Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Zavedenie systému manažmentu Informačnej bezpečnosti

Daniel Olejár

Jún 2013

KPMG
cutting through complexity™

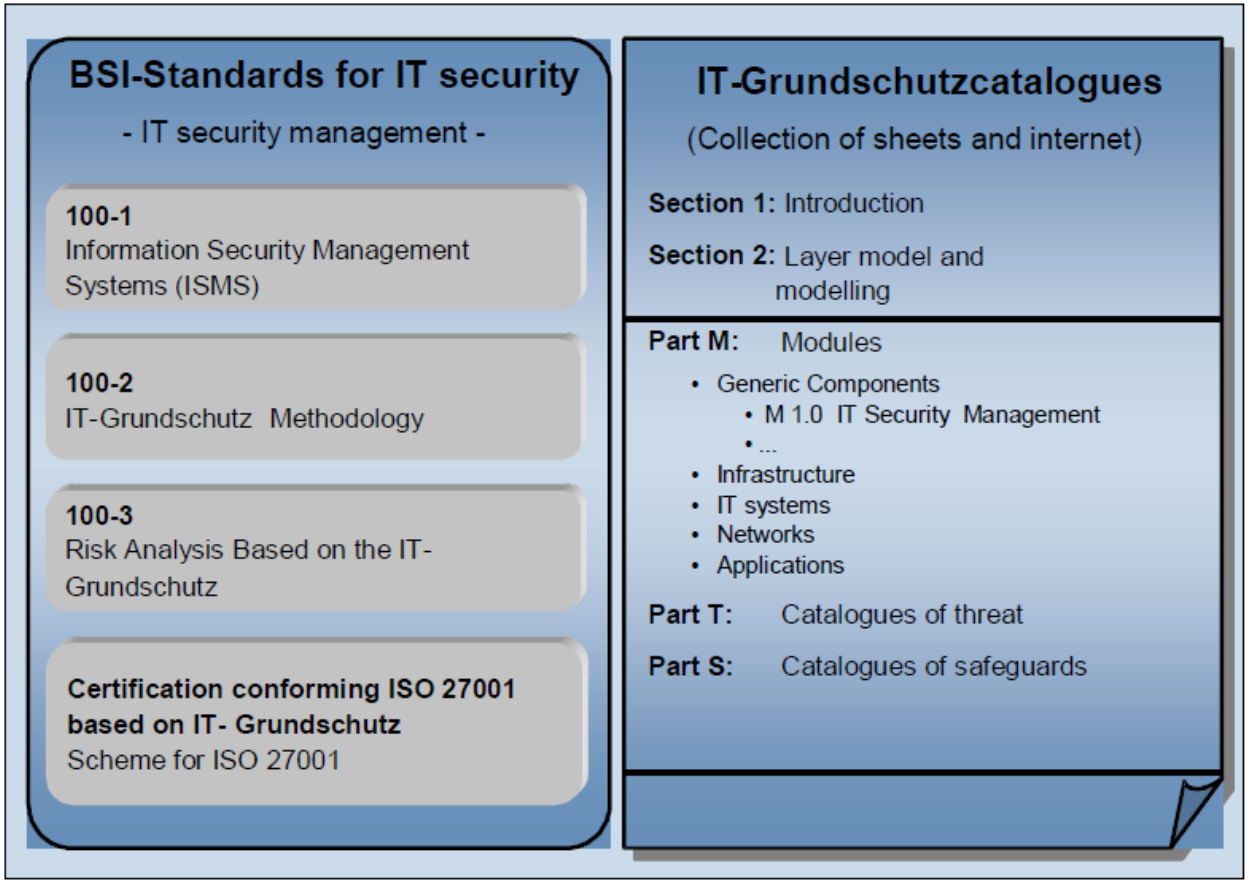
Úvod

- Zaistenie potrebnej úrovne ochrany prvkov CRITIS si vyžaduje systematický prístup k IB (zmeny podmienok)
- Forma: systém manažmentu informačnej bezpečnosti (ISMS)
- Základ ISO/IEC 27001,2; resp. Bezpečnostné štandardy ISVS
- Preberali sme viacero relevantných tém:
  - Analýza rizík
  - Bezpečnostný projekt
  - štandardy
  - Naposledy ISMS
- ISO normy:
  - 27001 požiadavky na ISMS
  - 27002 Bezpečnostné funkcie
  - 27003 Implementácia ISMS
- Vhodnejšie BSI Standards 100-1 a 2 (praktickejšie, kompatibilné s ISO 27001)

