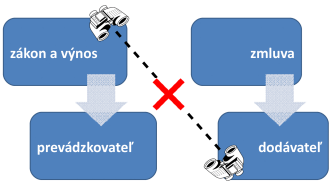
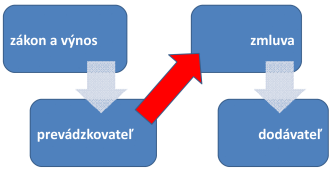
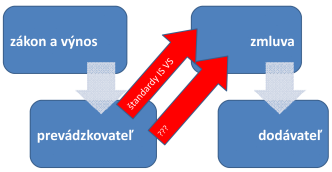
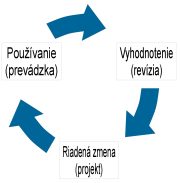
Vážené dámy, vážení páni, **rád by som Vám v tejto prezentácii priblížil praktický pohľad na cestu od Štandardov pre IS VS ku zmluve na správne fungujúci IS.**	**Informačné systémy vo verejnej správe** **-** **ŠTANDARDY** **a** **ZMLUVY**
Vždy, keď sa zavádzajú štandardy, sú dve možnosti – buď sa súčasne so štandardmi zavádzajú procesy a kompetencie pre atestovanie alebo nie. **IS pre VS sa na Slovensku neatestujú.** **Zákon o IS VS ukladá povinnosti prevádzkovateľom, teda obstarávateľom IS, nie dodávateľom.** **Dodávatelia IS pre VS sú teda viazaní iba zmluvami.**	**Povinnosti odberateľov a dodávateľov IS** 
Preto prevádzkovateľ potrebuje zmluvne preniesť na dodávateľov povinnosti určené Zákonom o IS VS a Vykonávacím pokynom – Štandardmi pre IS VS. **A z tohto dôvodu musí mať prevádzkovateľ pred uzavretím zmluvy odborný názor na implementáciu Štandardov pre IS VS a prípadných ďalších štandardných požiadaviek.** **Nemôže sa spoliehať na iniciatívu alebo profesionalitu dodávateľa.**	**Prenos (aj) zákonných povinností na dodávateľov zmluvou** 
Otázka je, či stačí zaviazať dodávateľa, aby sa riadil Štandardmi pre IS VS, alebo má byť tento záväzok širší. **Aby sme našli odpoveď na túto otázku, je potrebné uvedomiť si význam Štandardov pre IS VS v súvislostiach:** - **v kontexte systematickej štandardizácie,** - **v kontexte použitia – v procesoch objednávania, zadávania, vývoja, testovania, akceptácie, nasadzovania a používania informačných systémov.**	**Prenos (aj) zákonných povinností na dodávateľov zmluvou** 
Začneme tým, že si povieme aspoň nutné minimum o štandardizácii ako takej.	**Medzinárodné štandardy**

Štandardy sú <u>odporúčania od ľudí z praxe</u> pre ľudí z praxe. Ich základným odkazom je: „<u>poučte sa zo skúseností druhých</u> a vyhnite sa vlastným chybám".	**Vznik a vývoj štandardov** **Skúsenosti** **Odporúčania** **Štandardy**
Štandardy pre IS sa podobajú na technické normy. **Ich používanie je nepovinné.** **Ale pre dosiahnutie požadovaných vlastností produktov sú nutné,** **o sa najlepšie ukazuje pri <u>meraní</u> výsledných parametrov produktov.**	**Význam a poslanie štandardov** **Analógia technických noriem** **Nepovinné** **Podmieňujú vlastnosti produktov**
Ukážka – ako sa štandardy bežne používajú napríklad v nadnárodných koncernoch: **Používajú sa výbery z medzinárodných štandardov,** **ich používanie je v dcérskych spoločnostiach povinné** **a tým sa zaručujú vlastnosti produktov koncernových spoločností.** **<u>Štandardy sú najúčinnejším prostriedkom pre dosiahnutie garancií</u>.** **Prečo sa zaoberáme štandardizáciou v koncernoch? Pretože Štandardy pre IS VS sú ich <u>analógiou</u>.**	**Štandardizácia v koncernoch** **Výber zo štandardov** **Povinné používanie v koncerne** **Garancia vlastností produktov**
Štandardy pre IS VS takisto obsahujú výber z medzinárodných štandardov pre IS. **Takisto sa zákonom určuje povinnosť subjektov verejnej správy používať štandardy.** **Účelom je garantovanie vybraných vlastností IS, ktoré sa používajú vo verejnej správe.**	**Štandardy IS VS** **= analógia štandardizácie v koncernoch** **Výber zo štandardov** **Povinné používanie vo verejnej správe** **Garancia vlastností IS vo verejnej správe**
V tomto bode je dôležité uvedomiť si, komu štandardizácia slúži: **Štandardizácia IS VS slúži občanom.** **Nie je zameraná na prevádzkovateľov.**	**Štandardy IS VS** **Výber zo štandardov** **Povinné používanie vo verejnej správe** **Garancia vlastností IS vo verejnej správe** **GARANCIE PRE OBČANOV** **(~~nie pre prevádzkovateľa~~)**

