



Informačné systémy
Bezpečnosť
Infraštruktúra



Nové trendy v analýze rizík

RNDr. Michal Danilák

ISACA Open Day , 18.5.2011

Zohľadnenie globálnych rizík a ich dopadov

Analýza globálnych rizík:

Global risks 2011, sixth edition,
Initiative of the Risk Response Network
World Economic Forum, January 2011

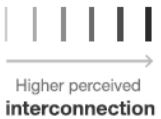
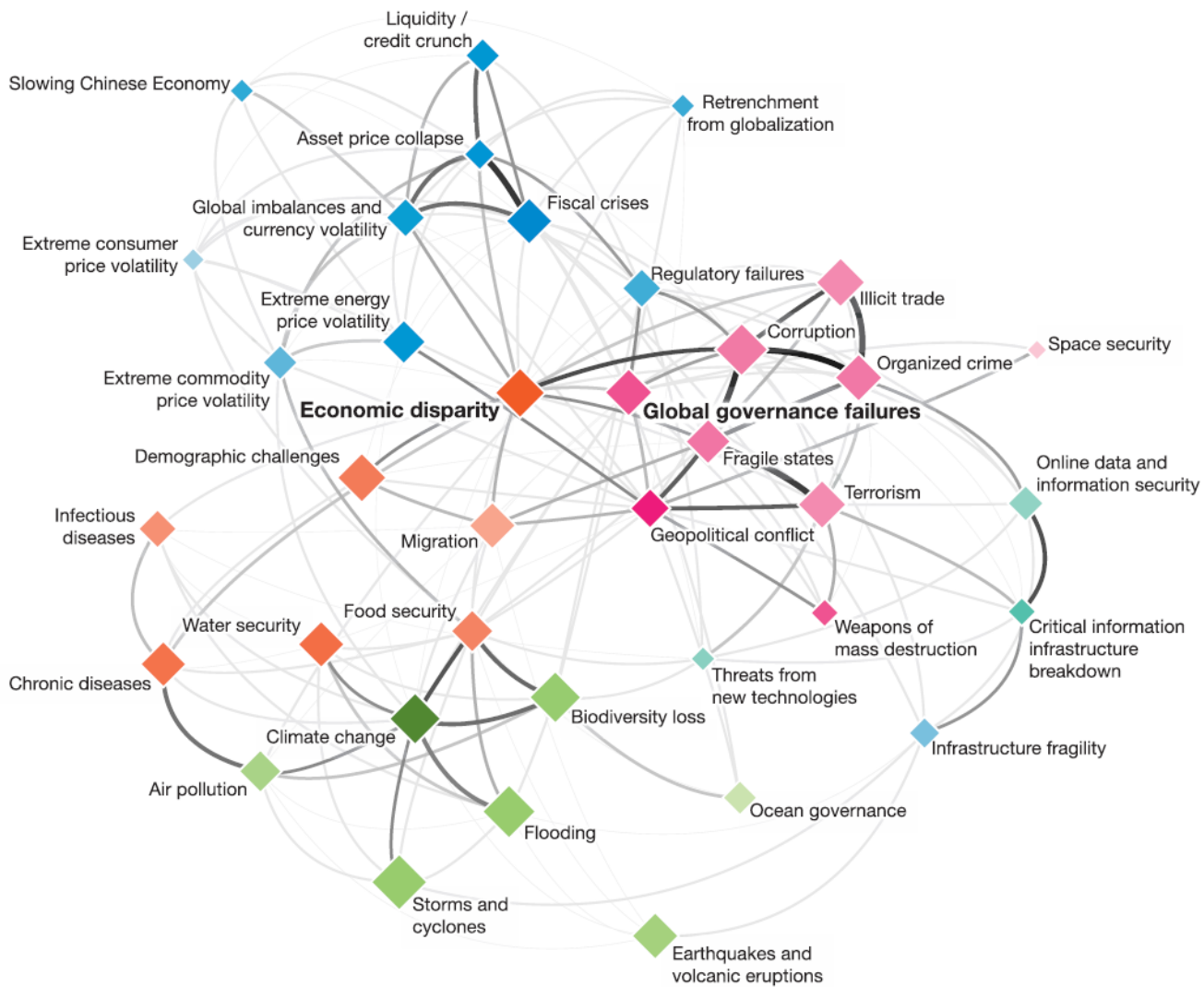
www.weforum.org/reports

Oblasti rizík

- Ekonomické (11)
- Environmentálne (7)
- Sociálne (7)
- Geopolitické (9)
- Technické (3)

Mapa prepojenia rizík: nasledujúci obr.