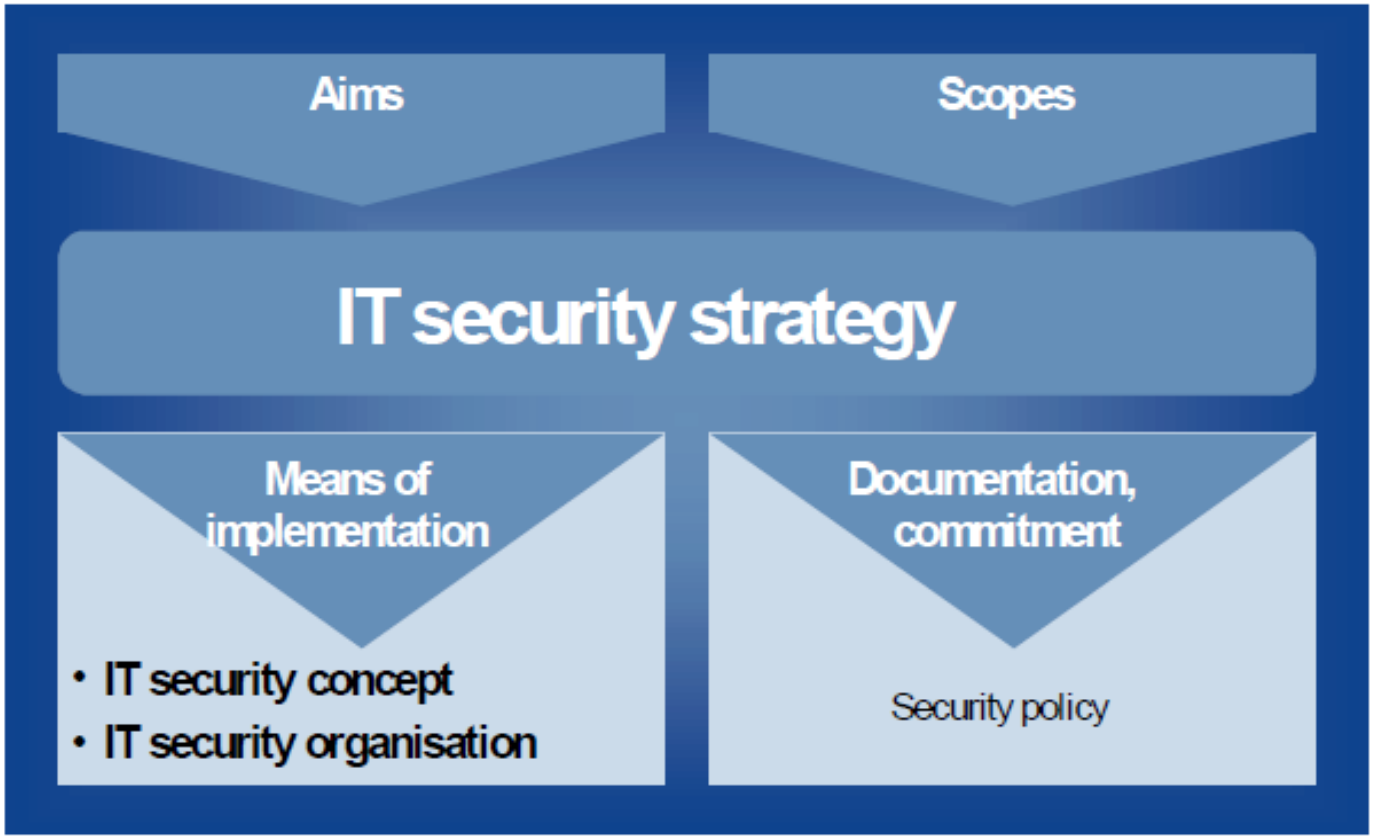
Filozofia IT-Grundschutz

- Pragmatický prístup:
  - IB je zložitá, drahá, nie je dosť kvalifikovaných ľudí, ale
  - Používajú sa rovnaké technológie, v podobných podmienkach na podobné účely:
  - Na rovnaké problémy možno použiť štandardné riešenia
  - Veľmi pomôže už systematická ochrana na základnej úrovni
  - Od 90. rokov IT-Grundschutz, každoročne vydávaný praktický manuál
  - Neskôr (2005): oddelenie a štandardizácia IT-Grundschutz od samostatného katalógu modulov
- Chráňme všetko na základnej úrovni a identifikujme systémy (aktíva), pre ktoré nestačí základná úroveň ochrany a tie riešme individuálne
- Podrobne rozpracovaná v BSI Štandardoch, dodatkoch ku Štandardom a Katalógu