Ak chceme štandardizáciu využiť aj v prospech prevádzkovateľov, budeme musieť rozšíriť okruh štandardov, ktoré budú určovať podmienky prevádzky nového systému. **Preto si teraz urobíme krátky prehľad dôležitých medzinárodných štandardov pre IS a porovnáme si ich obsah s obsahom Štandardov pre IS VS.**	**Štandardy IS VS a štandardy ISO**
Bezpečnosť informácií: prevzatá v plnom rozsahu. **Riadenie rizík: prevzaté, ale s obmedzením na bezpečnosť informácií.** **Procesy v životnom cykle IS – štandard, ktorý podrobne popisuje procesy a činnosti v jednotlivých etapách životného cyklu IS – nie je prevzatý.** **Hodnotenie parametrov IS, hodnotenie kvality SW – štandard, ktorý popisuje konkrétne kritériá pre hodnotenie SW – nie je prevzatý.**	**Štandardy IS VS - obsah** **Štandardy IS VS** • Formáty a protokoly • Bezpečnosť informácií • Projektové riadenie • Riadenie rizík bezpečnosti informácií • Pravidlá prístupnosti obsahu web-stránok + asistenčné technológie **Dôležité štandardy ISO** • Bezpečnosť informácií • Životný cyklus IS • Riadenie rizík procesov • Hodnotenie parametrov IS
Teraz si povieme základné informácie o vybraných štandardoch ISO pre informačné systémy, nezávisle na tom, či sú alebo nie sú prevzaté do Štandardov pre IS VS.	**Štandardy ISO pre informačné systémy**
Štandard pre riadenie bezpečnosti informácií určuje tri základné bezpečnostné parametre, ktoré musia byť vždy zaručené: • **dôvernosť informácie,** • **správnosť (integrita) informácie a** • **dostupnosť informácie.** **Často sa uvádza aj nepopierateľnosť autorstva informácie, to je ale osobitný prípad – ide o správnosť sprievodnej informácie o autorovi informácie.**	**ISO 2700x: Riadenie bezpečnosti informácií** **Dôvernosť** informácie **Správnosť** informácie **Dostupnosť** informácie
Riadenie bezpečnosti informácií je systematický cyklus založený predovšetkým na opakovaných analýzach rizík a porovnávaní potrebných a zrealizovaných opatrení.	**ISO 2700x: Riadenie bezpečnosti informácií** **Analyzovanie rizík** **Opatrenia** **Systematické riadenie**

Štandard Procesy v životnom cykle IS vychádza z faktu, že IS sa počas používania ďalej vyvíja a mení. **Podrobne popisuje procesy a činnosti hlavne vývojovej fázy – tie majú najväčší dopad.**	**ISO 12207:** **Procesy v životnom cykle IS** 
<u>Štandard pre riadenie rizík</u> upravuje riadenie <u>neurčitostí</u>, teda prípadov, kedy skutočnosti vstupujúce do procesov nie sú jednoznačné alebo nie sú zaručené. **<u>Procesné rámce</u>, spomínané aj v Štandardoch IS VS, sú takisto definované v tomto štandarde. Sú to zoskupenia vecne súvisiacich procesov.** **Napokon <u>rizikové scenáre</u> obsahujú podrobné rozpracovanie postupov pre konkrétne hrozby a riziká.**	**ISO 31000:** **Riadenie rizík / neurčitostí** **Neurčitosti v procesoch** **Procesné rámce** **Rizikové scenáre**
Pri porovnaní „originálu" s prevzatým štandardom vidíme, že kým Štandardy pre IS VS prevzali v plnom rozsahu riadenie projektových rizík a riadenie rizík bezpečnosti informácií, iné oblasti rizík vo výbere nie sú. **K tomuto uvádzam <u>príklad</u>: ak nový IS nebude podporovať likvidáciu neaktuálnych údajov, je veľmi pravdepodobné, že jeho prevádzka bude porušovať Zákon o archíve a registratúre a Zákon o ochrane osobných údajov (oboje závisí od spracúvaných údajov) a nepomôže, že informácie sú bezpečné (je garantovaná ich dôvernosť, správnosť aj dostupnosť). Riadenie rizík, obmedzené na bezpečnosť informácií, teda <u>nedokáže zabrániť riziku porušenia legislatívy</u>. Podobne nezabráni ďalším hrozbám ako je strata dobrého mena, finančné riziká a podobne. Tento príklad uvádzam s upozornením, že je v záujme povinnej osoby – prevádzkovateľa IS – použiť rozsah riadených rizík určený pôvodným štandardom, neobmedzovať ho v zmysle Štandardov IS VS.**	**ISO 31000:** **Riadenie rizík / neurčitostí** ***(vs. IS VS)*** · projekt · bezpečnosť informácií · legislatíva · dobré meno · ekonomika · prevádzka · …
Hodnotenie kvality SW – čo to nie je: **Hodnotenie kvality IS nie je Riadenie kvality.** **Certifikácia ISO 9000 neosvedčuje, že dodávateľ používa hodnotenie kvality IS.**	**ISO 250xx:** **Hodnotenie kvality SW** Hodnotenie kvality SW – ISO 250xx ≠ Riadenie kvality – ISO 900x