Figure 2 | Risks Interconnection Map (RIM) 2011



Economic Risks

Geopolitical Risks

Environmental Risks

Societal Risks

Technological Risks

Ekonomické riziká

- Kolaps hodnoty aktív
- Mimoriadna nestabilita cien komodít
- Mimoriadna nestabilita spotrebiteľských cien
- Mimoriadna nestabilita cien energií
- Fiškálne krízy
- Globálne nerovnováhy a nestabilita mien
- Krehkosť, zraniteľnosť infraštruktúry
- Narušená likvidita/kreditu
- Zlyhania kontroly
- Negatívne dopady globalizácie
- Spomalenie čínskej ekonomiky (<6% rast)

Environmentálne riziká

- Znečistenie ovzdušia
- Strata biodiverzity
- Klimatická zmena
- Zemetrasenia a sopečné erupcie
- Záplavy
- Kontrola nad oceánmi
- Búrky a cyklóny

Geopolitické riziká

- Korupcia
- Krehké, nestabilné štáty
- Geopolitický konflikt
- Zlyhania globálneho riadenia
- Nezákonný obchod
- Organizovaný zločin
- Bezpečnosť priestoru
- Terorizmus
- Zbrane hromadného ničenia

Sociálne a technologické riziká

Sociálne riziká:

- Chronické choroby
- Demografické výzvy
- Ekonomická disparita
- Potravinová bezpečnosť
- Infekčné choroby
- Migrácia
- Bezpečnosť vodných zdrojov

Technologické riziká:

- Narušenie kritickej informačnej infraštruktúry
- Informačná bezpečnosť
- Hrozby z nových technológií

Úrovne dopadov

- **Celosvetovo** dané (napr. rastúce ceny potravín, ropy, klimatická zmena, Internet ako celosvetová entita)
- Dané špecifikami **EÚ** (napr. fiškálne krízy PIIGS, pozícia eura, európska legislatíva)
- Špecifické pre **Slovensko** (napr. iná miera sociálnych rizík, ekonomickej štruktúry, špecifický geopolitický priestor, úroveň bezpečnosti)
- Špecifické pre **organizáciu** (napr. zmena rozpočtu v dôsledku fiškálnej krízy, zvýšené náklady na energie)
- Špecifické pre **IKT organizácie** (napr. následné krátenie rozpočtu na IT a teda aj bezpečnosť)

Poučenia (lessons learned)

- Rastie vzájomná prepojenosť rizík a klasické prístupy k manažmentu rizík nepostačujú (napr. pre udalosti typu Black Swan).
- Vznikajú rýchle reťazové a domino efekty (napr. pádom Lehman Brothers, nepokoje v Tunisku).
- Následné dopady - napr. dopady fiškálnej krízy iniciujú množstvo ďalších hrozieb a ich dopadov aj pre inštitúcie, firmy.
- Neschopnosť predikcie dopadov rizík (napr. dlh Grécka – Írsko - euroval – Portugalsko - kríza eura – čo SK?).
- Neschopnosť alebo neochota rozpoznať začiatky realizácie hrozieb (MMF, SB, G20, EÚ, iné).
- Nutná je medzinárodná spolupráca.

Udalosti typu Black Swan (Čierna labuť)

- Veľká výzva pre manažment rizík.
- Atribúty:
 - Udalosť je ťažko predikovateľná.
 - Dopady v prípade nastania udalosti sú veľké, s ešte väčšími následnými dopadmi.
 - Následné dopady sú neočakávané.
 - Udalosť je s malou historickou skúsenosťou, ale po realizácii je spätne jasne pochopiteľná.
- Príklady: Pád Lehman Brothers, grécka fiškálna kríza, revolúcia v Tunisku, zemetrasenie v Japonsku.

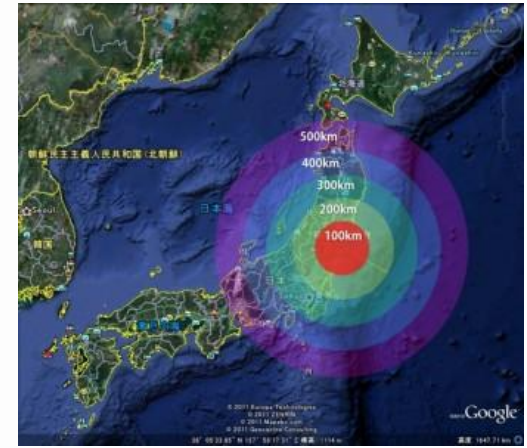


Zemetrasenie v Japonsku

Reťazenie dopadov (príklady):

- Cunami.
- Poškodenie jadrovej elektrárne Fukušima.
- Stop jadrovej energetike v Nemecku.
- Zvýšený dopyt po rope.
- Budúci nárast cien energie.

- Výpadky japonských subdodávateľov.
- Oslabenie pozície Japonska na svetovom trhu (napr. Toyota).
- Zvýšenie dopadov fiškálnej krízy v Japonsku.
- Psychologický zlom vnímania Japonska ako lídra.
- Priame straty: vyše 300 mld. USD.