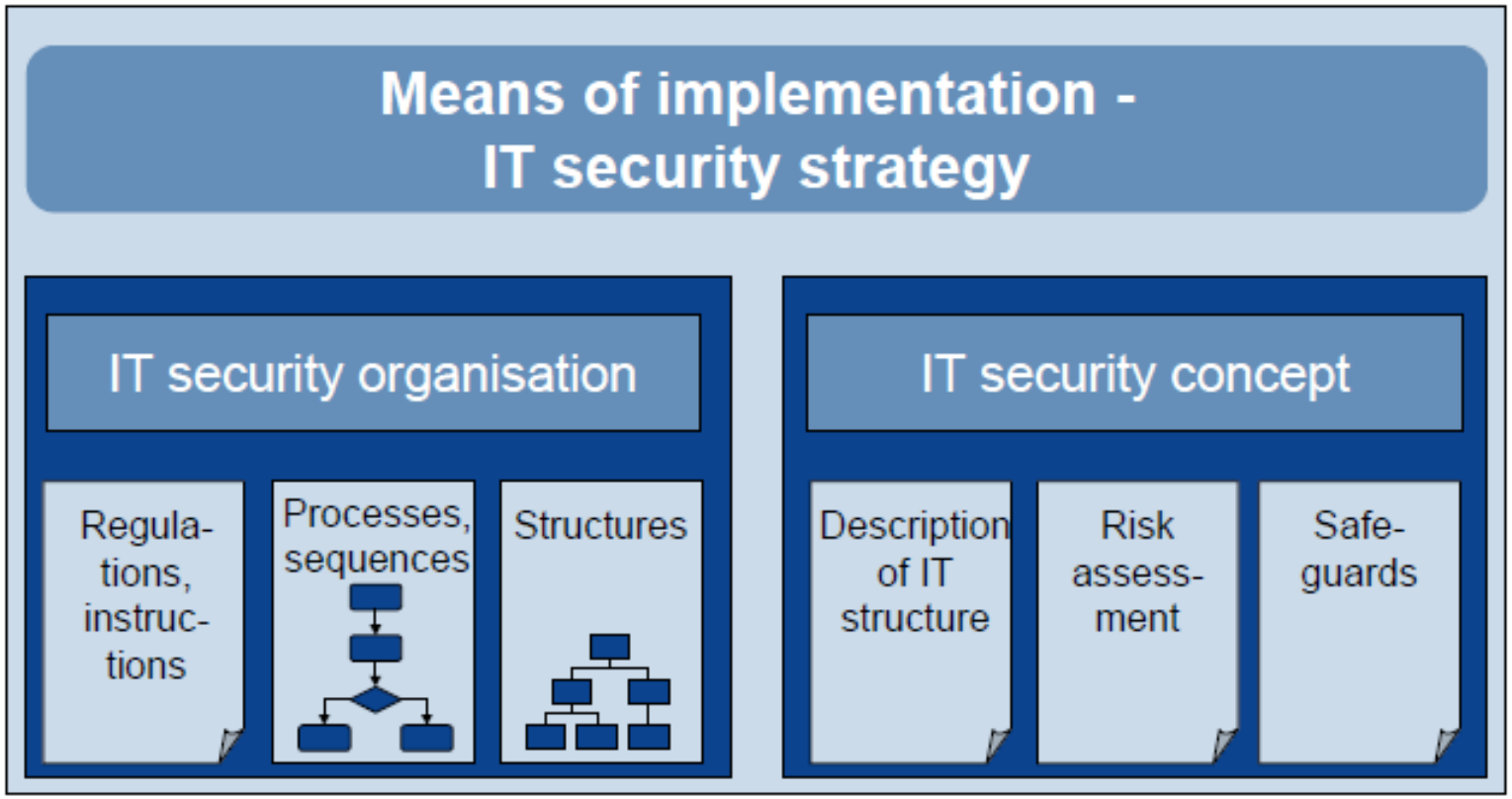
Publikácie BSI týkajúce sa manažmentu IB



ISMS podľa BSI



Implementácia IT bezpečnostnej stratégie (BSI)



IB ako proces

- BSI chápe IB ako súvislý proces, ktorý nazýva IT bezpečnostný proces
- Problém:
  - IT bezpečnostný proces nie je lineárny (rekurzia), tá istá úloha sa rieši iteratívne
  - Aj IT proces má životný cyklus
- Klasický Plan-Do-Check-Act

Inicializovanie IT bezpečnostného procesu 1/3

- Návrh a plánovanie ITSEC procesu:
- ITSEC proces musí inicializovať vedenie organizácie
- Určenie podmienok prostredia
  - Stanovenie kľúčových procesov, špeciálnych úloh a ich závislosti od IT
    - Bez ktorých procesov by organizácia nemohla plniť svoje poslanie?
    - Ktoré procesy by nemohli bežať, keby nefungovali IKT?
  - Každý proces, aplikácia má stanoveného vlastníka (pozná proces/aplikáciu a má dostatočné kompetencie), ktorý vie odhadnúť ich dôležitosť
  - Pre každý proces/aplikáciu – definovaná potrebná úroveň ochrany
    - Ktorá informácia sa spracováva pre potreby kľúčových procesov
    - Ktorú informáciu treba chrániť (CIA)
- 3 úrovne ochrany
  - Normálna
  - Vysoká
  - Veľmi vysoká

