FAKULTA ELEKTROTECHNIKY A INFORMATIKY

Computer CNL Networks Laboratory

Riziká KB

Bezpečnostný manažment

Miroslav Michalko

Laboratórium počítačových sietí

Riadenie hrozieb a rizík

- Čo chceme v spoločnosti chrániť?

AKTÍVUM

Aktívum – akýkoľvek finančne hodnotný komponent, ktorý sa podieľa na dodávke produktov, alebo služieb

Ide o hmotné alebo nehmotné ekonomické prostriedky, ktoré majú pre organizáciu súčasnú, alebo potenciálnu hodnotu.

Tu patria: procesy, dáta informácie, softvér, služby, objekty, priestory organizácie.

Ešte pár pojmov

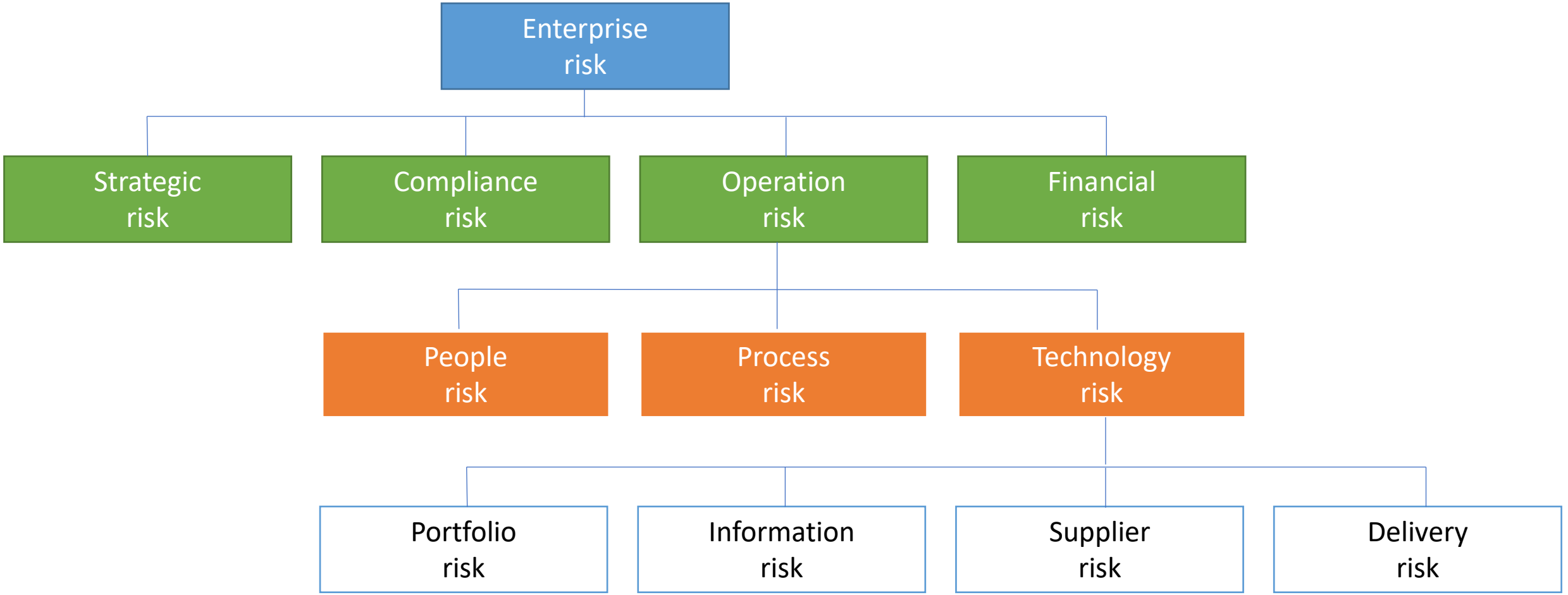
- **Zraniteľnosť** slabé miesto informačného aktíva, slabina v informačnom systéme, v bezpečnostných procedúrach systému, opatreniach alebo implementácii, ktoré následne môže aktivovať alebo využiť nositeľ hrozby.
- **Hrozba** je podľa § 3 písm. j) zákona č. 69/2018 Z z. o kybernetickej bezpečnosti každá primerane rozpoznateľná okolnosť alebo udalosť proti sieťam a informačným systémom, ktorá môže mať nepriaznivý vplyv na kybernetickú bezpečnosť. T.j. potenciál, že akákoľvek okolnosť či udalosť využije zraniteľnosť informačného aktíva a spôsobí škodu, alebo iný nepriaznivý následok.
- **Riziko** je funkcia pravdepodobnosti, že hrozba (potenciálna príčina nechceného) využije známu, alebo neznámu zraniteľnosť, pričom jej následkom nastane udalosť, typicky prinášajúca nežiadúci dopad na hodnoty.