Výzvy

- **Potreba nových prístupov v manažmente rizík**
 - ✓ Proaktívne riešenie príčin, nie symptómov
 - ✓ Identifikácia bodov efektívnej intervencie v daných štruktúrach a systémoch
 - ✓ Zohľadniť fakt, že stále silnejšou závislosťou medzi rizikami vzniká stále viac nezamýšľaných a netušených dopadov
 - ✓ Pracovať aj s hrozbami, ktoré sa prejavia v časovej škále desiatok rokov a dlhšie (napr. sociálne)
 - ✓ **Všetky organizácie, firmy musia zohľadňovať globálne riziká**

- **Silná medzinárodná spolupráca**
 - ✓ Nové medzinárodné a národné orgány pre koordináciu
 - ✓ napr. Rada pre finančnú stabilitu
 - ✓ The World Economic Forum's **Risk Response Network**

IT a globálne riziká

Nástroj v znižovaní globálnych rizík (napr. eHealth šetrí zdroje v zdravotníctve, rast konkurencieschopnosti...)

Zdroj nových hrozieb (riziká kyber sveta)

- IT je súčasťou kritickej infraštruktúry so svojimi hrozbami (IT aj non-IT)
- IT nástroje umožňujú vznik nových hrozieb (napr. automatizované on-line obchody na burzách)
- IT nástroje sú nástrojmi kyber zločinu (cyber crime)
- IT menia správanie sa ľudí
 - sociálne siete
 - informačná preťaženosť mozgov
 - Virtuálne svety

Zložité väzby medzi rizikami

Príklad: Fiškálna kríza a kyber riziká

- menej zdrojov verejnú správu, bezpečnosť a teda aj na IT a následne IT SEC
- únik kvalifikovaných IT / SEC ľudí z verejnej správy
- prepúšťanie zamestnancov, väčšia frustrácia - úniky dát
- nedostatok zdrojov aj cyber crime svete – hľadanie nových foriem príjmov
- spoločenská frustrácia:
 - ❖ menšia úcta k zákonu, autoritám
 - ❖ čas Wiki leaks, Pirate leaks , ...
 - ❖ zefektívňovanie procesov v čase fiškálnej krízy vedie k vyššej informatizácii – vznikajú nové IT SEC riziká (napr. v eHelth)
- IT je súčasťou kritickej infraštruktúry so svojimi hrozbami

Procesne orientované analýzy rizík

Príklad:

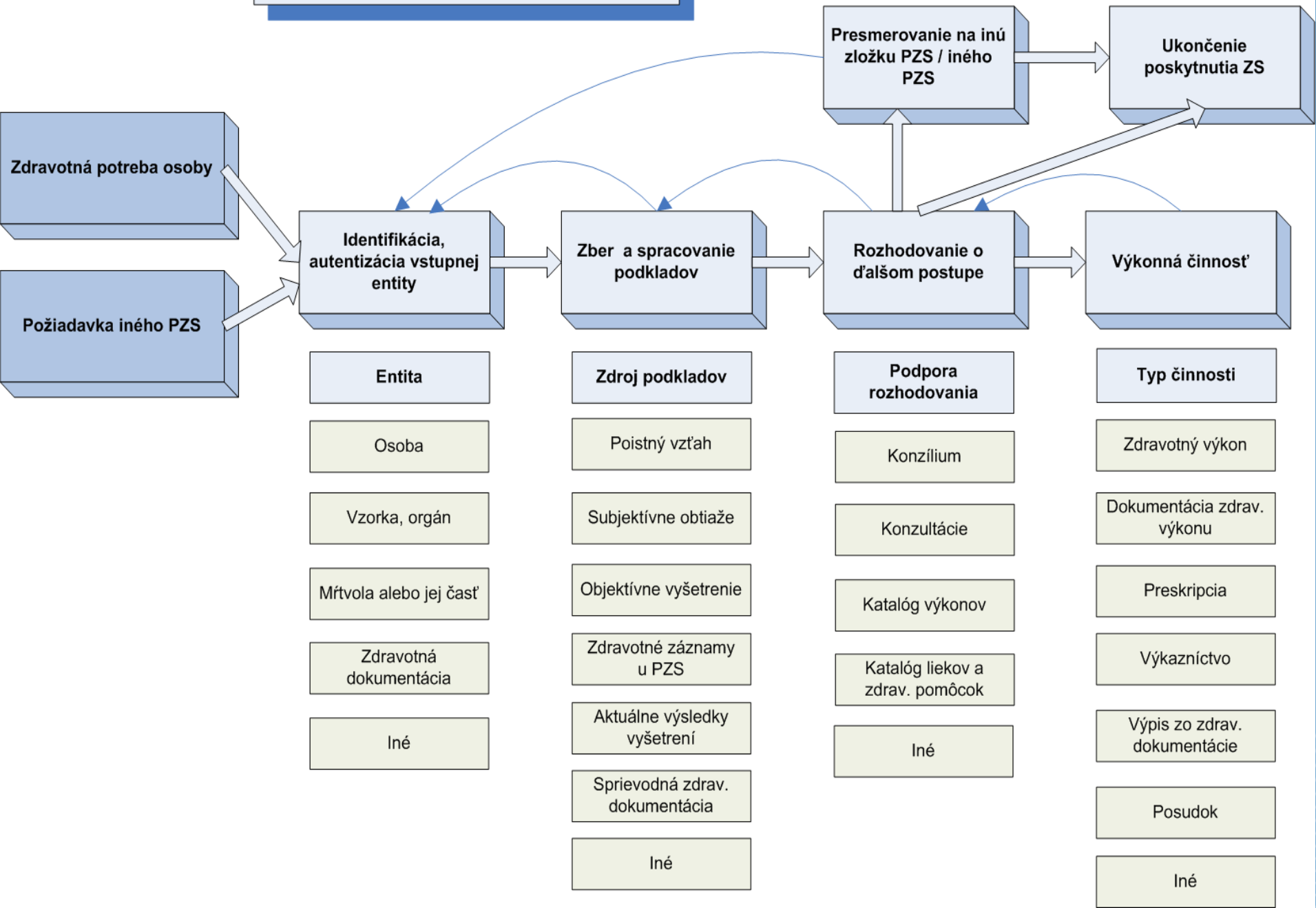
Procesy poskytovania zdravotnej starostlivosti