Inicializovanie IT bezpečnostného procesu 2/3

- Úrovne ochrany podľa BSI:
  - **Veľmi vysoká** (zlyhanie IKT vedie ku kolapsu organizácie, a/alebo má veľký vplyv na spoločnosť) striktné požiadavky na dôvernosť, integritu a dostupnosť (nepripúšťa sa výpadok systému)
  - **Vysoká** (zlyhanie IKT vyradí z činnosti kľúčové časti inštitúcie; významné poškodenie organizácie a dopad na tretie strany) striktné požiadavky na dôvernosť a integritu a pripúšťa sa len krátky výpadok systému
  - **Normálna** (výpadok IKT poškodzuje inštitúciu) ochrana dôvernosti internej informácie, nepodstatná strata integrity, krátke výpadky (neohrozujúce termíny plnenia úloh)

- Porovnanie s predchádzajúcimi bezpečnostnými požiadavkami
- Nejde sa do podrobností (konkrétne systémy, aplikácie, nerobí sa ešte analýza rizík)

Inicializovanie IT bezpečnostného procesu 3/3

- V tejto fáze sa zohľadňujú aj externé podmienky relevantné pre IB
- Súhlas vedenia organizácie s bezpečnostnými požiadavkami (kvôli potrebným zdrojom)

- Príprava bezpečnostnej politiky (význam a obsah už poznáme)
  - Získať poverenie vedenia vypracovať Bezpečnostnú politiku (BP)
  - Definovať pôsobnosť BP (scope)
  - Vytvoriť pracovnú skupinu, ktorá pripraví BP
  - Príprava BP
  - Schválenie vedením organizácie
  - Zverejnenie BP
  - Pravidelná kontrola a aktualizácia BP

Organizácia IB 1/5

- Organizácia IB = organizačná štruktúra na podporu a implementáciu IT bezpečnostného procesu

- Základná požiadavka: definovať roly v IB
  - Celková zodpovednosť za IB – vedenie inštitúcie
  - Aspoň jeden človek primárne zodpovedný za presadzovanie a koordinovanie IB (bezpečnostný manažér)
  - Každý zamestnanec organizácie je zodpovedný za IB v okruhu svojej pôsobnosti

- Integrovanie IB do všeobecných procedúr a procesov

- Ustanovenie organizácie IB
  - Závisí od veľkosti a potrieb organizácie

Organizácia IB 2/5

- Prepojenie na vedenie inštitúcie

- Veľká inštitúcia
  - Hierarchická štruktúra organizácie IB (výbor pre koordináciu IT, tím pre IB, reprezentanti používateľov IT)
  - Manažér IB
  - Špecialisti IB aj iní zamestnanci s povinnosťami v IB
  - Ľudia s explicitnou zodpovednosťou za IB aj na nižších úrovniach (oblasti činnosti, projekty)

- Stredne veľká inštitúcia
  - Nemá tím pre IB
  - Len manažér IB a manažérov IB pre systémy/projekty
  - Vypadli manažéri IB pre oblasti

Organizácia IB 3/5

- Malá inštitúcia
  - IT manažér
  - IB manažér

- Vo všetkých typoch inštitúcií
  - Jasne definované úlohy pre každého člena bezpečnostného manažmentu
  - Dostatočné kompetencie (zapojení do rozhodovania)