zdroj: https://www.nbu.gov.sk/kyberneticka-bezpecnost/riadenie-rizik/index.html

Analýza a riadenie rizík

riešiť problémy až keď nastanú nie je vhodná stratégia

Podnikové riziká



zdroj: KKCB, KM-1

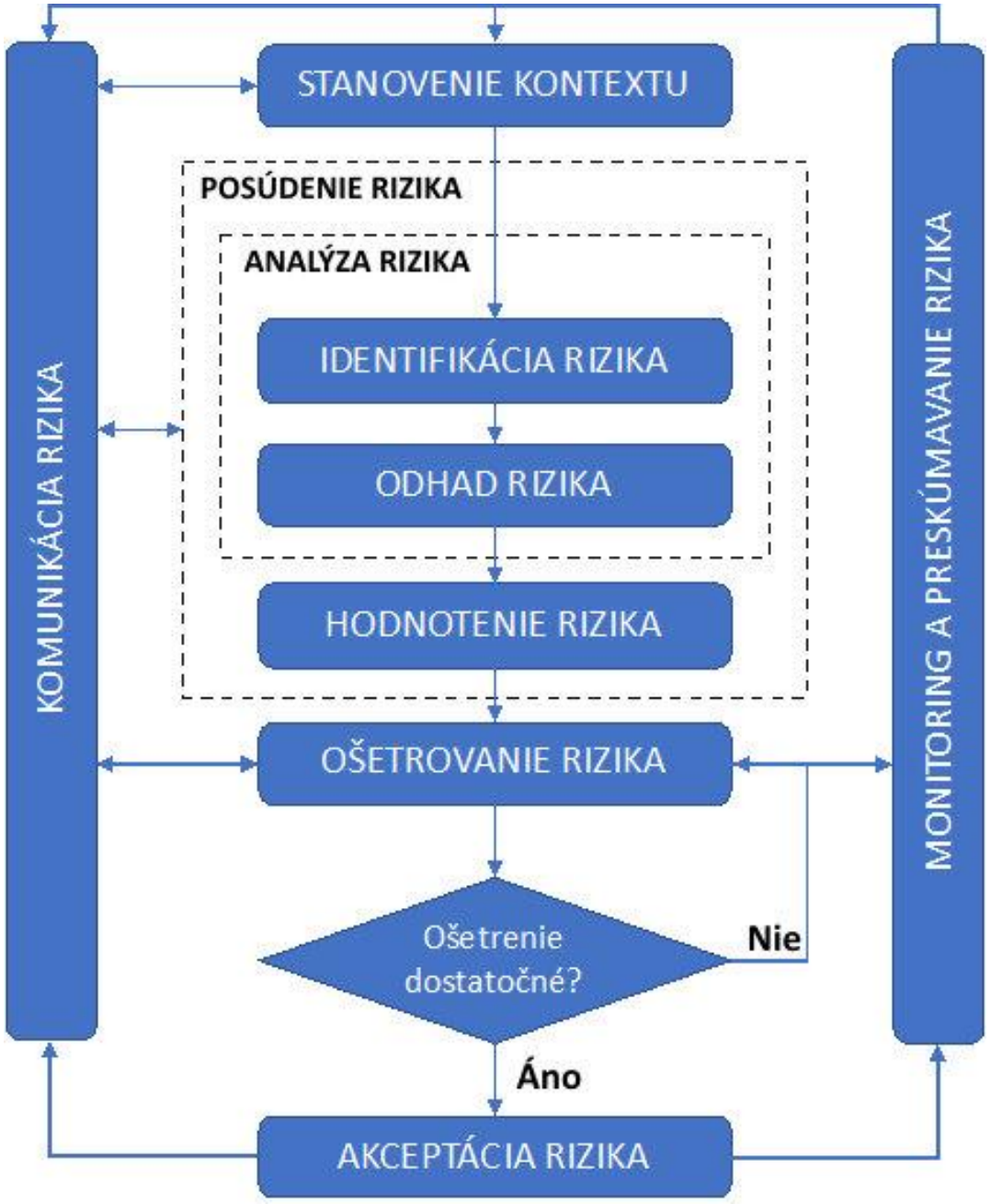
Riadenie rizík

Riadenie rizika možno vymedziť ako vopred nastavené a koordinované činnosti, ktorých cieľom je kontrolovať mieru rizika pôsobiaceho na organizáciu.

Pozostáva z dvoch fáz:

- analýza rizík,
- ošetrovanie rizík.

Vyhláška NBÚ č.362/2018 Z.z.



Analýza rizík

Analýza rizík je typicky založená na posúdení pravdepodobnosti výskytu hrozby a odhadu možného dopadu hrozby.

Analýzou rizík sa určuje pravdepodobnosť vzniku budúcej škodlivej udalosti, ktorá môže byť spôsobená zneužitím existujúcej zraniteľnosti aktíva potenciálnou hrozbou v spojitosti s existujúcimi bezpečnostnými opatreniami a identifikáciou dopadov pri narušení dôvernosti, integrity alebo dostupnosti aktíva.

Výsledok analýzy rizík sa opiera o základný vzorec, podľa ktorého je riziko súčinom pravdepodobnosti hrozby a jej potenciálneho dopadu podľa vzorca:

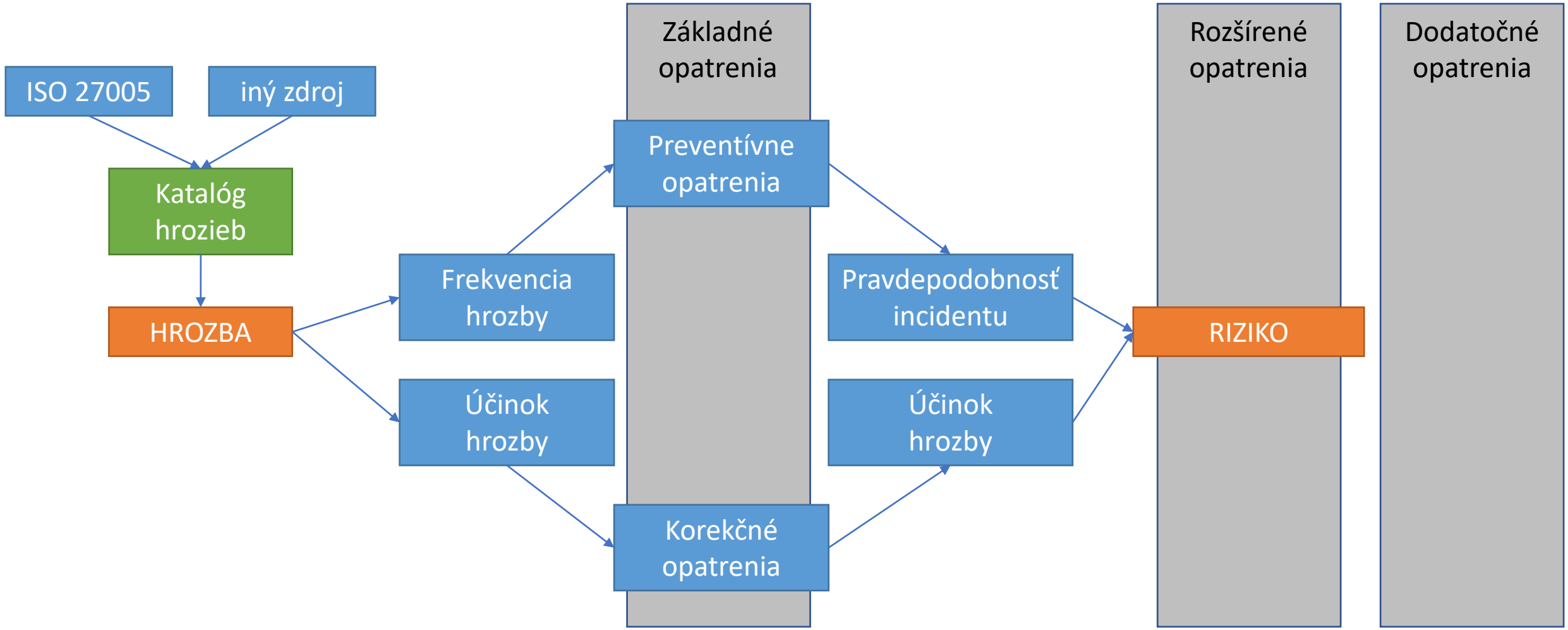
$$Rn = Pn \times Dn.$$

Úroveň závažnosti	Slovný opis závažnosti
Mimoriadne vysoké	riziko bezprostredne ohrozuje poskytovanie základnej služby, bezpečnosť organizácie, resp. kritického procesu, alebo systému (typicky prekročenie stanoveného limitu tolerancie rizika, katastrofálna finančná strata alebo škoda na majetku, dopady na zdravie a život, dopad na životné prostredie, atď.)
Vysoké	riziko potenciálne ohrozuje poskytovanie základnej služby, bezpečnosť organizácie resp. kritického procesu, alebo systému
Nízke	riziko neohrozuje poskytovanie základnej služby, ohrozuje výkon niektorých podporných procesov, kritické procesy, alebo systémy však nie sú rizikom ohrozené
Zanedbateľné	riziko neohrozuje poskytovanie základnej služby, výkon procesov a prevádzka systémov nie sú rizikom ohrozené

Riziko = **Pravdepodobnosť** x **Dopad**

- kvalitatívne metódy (slovné vyjadrenie)
- kvantitatívne metódy (číselné vyjadrenie)
- semikvantitatívne metódy (kombinácia, stupnice)

Postup pri analýze rizík



zdroj: KKCB, KM-1

Katalóg hrozieb

ISO/IEC 27005 - typické príklady

A – náhodné konanie (Accidental)

B – úmyselné konanie (Deliberate)

E – vyššia moc (Environmental)

Typ	Hrozby	Pôvod
Fyzické	Požiar	A,D,E
	Poškodenie vodou	A,D,E
	Znečistenie	A,D,E
	Prach, korózia, mrznutie	A,D,E
Prírodné udalosti	Povodeň	E
	Klimatický jav	E
	Sopečný jav	E
Strata základných služieb	Prerušenie dodávky elektriny	A,D,E
Poruchy spôsobené žiarením	Elektromagnetické žiarenie	A,D,E
	Termálne žiarenie	A,D,E
Ohrozenie informácií	Krádež médií, dokumentov	D
	Krádež zariadení	D
	Vzdialená špionáž	D
	Odpočúvanie	D
Technické zlyhanie	Chybné fungovanie zariadenia	A
	Preťaženie systému	A,D
	Chyba údržby	A,D
Neoprávnené činnosti	Poškodenie dát	D
	Nezákonné spracovanie dát	D
Ohrozenie funkčnosti	Chyba v používaní	A
	Zneužitie oprávnenia	A,D
	Nedostatok personálu	A,D,E

zdroj: https://isocertifikat.sk/iso-27001-identifikacia-hrozieb-a-zranitelnosti/

Pravdepodobnosť výskytu hrozieb

Typické príklady hrozieb a príklady ich súvisiacich zraniteľností.

Pravdepodobnosť:

1 – najmenej pravdepodobná

5 – najviac pravdepodobná

Rozpoznaná hrozba	Pravdepodobnosť hrozby	Príklad súvisiacich zraniteľností
Zlyhanie hardvéru	3	Náchylnosť zariadenia na vlhkosť, prach a ušpinenie
Zlyhanie softvéru	3	Nejasné alebo neúplné špecifikácie pre vývojárov
Krádež	2	Nedostatok fyzickej ochrany budov, dverí a okien
Povodeň	1	Umiestnenia v miestach ktoré sú ohrozované povodňami
Zlomyseľné kódy	5	Nedostatok aktualizácií softvéru na ochranu pred zlomyseľnými kódmi
Neúmyselná modifikácia	5	Nedostatočný výcvik bezpečnosti
Zlyhanie komunikačných služieb	4	Nechránené verejné sieťové pripojenia

zdroj: https://isocertifikat.sk/iso-27001-identifikacia-hrozieb-a-zranitelnosti/

Pravdepodobnosť hrozby	Dopad				
	Zanedbateľný (20)	Malý (40)	Stredný (60)	Značný (80)	Katastrofický (100)
Vysoká (1)	20*1,0=20	40*1,0=40	60*1,0=60	80*1,0=80	100*1,0=100
Stredná (0,7)	20*0,7=14	40*0,7=28	60*0,7=42	80*0,7=56	100*0,7=70
Malá (0,4)	20*0,4=8	40*0,4=16	60*0,4=24	80*0,4=32	100*0,4=40
Veľmi malá (0,2)	20*0,2=4	40*0,2=8	60*0,2=12	80*0,2=16	100*0,2=20