Oblasti rizík, ktoré je potrebné identifikovať:

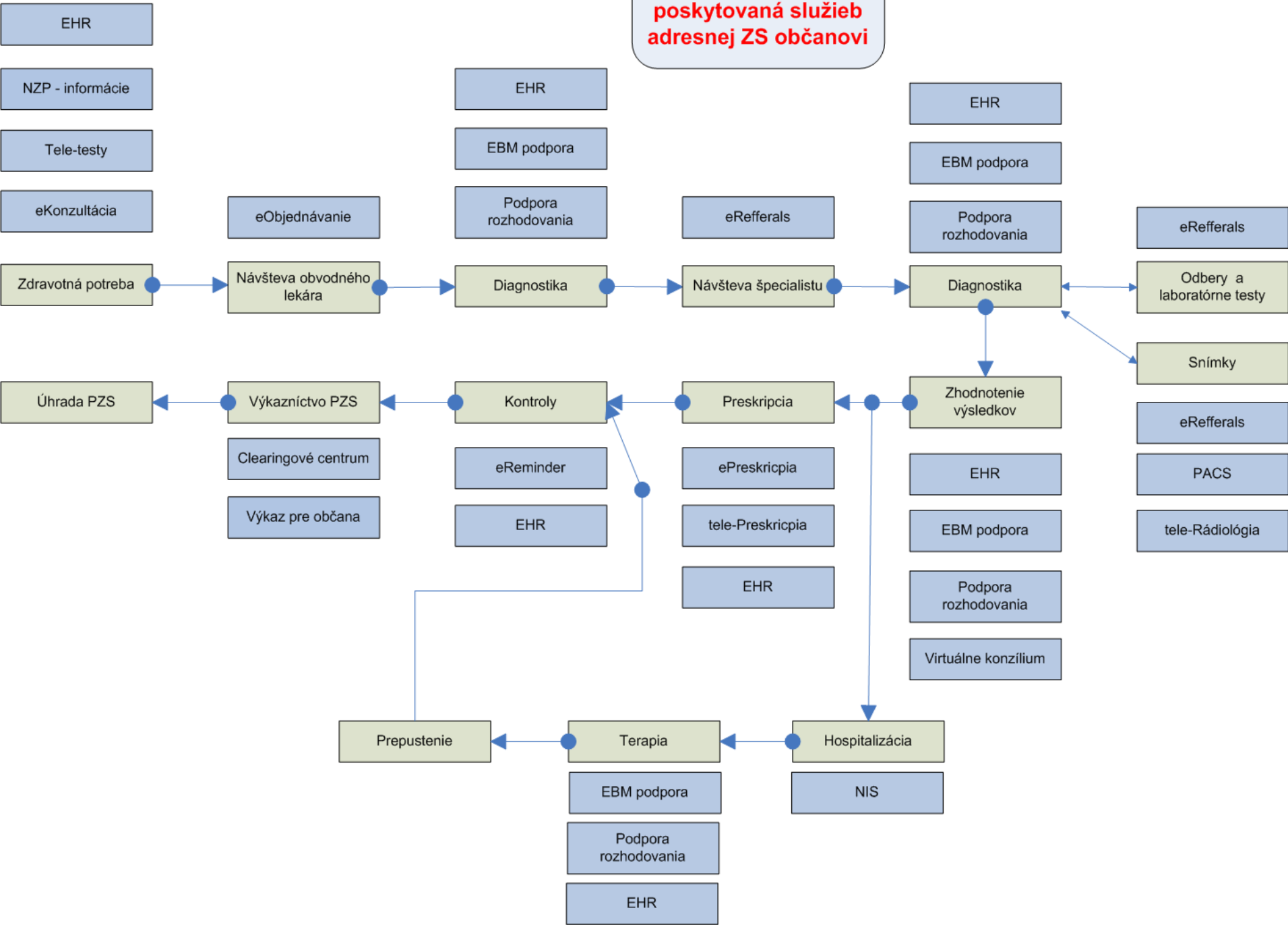
- Zdravotné (klinické),
- Finančné,
- IT,
- Procesné, ...