Hodnotenie kvality IS – čo to je:
(SQuaRE = Software Quality, Requirements and Evaluation) je hneď niekoľko štandardov:

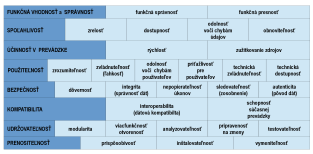
- **riadenie,**
- **modelovanie,**
- **meranie,**
- **požiadavky a**
- **hodnotenie**
  kvality software.

ISO 250xx:
Hodnotenie kvality SW

ISO 25000 Riadenie kvality SW
ISO 25010 Modelovanie kvality SW
ISO 25020 Meranie kvality SW
ISO 25030 Požiadavky na kvalitu SW
ISO 25040 Hodnotenie kvality SW

Konkrétne sú to parametre, ktoré vystihujú správne fungujúci IS:
bezproblémová funkčnosť + spoľahlivosť + vysoká účinnosť + bezproblémová použiteľnosť + bezpečnosť + otvorenosť + bezproblémová údržba a prenositeľnosť.
Každý z týchto parametrov obsahuje ďalšie podrobné ukazovatele.

ISO 25010
Model kvality SW



Na ďalšom obrázku sú zelenou resp. žltou zvýraznené ukazovatele, ktoré majú výraznú resp. relevantnú oporu v Štandardoch IS VS.

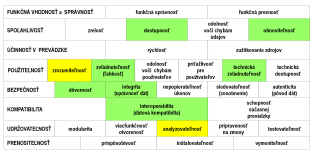
Interoperabilita, čiže schopnosť systému spolupracovať s inými systémami, má výraznú podporu vďaka podrobnej úprave formátov a protokolov.

Veľmi dobrú podporu má aj použiteľnosť používateľského rozhrania, keďže sú prevzaté aj Štandardy prístupnosti webových stránok.

Žiaľ väčšina ukazovateľov kvality nemá porovnateľnú podporu v Štandardoch pre IS VS. Tie iba uvádzajú v ustanovení o riadiacom výbore projektu, že „projekt bude spĺňať dohodnuté kritériá a vytvorí výstupy, dielo alebo službu podľa dohodnutej špecifikácie a v príslušnej kvalite".

Na ďalšom obrázku si preto predvedieme príklad úpravy, ktorá nie je v Štandardoch pre IS VS – ako sa dá dosiahnuť konkrétny parameter: správne fungovanie.

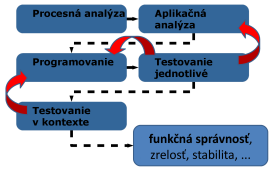
ISO 25010
Model kvality SW
(vs. IS VS)



Vývoj začína procesnou analýzou, po ktorej nasleduje aplikačná analýza a až potom začína samotné programovanie. Procesná analýza zmapuje všetky činnosti a ku každej činnosti priradí vstupujúce a vystupujúce údaje. Aplikačná analýza premietne jej výsledky do návrhu technického riešenia.