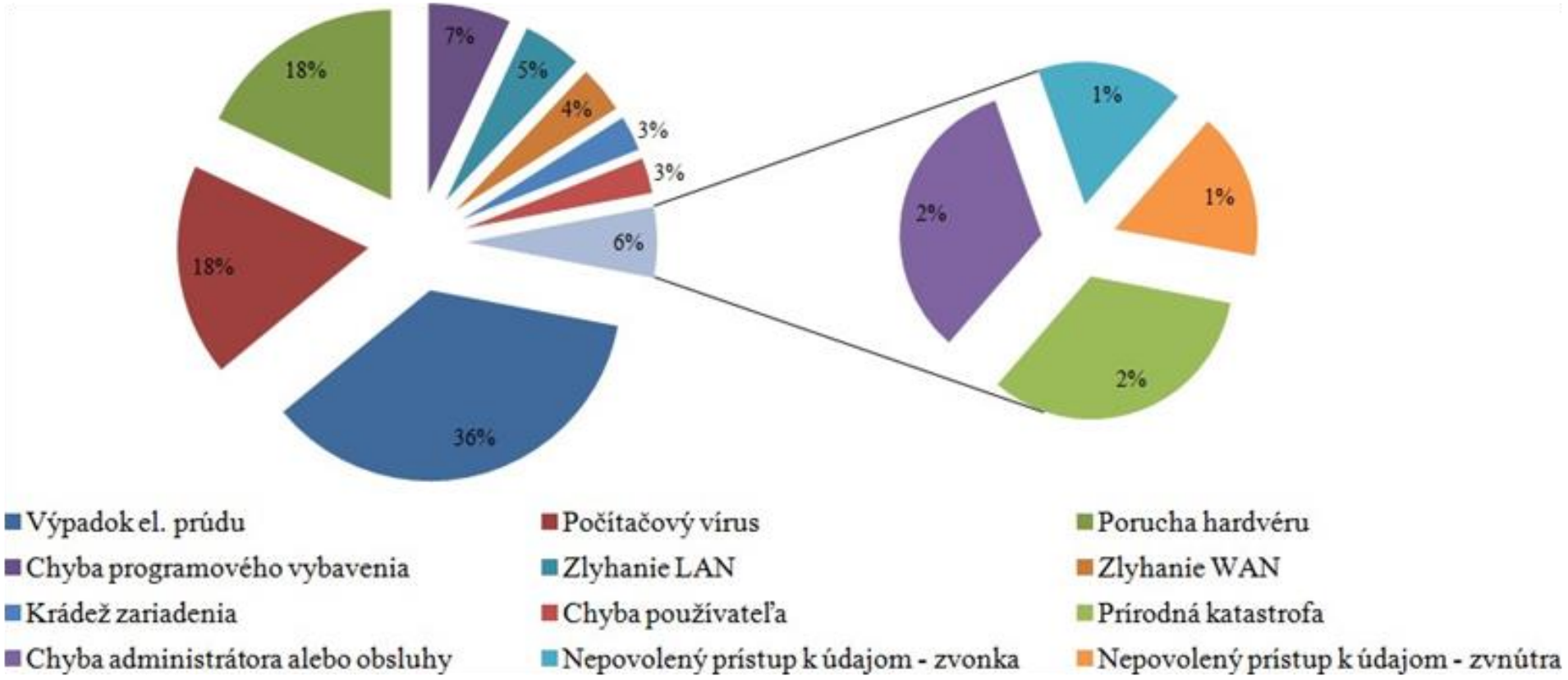
zdroj: KKCB, KM-1

URČENIE HODNOTY DOPADU RIZIKA

Hod-nota	Opis dopadu	Finančný dopad (príklad)	Prevádzkový dopad	Legislatívny dopad	Strata dôvery
1	Riziko nemá dopad	0	Žiaden prevádzkový dopad	Regulácie a nariadenia neporušené	Žiaden reputačný dopad
20	Zanedbateľný vplyv, strata	1 – 15 000 €	Interne, oddelenie	Zlyhanie interného procesu	Určité prekážky v komunikácii v rámci spoločnosti
40	Malý vplyv, strata	15 001 – 150 000 €	Interne, viacero oddelení v rámci divízie	Začatie správneho konania smerujúce k opatreniu na nápravu	Závažné prekážky v komunikácii v rámci spoločnosti
60	Stredný vplyv, strata	150 001 – 1 500 000 €	Firma, malá časť klientov	Začatie správneho konania smerujúce k uloženiu pokuty	Určitá nepriaznivá publicita na národnej úrovni
80	Značný vplyv, strata	1 500 001 – 15 000 000 €	Spoločnosť, značná časť klientov	Pozastavenie / ukončenie činnosti časti služieb	Intenzívna nepriaznivá publicita na národnej úrovni
100	Katastrofický vplyv, strata	Viac ako 15 000 000 €	Spoločnosť, všetci klienti	Pozastavenie / ukončenie činnosti – kľúčové služby	Nepriaznivá medzinárodná publicita