Organizácia IB vo veľkej inštitúcii podľa BSI

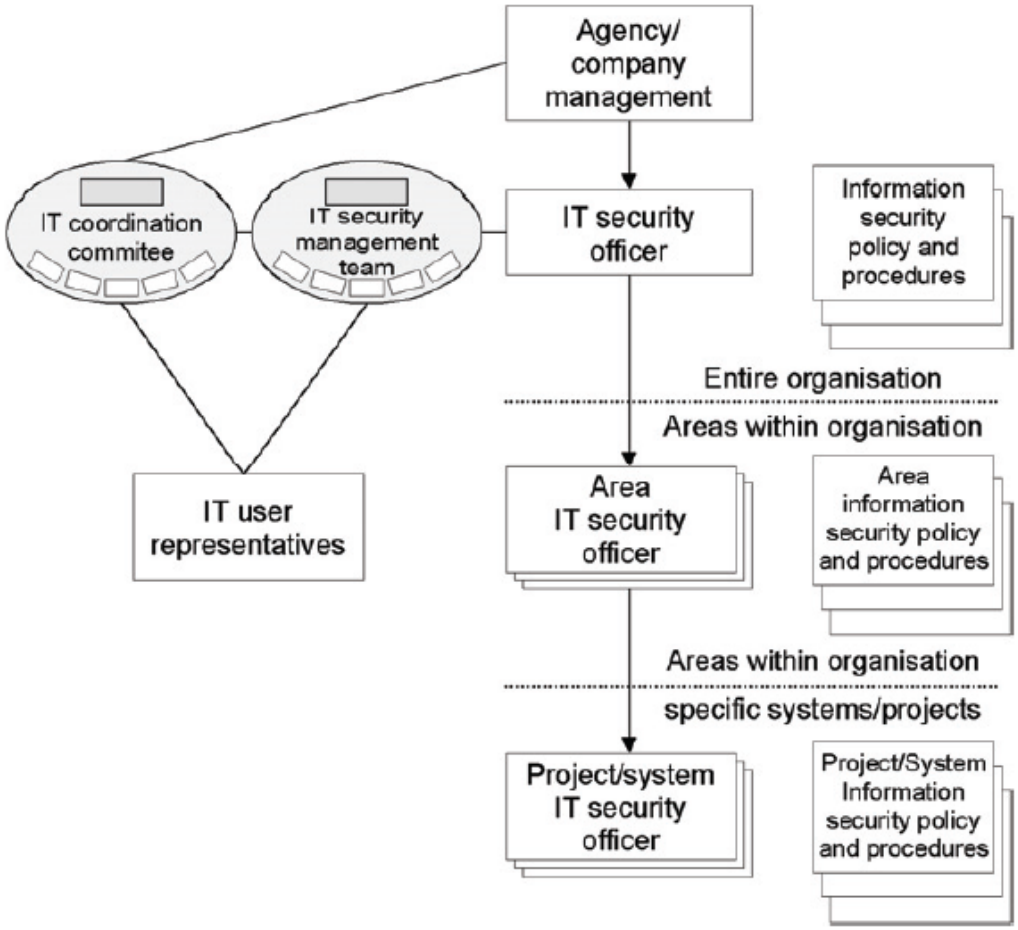


Figure: Structure of the IT security organisation in a large institution

Organizácia IB v stredne veľkej inštitúcii podľa BSI

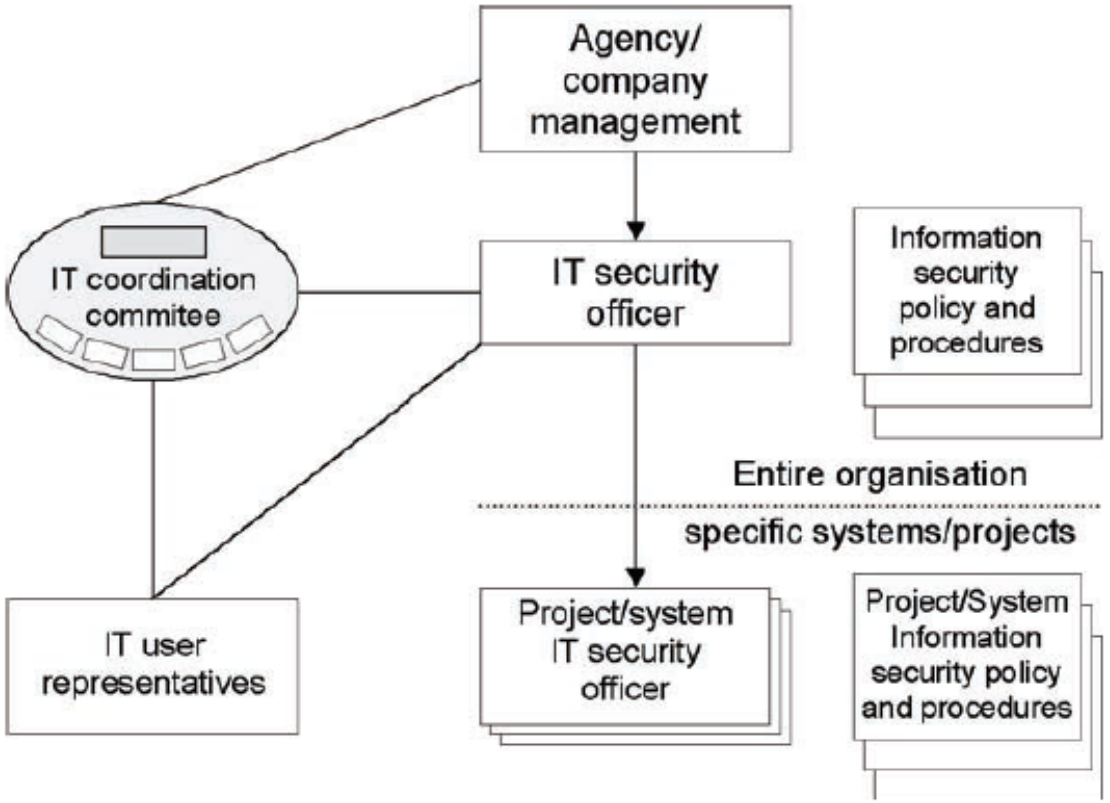


Figure: Structure of the IT security organisation in a medium-sized institution

Organizácia IB v malej inštitúcii podľa BSI

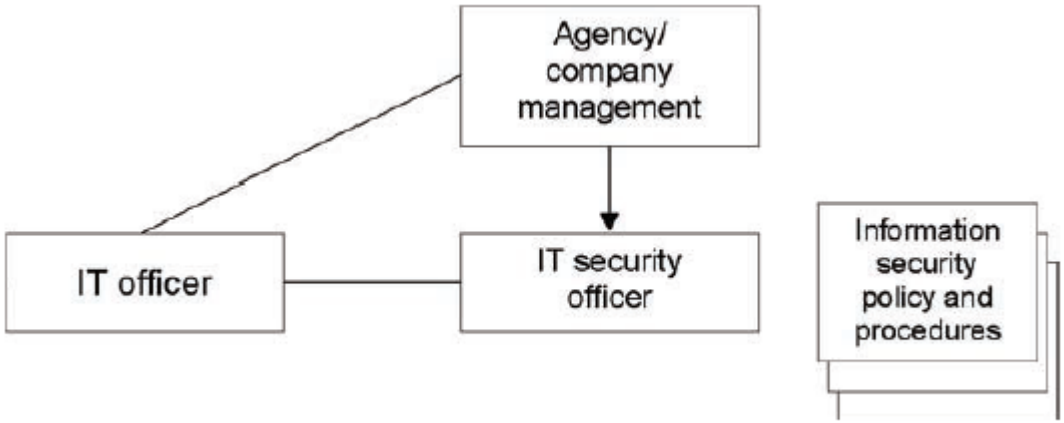


Figure: Structure of the IT security organisation in a small institution

Organizácia IB 4/5

- Bezpečnostný manažér
  - Manažment IB a plnenie úloh súvisiacich s IB
  - „bezpečnostný expert“ vedenia inštitúcie
  - Koordinuje tvorbu koncepčných bezpečnostných dokumentov a bezpečnostnej dokumentácie nižšej úrovne
  - Iniciuje implementáciu a monitoruje implementované bezpečnostné aktivity (opatrenia)
  - Podáva správy vedeniu o stave IB
  - Koordinuje projekty súvisiace s IB
  - Vyšetruje bezpečnostné incidenty