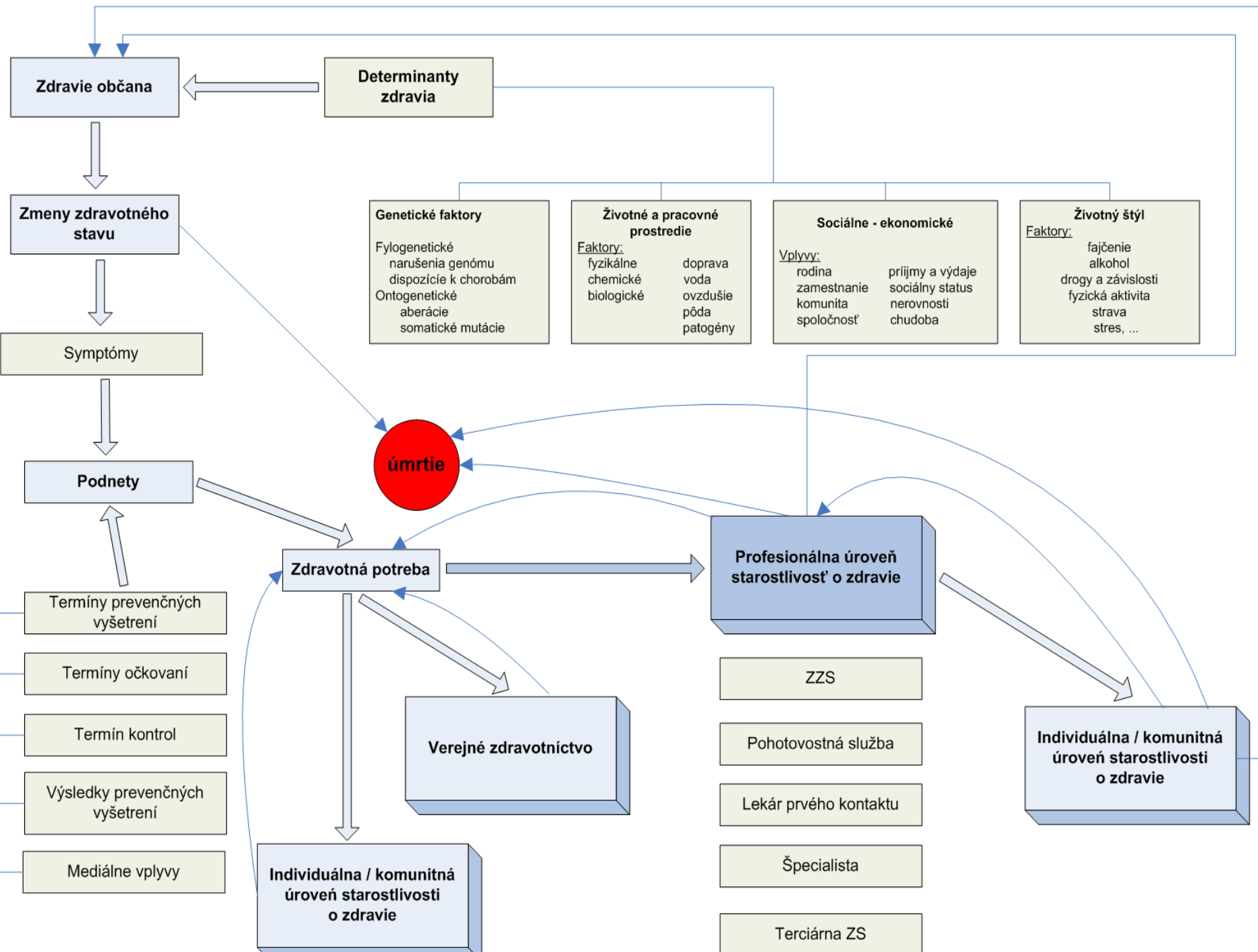
viď nasledujúce obr. procesov

Štandardné poskytovanie ZS (aktuálny stav – as is)



