanie**
  - IDS/IPS – detekcia a prevencia prienikov.
  - Pravidelné logovanie a audit komunikácie.
  - Monitorovanie neobvyklého správania (SIEM, SOC).
- 8. **Bezpečné protokoly a štandardy**
  - Používať moderné bezpečné protokoly (HTTPS/TLS 1.3, SSH, SFTP).
  - Vyhýbať sa zastaraným technológiám (SSL 2.0/3.0, TLS 1.0, FTP, Telnet).
  - Certifikáty od dôveryhodných autorít.



Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE



# Podporné opatrenia

# Podporné opatrenia

- Školenie vývojárov a administrátorov v oblasti bezpečnosti.
- Pravidelné audity a dodržiavanie noriem (ISO/IEC 27001, ISO/IEC 20000..).
- Pravidelné audity a dodržiavanie rámcov (COBIT, IT4IT, NIST...)
- Dodržiavanie legislatívy (GDPR, zákon o kybernetickej bezpečnosti).

# Priestor na otázky

Financované Európskou úniou
NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI
ŽILINSKEJ UNIVERZITY V ŽILINE

# Ďakujem za pozornosť

Bezpečnosť pri nadobúdaní, vývoji a údržbe IS a siete, komunikačná bezpečnosť

Technické opatrenia (Blok IV)

**Kurz: Manažér kybernetickej bezpečnosti vo verejnej správe**


Milan Kubina

**KC KYB UNIZA, https://kc.uniza.sk/**

milan.kubina@fri.uniza.sk