zdroj: KKCB, KM-1

Analýza najčastejších hrozieb



zdroj: https://isocertifikat.sk/iso-27001-identifikacia-hrozieb-a-zranitelnosti/

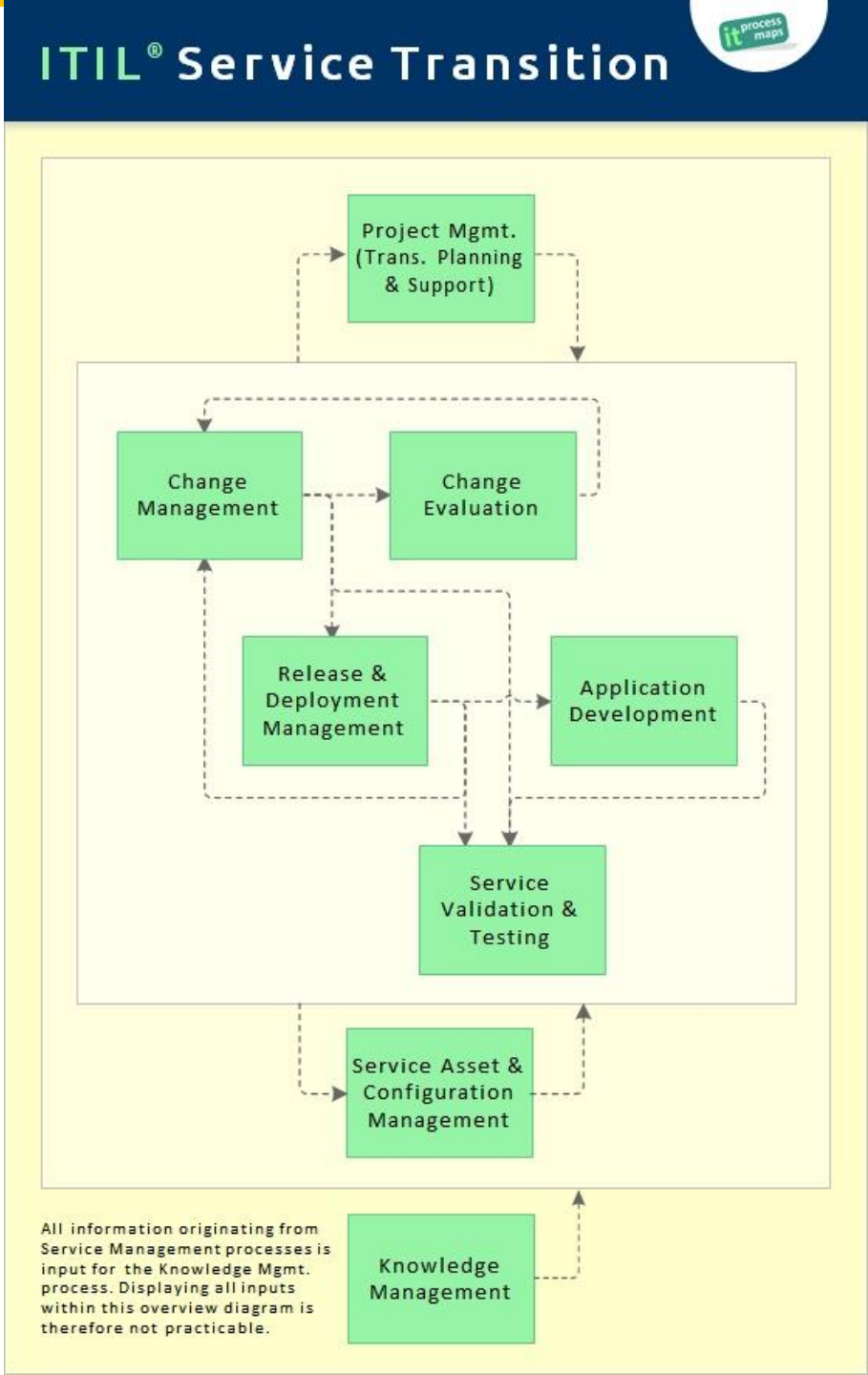
Prechod na nové služby

Prechod na nové služby

Prechod služby (angl. Service Transition) – cieľom je vybudovať a nasadiť IT služby. Fáza životného cyklu prechodu služby tiež zabezpečuje, že zmeny služieb a procesov riadenia služieb sa vykonávajú koordinovaným spôsobom.

Plánovanie a podpora prechodu (angl. Transition Planning and Support) sa zameriava na plánovanie a koordináciu zdrojov na nasadenie hlavnej verzie v rámci predpokladaných nákladov, času a odhadov kvality.

Riadenie zmien (angl. Change management) - je systematický prístup, ktorý zahŕňa riešenie zmien alebo transformácie organizačných cieľov, základných hodnôt, procesov alebo technológií. Cieľom je minimalizovať dopad incidentov.



https://wiki.en.it-processmaps.com/index.php/ITIL_Service_Transition

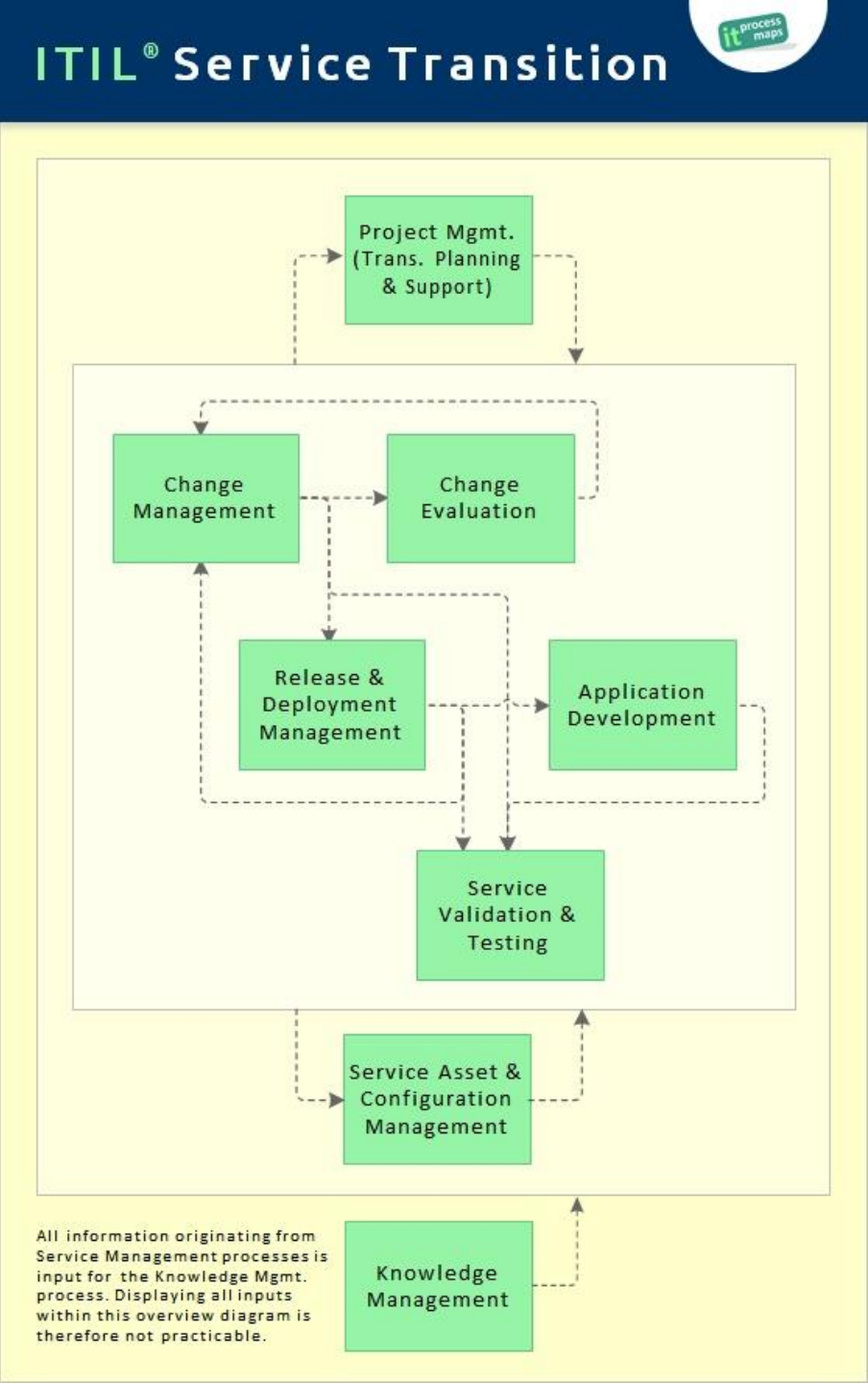
Manažment vydaní a nasadení

Manažment vydaní a nasadení - cieľom je nastaviť proces plánovania a riadenia zmien služieb do produkcie a tak vytvoriť efektívne využívanie nových a zmenených služieb.

(angl. Release and Deployment Management)

Prínosy:

- stabilné prostredie (testovacie, produkčné),
- minimalizácia chybovosti,
- vyššia dostupnosť prevádzkovaných služieb,
- predikovateľné prostredie a vyššia efektívnosť využívania IT zdrojov.