  - Iniciuje a koordinuje vzdelávanie v IB a zvyšovanie bezpečnostného povedomia
  - Zapája sa do nových projektov (zakomponovanie IB)

- Kvalifikačné a osobnostné predpoklady

Organizácia IB 5/5

- Tím pre manažment IB
  - V krajnom prípade jednočlenný (manažér IB)
  - Pomáha manažérovi IB riešiť úlohy
  - Skôr pracovná skupina zložená z relevantných ľudí
  - Aspoň pri Iniciovaní IT bezpečnostného procesu (priorita)
- Manažéri IB pre oblasť, projekt, systém
- IT koordinačný výbor (trocha umelý prvok)
  - Nie je stály
  - Koordinuje spoluprácu
    - Vedenia
    - Tímu pre manažment IB
    - IT používateľov

Zdroje pre IB

- Spravidla obmedzené zdroje
- Uplatniť Cost/benefit ratio (spravidla logaritmická krivka)
- Najprv poriadok (organizačné a technické opatrenia)
  - Napr. IT: zlá štruktúra, málo zdrojov, nedostatok kvalifikovaných ľudí
- Manažér IB, ostatní členovia IB tímu robia IB len ako jednu z úloh
- Prostriedky na manažment a monitoring IB
- nedostatok IB ľudí (outsourcing, ale čo a za akých podmienok)