Každá naprogramovaná funkcia sa testuje a to jednotlivo aj v súvislostiach. Vykonáva sa pozitívne aj negatívne testovanie, t. zn. zisťuje sa nielen, či funkcia „robí, čo má robiť", ale aj, či

Príklad:
dosiahnutie požadovaných parametrov (ISO25xxx) použitím štandardu Procesy ŽC IS (ISO12207)
parameter: funkčná správnosť

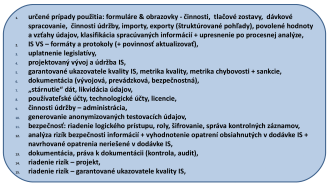


„nerobí, čo nemá robiť“. **Uvedené činnosti sa opakujú, kým výsledky testov nepotvrdia úplný súlad s požiadavkami. Takýto postup vedie nielen ku správnosti funkcionality, ale aj k jej zrelosti a stabilite.**	
Porovnali sme si informácie o medzinárodných štandardoch pre informatiku s Výnosom o štandardoch pre IS VS. **Teraz môžeme zhrnúť, čo je potrebné dojednať v zmluvách nad rámec Štandardov pre IS VS a ako to dosiahnuť.**	**Odporúčaný postup k dobrým zmluvám**
Odporúčam doplniť postup obstarávania IS o predkvalifikáciu s obsahom: • **zistiť, ako sa v informačných systémoch od dodávateľov uplatňuje legislatíva a jej zmeny,** • **preveriť, či dodávatelia projektujú vývoj IS alebo sú niektoré činnosti vývoja spontánne,** • **preveriť, či dodávatelia dokážu zaručiť kvalitatívne parametre IS a či ich dokážu zaručiť súčasne,** • **preveriť štruktúru a kvalitu dokumentácie informačných systémov,** • **preveriť stárnutie dát –etapy životného cyklu informácií v informačných systémoch,** • **zistiť (skryté) nároky na používateľské účty, technologické účty a na licencie,** • **zistiť činnosti údržby – administrácie, majú byť naprojektované,** • **zistiť schopnosť dodávateľov vytvoriť anonymnú testovaciu databázu s takými parametrami, aké má prevádzková databáza – táto otázka preveruje nielen nezávislosť dodávateľa na produkčnej databáze, ku ktorej nemá mať prístup, ale aj zisťuje, či rozumie procesom a vzťahom medzi údajmi,** • **zistiť, ako budú chránené informácie v systéme, najmä riadenie logického prístupu, použitie prístupových rol (pozícií), šifrovanie, správa kontrolných záznamov (prednostne zápis činností používateľov, až následne ich vplyv na dáta, možnosť štruktúrovaných pohľadov na kontrolné záznamy, riadené vymazávanie kontrolných záznamov)** • **metodicky môže pomôcť napríklad katalóg opatrení podľa vyhlášky 164/2013 Z. z.**	**Odporúčaný postup:** **PREDKVALIFIKÁCIA** **– nároky na dodávateľov** 1. uplatnenie legislatívy pri vývoji a aktualizáciách SW (archív a registratúra, ochrana osobných údajov...), 2. proces tvorby IS – projektovanie, analýzy, vývoj, priebežné testovanie..., 3. garantované ukazovatele (parametre + súčasné plnenie, metrika vrátane metriky chýb), kvantifikácia akceptačných kritérií, 4. dokumentácia (vývojová, prevádzková, bezpečnostná), 5. „stárnutie“ dát, vymazávanie / likvidácia údajov, 6. používateľské účty, technologické účty, licencie, 7. činnosti údržby – administrácia, 8. generovanie anonymizovaných testovacích údajov, 9. bezpečnosť: riadenie logického prístupu, roly, šifrovanie, správa kontrolných záznamov / zápis činností, výber, vymazávanie, ... pomôcka: vyhláška 165/2013 Z. z. - opatrenia

A napokon finále: <u>rekapitulácia</u>, čo má obsahovať zmluva – dôležité body, vďaka ktorým sa vyhneme veľkým problémom:

- **prípady použitia – všetky činnosti používateľov, činnosti dávkového spracovania, činnosti údržby, importy, exporty alebo štruktúrované pohľady, povolené rozsahy hodnôt údajov individuálne a vo vzájomných vzťahoch, určenie stupňa utajenia spracúvaných informácií,**
- **formáty a protokoly určené v Štandardoch pre IS VS + povinnosť dodávateľa riadiť sa zákonom o IS VS,**
- **všetky body prerokované v predkvalifikácii – ich výsledky,**
- **analýzu rizík bezpečnosti informácií, vyhodnotenie opatrení obsiahnutých v dodávke IS + potrebné opatrenia neriešené v dodávke IS,**
- **ujednanie o právach k dokumentácii, hlavne právo sprístupniť všetky dokumenty kontrolným orgánom,**
- **riadenie rizík procesov projektu,**
- **riadenie rizík súvisiacich s vlastnosťami informačného systému, najmä ukazovateľov kvality IS.**

Odporúčaný postup:
odporúčaný
OBSAH ZMLÚV



Ďakujem za pozornosť

Ing. Ľubomír Janoška
LJanoska@OchranaOsobnychDat.sk
www.OchranaOsobnychDat.sk
+421 908 112 372