FAKULTA ELEKTROTECHNIKY A INFORMATIKY

Computer CNL Networks Laboratory

Manažment aplikácií

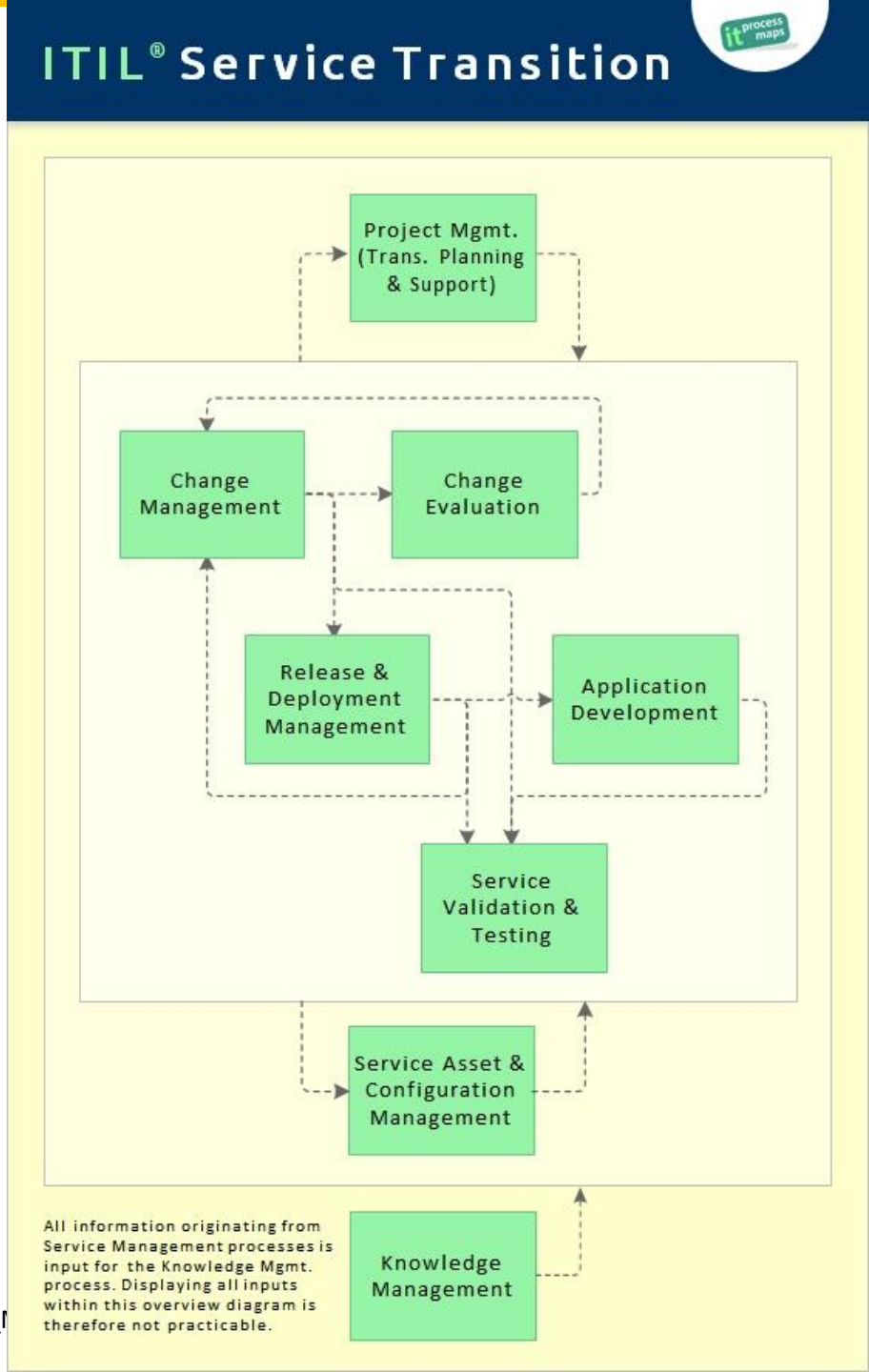
Manažment aplikácií je zodpovedný za správu aplikácií počas ich životného cyklu. Tento proces ITIL hrá dôležitú úlohu v aplikačných aspektoch navrhovania, testovania, prevádzky a zlepšovania IT služieb, ako aj pri rozvíjaní zručností potrebných na prevádzku aplikácií IT organizácie.

(angl. Application Management)

Vývoj aplikácií – cieľom je sprístupniť aplikácie a systémy, ktoré poskytujú požadovanú funkčnosť pre IT služby. Zahŕňa to ich vývoj a integráciu do požadovaného prostredia.

(angl. Application Development)

Manažment aplikácií je nepretržitá činnosť, na rozdiel od vývoja aplikácií, čo je zvyčajne jednorazový súbor činností na vytváranie aplikácií.