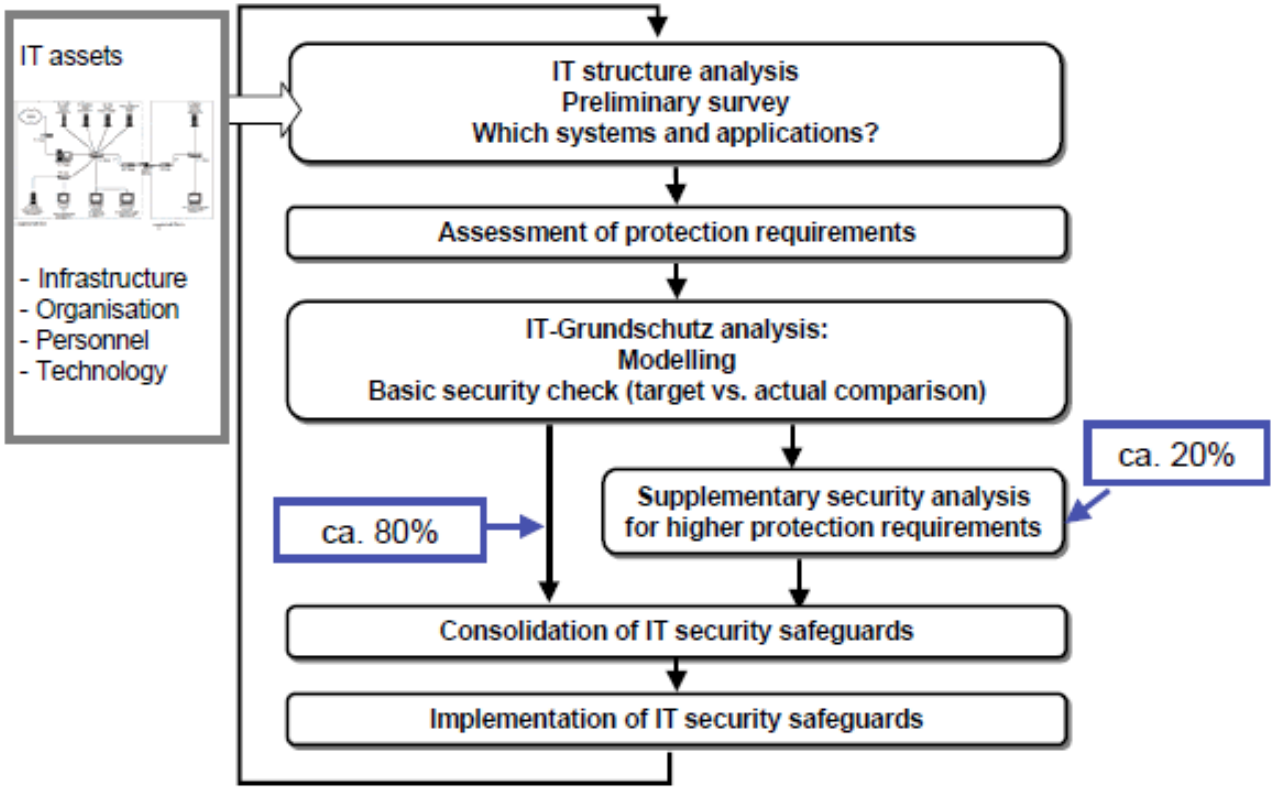
Zapojenie zamestnancov

- Všetci zamestnanci, aj externí + dodávatelia
- Od vstupu do zamestnanie, po ukončenie zamestnania
- Vedenie príkladom
- Vzdelávanie a zvyšovanie bezpečnostného povedomia
- Kontaktná osoba a známe informačné kanály (na oznamovanie zraniteľností, bezpečnostných incidentov)
- Zapojenie zamestnancov do tvorby a implementácie IB koncepcií
- Procedúry pri zmene zamestnania/pracovného zaradenia

Vytvorenie bezpečnostnej koncepcie 1/2

- Kde sme
- Inicializovali sme IT bezpečnostný proces
- vytvorili Bezpečnostnú politiku
- Zaviedli organizáciu IB
- Teraz nasleduje IT bezpečnostná koncepcia organizácie
- BSI Štandard vychádza z IT-Grudschutz metodológie, ktorá však je použiteľná aj v našich podmienkach (bez použitia katalógov BSI: hrozby a opatrenia)
- Analýza rizík
- U nás kompletná
- Podľa IT-Grudschutz: identifikácia aktív vyžadujúcich špeciálnu ochranu