Podpora eHealth pri poskytovaní služieb adresnej ZS občanovi





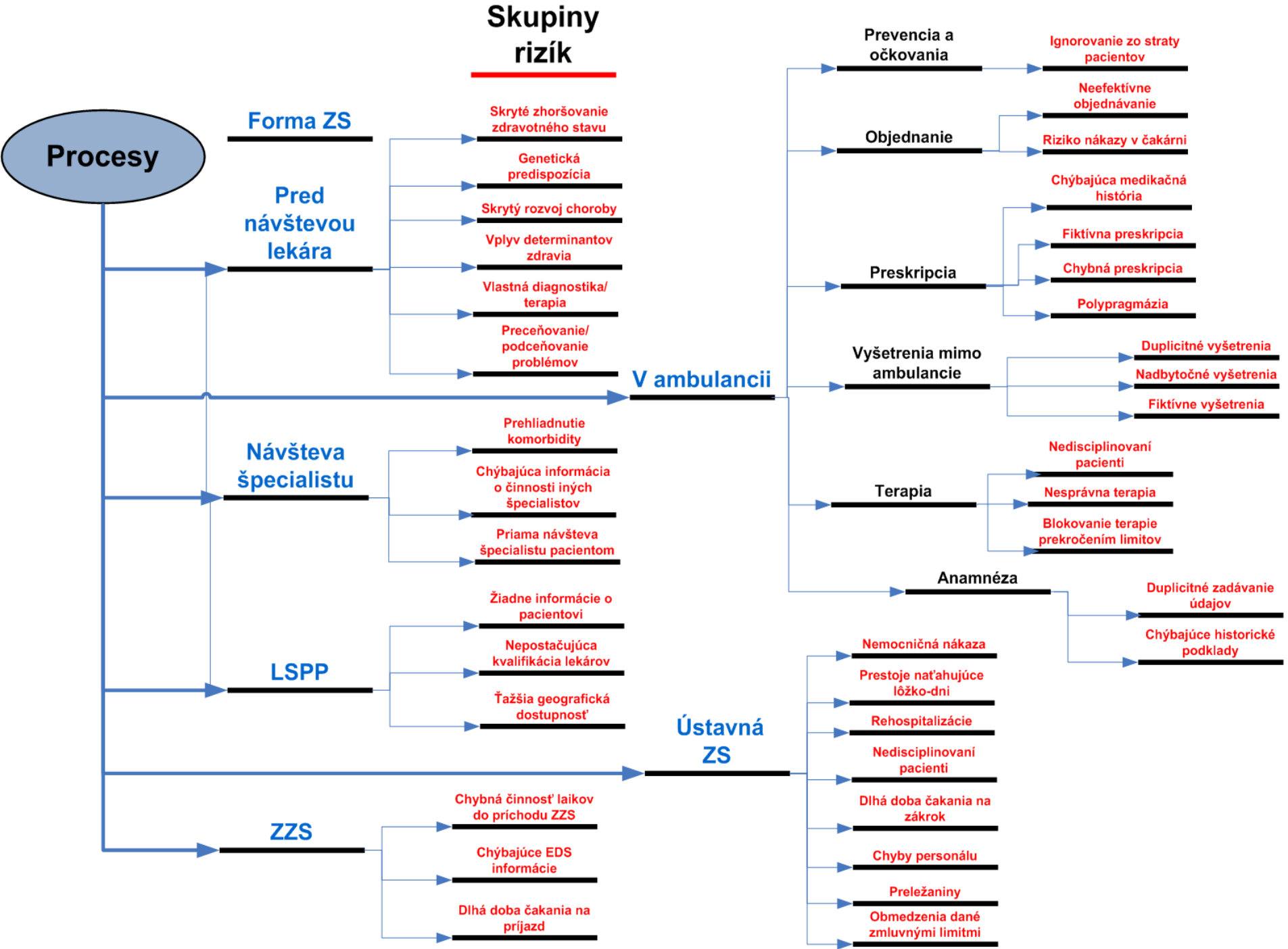
Identifikácia rizík v poskytovaní ZS

Úrovne v analýze:

- Všetky procesy v starostlivosti o zdravie
- Skupina procesov pre daného poskytovateľa ZS
- Konkrétny proces u poskytovateľa ZS
- Subprocesy
- Aktivity

- Relevantné entity z hľadiska analýz rizík:
 - Aktéri , dátové objekty, aktivity, vstupy a výstupy, súvisiace procesy, prostredie, prostredie realizácie procesu, potrebné nástroje pre jeho vykonanie

Nasledujúci obr. : identifikované riziká



Klinické vs. IT riziká v danom procese

Príklad: proces poskytovania neodkladnej ZS

Klinické riziko: chýbajúce informácie o pacientovi (napr. alergie, niektoré lieky, kardiostimulátor)

Manažment rizika: prostredníctvom eHealth dostane záchranár rýchlo EDS (emergency data set)

IT riziko: narušenie dôvernosti osobných údajov

Manažment rizika: manažment súhlasu, autentizácia zdravotníka, bezpečný prenos údajov, logovanie

Procesne orientovaná analýza rizík

Príklad č.2: Procesný pohľad a riziká

Generické oblasti rizík pre procesy (príklady)