zdroj: https://wiki.en.it-processmaps.com/index.php/ITIL_Application_M

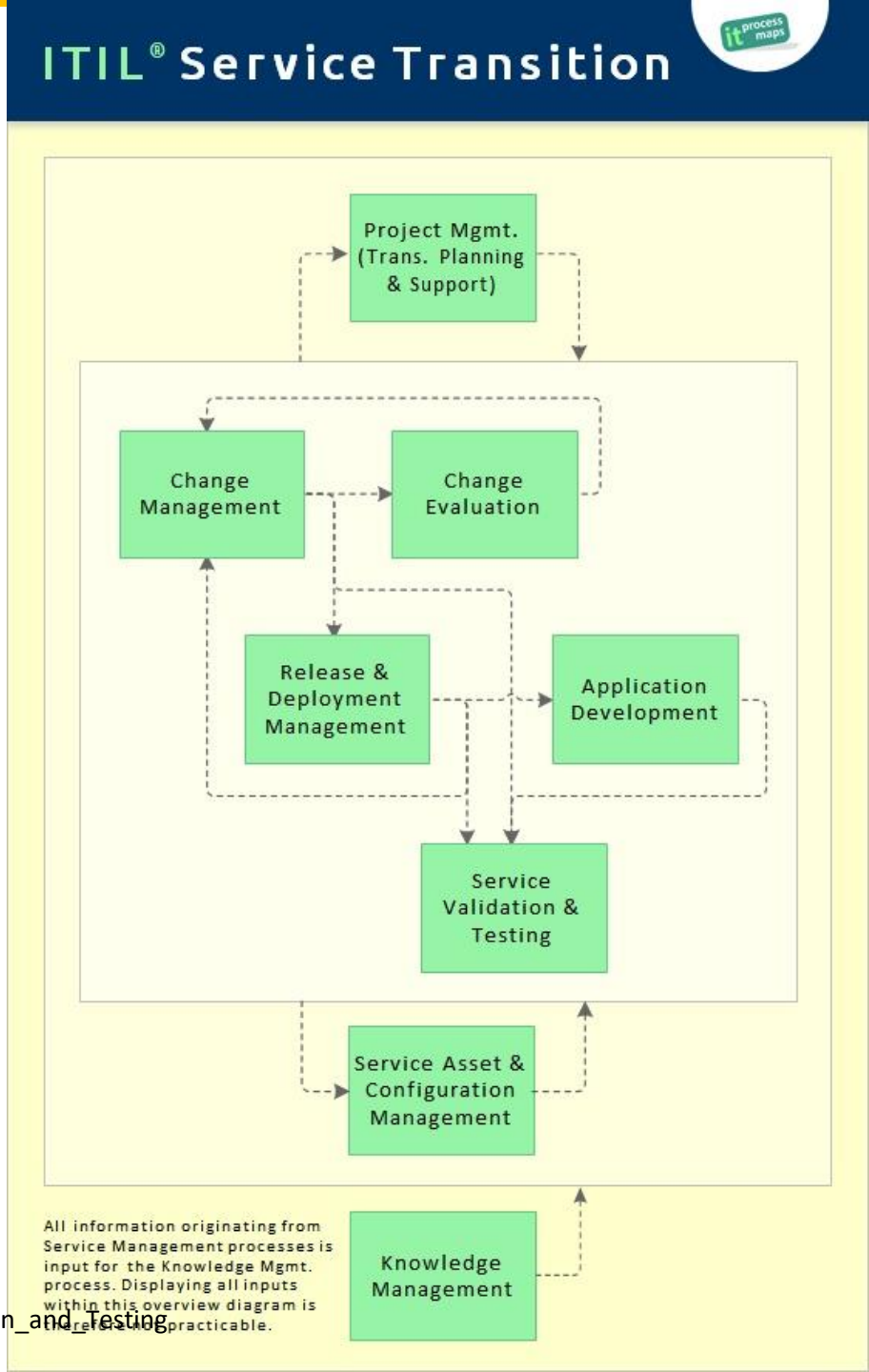
Validácia a testovanie služieb

Cieľom overovania a testovania služieb je zabezpečiť, aby nasadené vydania a výsledné služby spĺňali očakávania zákazníkov. V tejto fáze sa overuje, že IT riešenia a pripravené operácie sú schopné podporovať novú službu.

(angl. Service Validation and Testing)

Prínosy:

- garantovať, že zmeny prinášajú korektnú požadovanú službu a očakávané výstupy,
- overiť, že požiadavky a kritériá zákazníka sú korektne a úplne implementované (overenie aj komplexnosti zákazníckej definície požiadaviek).



zdroj: https://wiki.en.it-processmaps.com/index.php/Service_Validation_and_Testing

Riadenie konfigurácií IT služieb

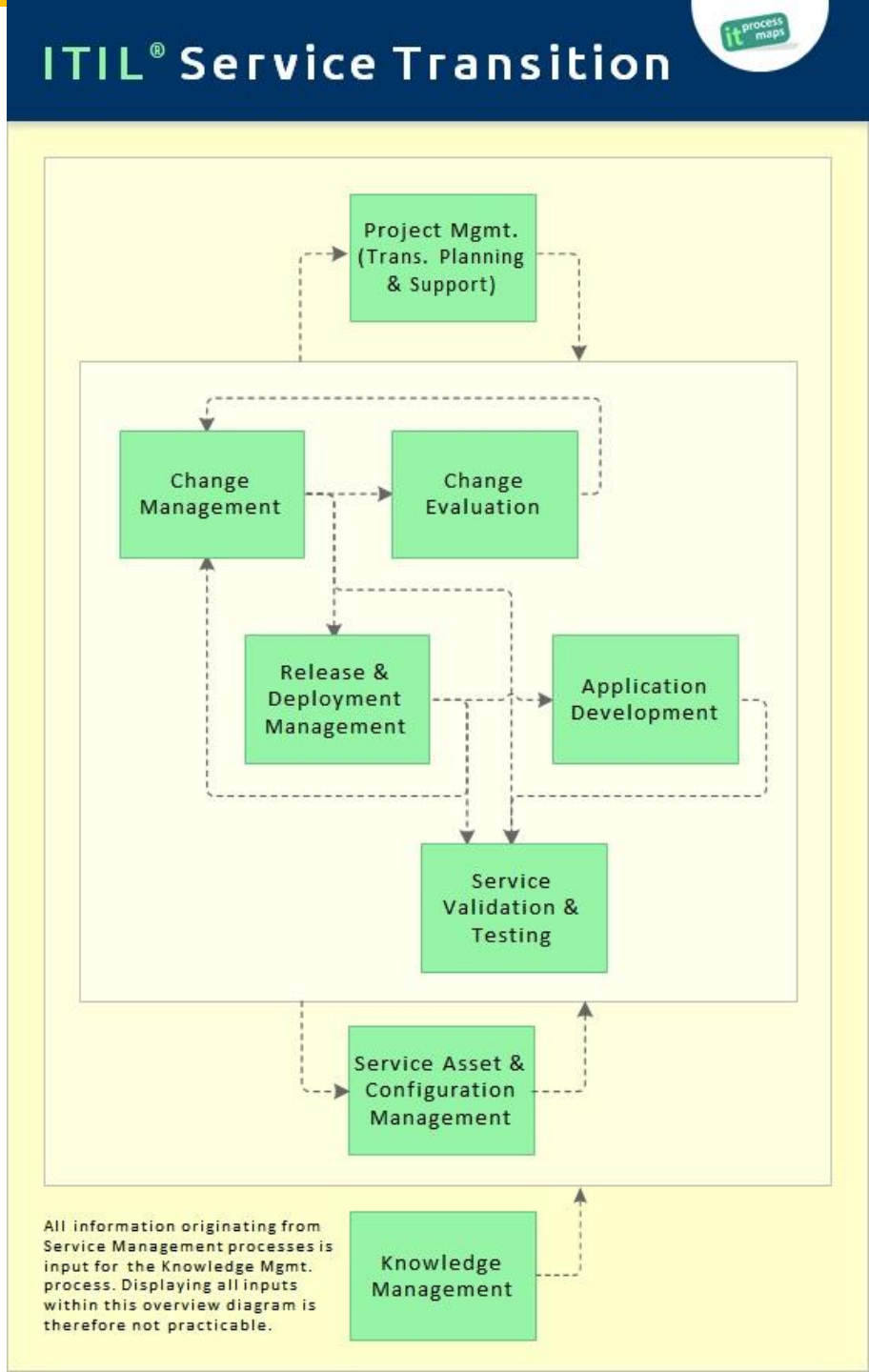
Cieľom procesov zameraných na **riadenie konfigurácií IT služieb** je zabezpečiť, že sú stále dostupné aktuálne konfiguračné nastavenia a všetky relevantné konfiguračné položky (angl. Configuration Items) z ktorých je služba zložená.