- Proces nie je formálne identifikovaný a popísaný
- Proces je zle navrhnutý
- Proces nemá vlastníka
- Proces má nesprávne identifikovaných účastníkov
- Proces nenapĺňa požiadavky kvality (príslušných noriem)
- Proces okrem jeho dokumentácii nie je aplikovaný v praxi/je nedodržiavaný
- Proces nie je aktualizovaný/spravovaný

Procesne orientovaná analýza rizík

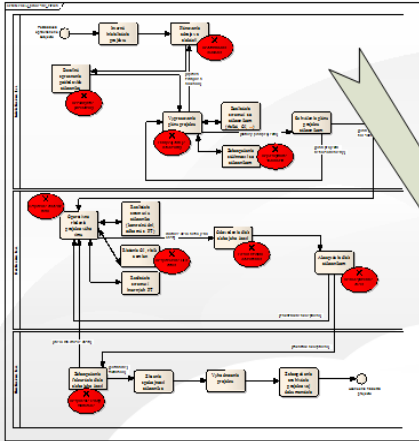
Riziká v konkrétnom procese: Riadenie projektov

Oblasti rizík, ktoré je potrebné identifikovať:

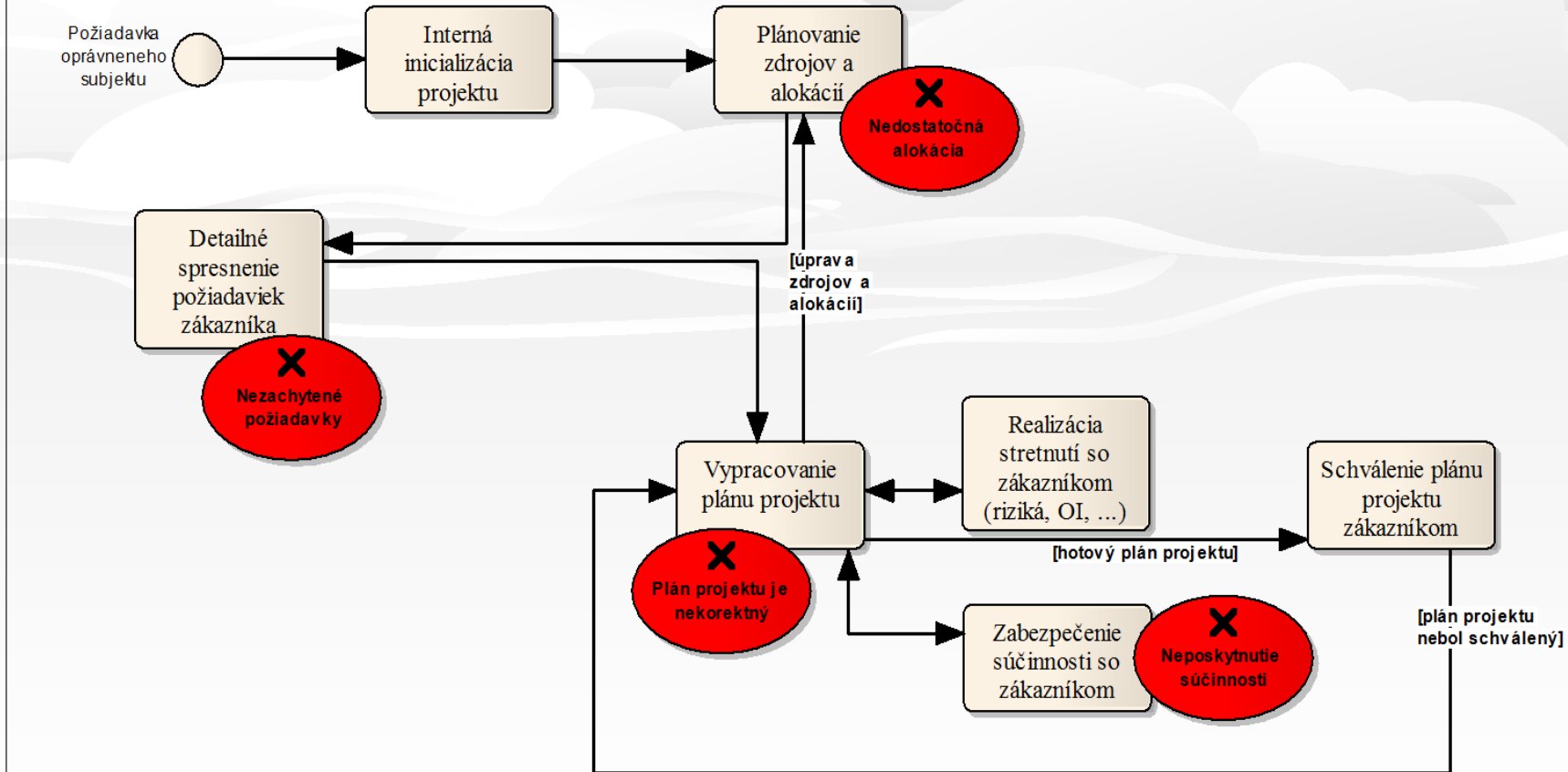
- Projektové (interné a externé riziká pre projekt)
- Finančné
- IT
- Administratívne, personálne ...

viď nasledujúce obr. procesu

Riziká v procese



BPMN PROJ_procesne_rizika



Proces – riadenie projektov

Aktivita: Alokácia zdrojov

Riziká:

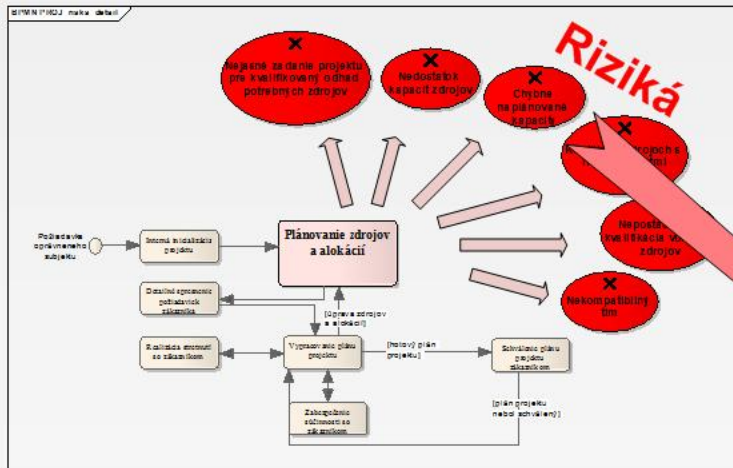
- Nedostatok odborných kapacít.
- Nepostačujúca kvalifikácia voľných zdrojov.
- Konflikty v zdrojoch s inými projektmi.
- Chybne naplánované zdroje.

Zraniteľnosti:

- Neznalosť rozsahu alokácií na iné plánované projekty.
- Nejasné zadanie projektu pre kvalifikovaný odhad potrebných zdrojov.
- Projekt je výnosovo nezaujímavý pre tím.
- Neskúsený PM.
- Nepodpísaná NDA pre externé zdroje.

Riziko a jeho manažment

Analýza rizík procesu



RIZIKO:

Chybné naplánované zdroje



ZDROJ RIZIKA

Zodpovedný pracovník definuje tím ktorý nie je schopný realizovať projekt podľa požiadaviek

Požiadavky na projekt nie sú jednoznačné pre úspešné definovanie tímu

ZRANITEĽNOSTI

Neskúsenosť pracovníka

Chybné pre

Krátky čas prípravy

Nedostatočný základ

MIERA VÝSKYTU

Stredná

MOŽNÉ

OPATRENIA 😊

DOPADY

Narušenie plánovaného termínu projektu

Overenie požiadaviek na tím so zákazníkmi

Sledovanie výkonnosti tímu

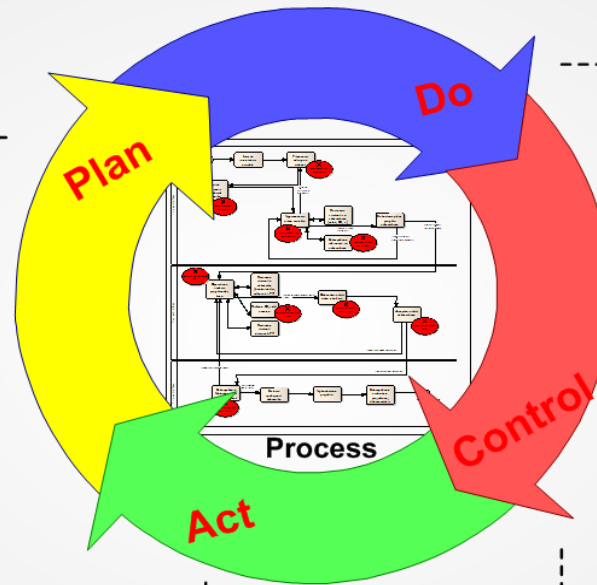
Generické riziká a zraniteľnosti procesu

Identifikácia podľa fáz PDCA metódy

PDCA

Plan
Do
Control
Act

Lifecycle of process



- Proces nie je formálne identifikovaný a popísaný
- Nekorektne zachytené kroky procesu
- Neidentifikovaná náväznosť s inými procesmi
- Nekorektne definované zdroje procesu
- Nekorektne definovaní účastníci procesu
- Nenapĺňané požiadavky organizácie a noriem kvality

- Neaktívny vlastník procesu
- Neaktívni účastníci procesu
- Neoptimálny manažment zdrojov procesu
- Nedodržiavanie definovaného postupu

- Neprijatie plánovaných vylepšení
- Nevyužitie možnosti automatizácie procesu
- Neprebiehajúce neustále zlepšovanie a optimalizácia

- Nedostatočné sledovanie a meranie
- Chýbajúce metodiky hodnotenia
- Nekorektné parametre sledovania



Ďakujem za pozornosť

michal.danilak@lynx.sk