(angl. Service Asset and Configuration Management)

Prínosy:

- existencia informácií o CI a väzbách medzi nimi,
- verifikácia splnenia zákonných požiadaviek,
- zvýšenie bezpečnosti a rýchla reakcia pri incidentoch,
- eliminácia neautorizovaných CI (napr. nedovolený softvér).

Riadenie IT aktív je zamerané primárne na ekonomické dopady/prevádzku. V porovnaní s tým je riadenie IT konfigurácií zamerané na konfiguráciu komponentov služby.

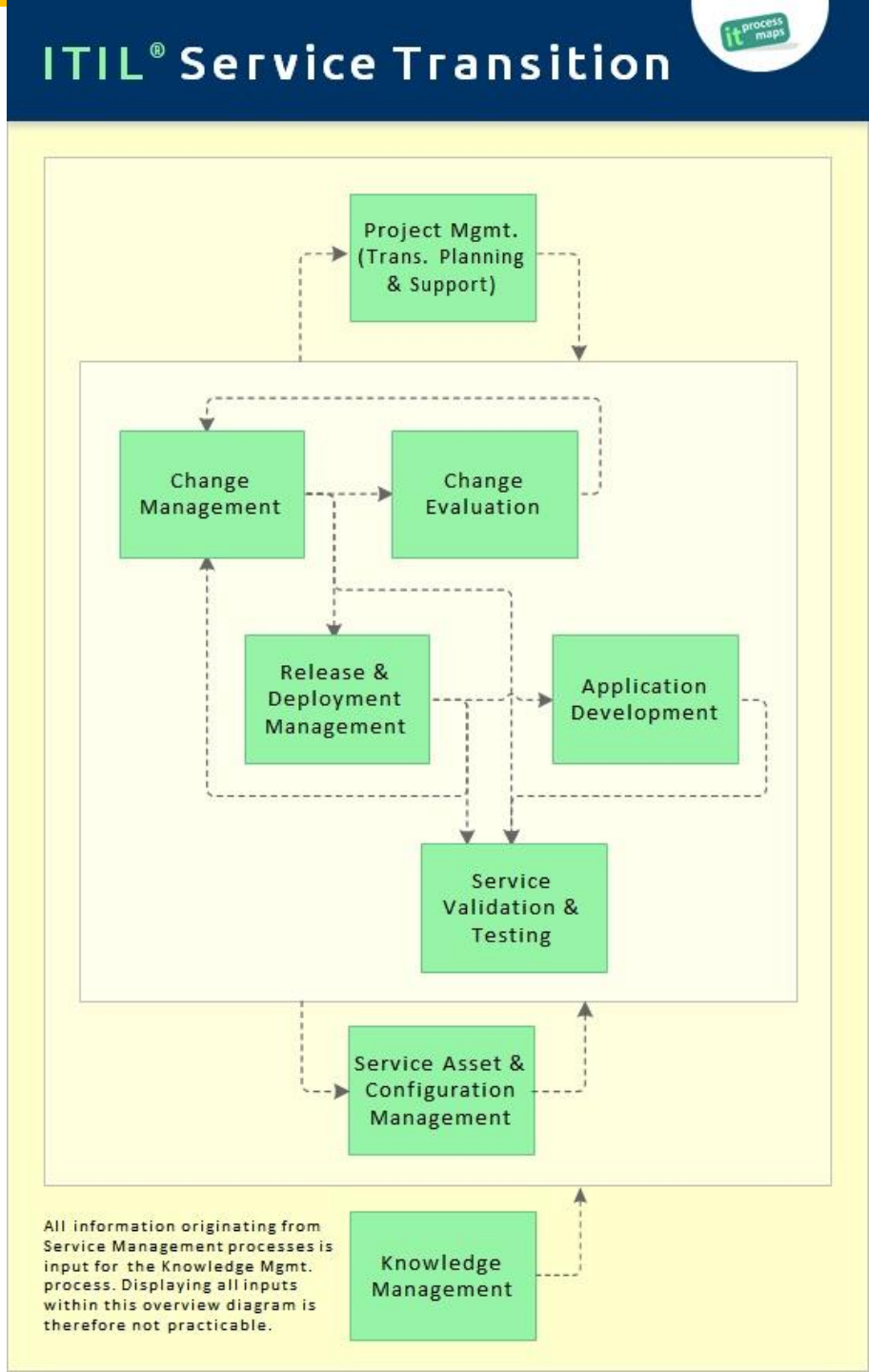


Manažment znalostí

Manažment znalosti má za cieľ zhromažďovať, analyzovať, uchovávať a zdieľať znalosti a informácie v rámci organizácie.

(angl. Knowledge Management)

Primárnym účelom tohto procesu je zlepšiť efektivitu znížením potreby znovu objavovania vedomostí. Zároveň je možné identifikovať osobu, ktorá vie v správnom čase poskytnúť podporu.



Procesy prevádzky služieb

Prevádzka služieb si vyžaduje ich prevádzku, podporu, údržbu – s cieľom zabezpečiť stabilitu a bezchybový stav.

Prevádzka je riešená prostredníctvom:

- manažment udalostí (Event Management) – indikuje stav monitorovaného objektu – rutinne, alebo sa vyžaduje zásah, reakcia môže byť manuálna alebo automatická,
- manažment incidentov (Incident Management) – pri narušení IT služby, alebo pri znížení jej kvality sa vyžaduje zásah s cieľom minimalizácie nepriaznivých vplyvov,
- spracovanie požiadaviek (Request Fulfillment) – prijíma a rieši požiadavky používateľov zabezpečujúcich prevádzkovanú službu,
- manažment problémov (Problem Management) – výsledok jedného alebo viacerých incidentov, ktorým sa nepredišlo – zahŕňa diagnostiku, elimináciu incidentu, elimináciu opakovania sa incidentov.
- manažment prístupov (Access Management) – rieši indetitu jednotlivca a jeho práva s cieľom dodržať CIA, automatizovaná správa používateľov pri zmene/rušení rolí.

Ďakujem za pozornosť

miroslav.michalko@cnl.sk

Laboratórium počítačových sietí

Katedra počítačov a informatiky, FEI TUKE