Príprava IT bezpečnostnej koncepcie podľa BSI



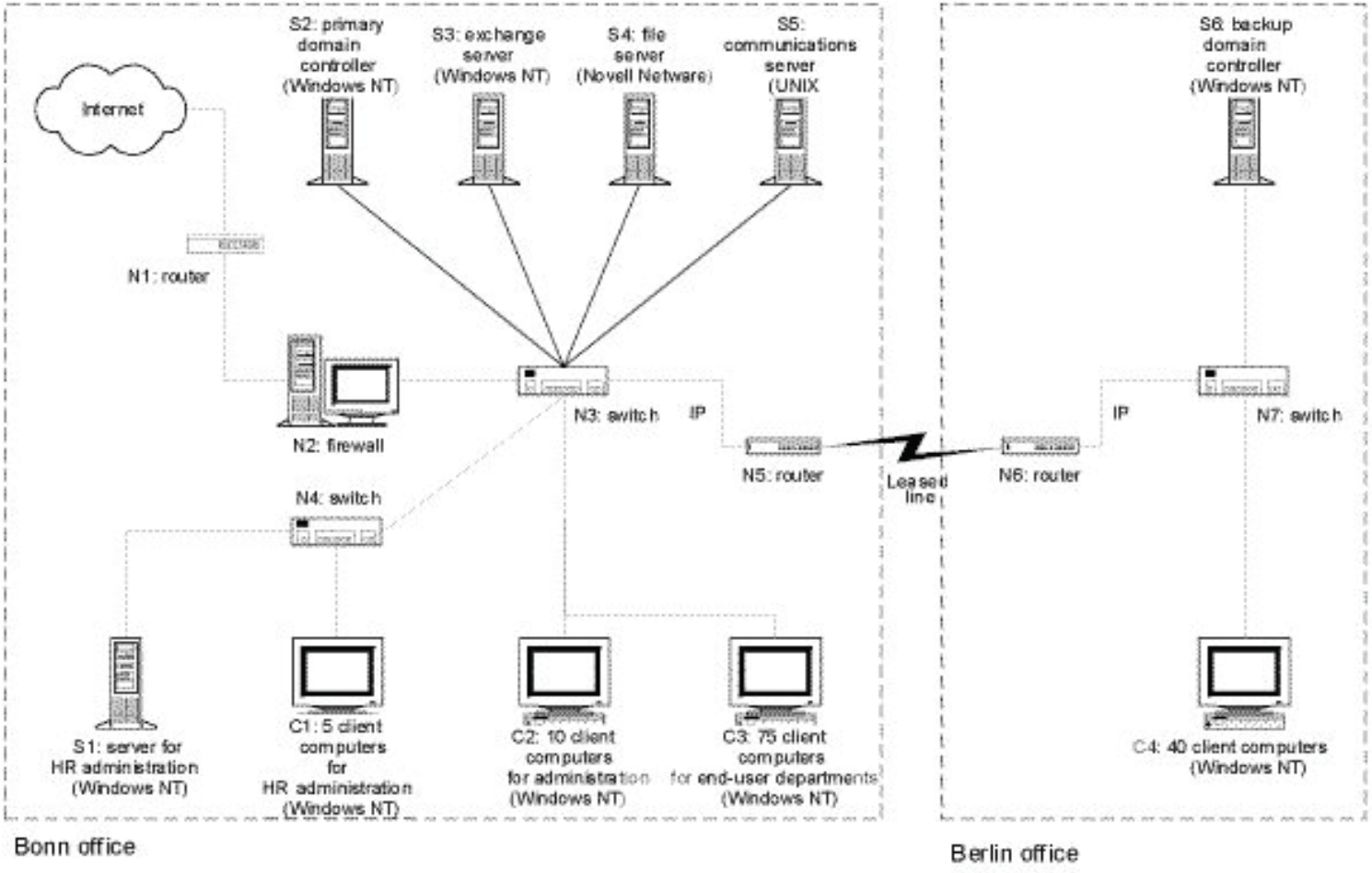
Vytvorenie bezpečnostnej koncepcie 2/2

- Postup podobný ako pri tvorbe bezpečnostného projektu, resp. analýze rizík
- Identifikácia (IT) aktív
- Analýza IT infraštruktúry
- Definovanie bezpečnostných požiadaviek
- Návrh IT bezpečnosti
- Kontrola základnej úrovne IB
- Audit bezpečnosti IT
- Dodatočné bezpečnostné opatrenia
- Implementácia bezpečnostnej koncepcie IT
- Prípadná certifikácia

Analýza IT štruktúry 1/3

- BSI Štandard poskytuje veľmi podrobný návod, v prezentácii ho uvedieme, ale nebudeme rozoberať
- Dokumentácia IT aktív
  - Dá sa postupovať aj opačne: dôležitá informácia – IT aplikácia – IT systém
  - Siete, IT systémy, aplikácie, miestnosti, kategorizácia IT položiek
- Siete
  - Základná informácia v podobe obrázku topológie siete
  - IT systémy, aktívne sieťové komponenty, sieťové tlačiarne, a.i. [meno, typ a funkcia, platforma (HW a OS), umiestnenie, správca, komunikačné rozhrania, sieťové spojenie a sieťová adresa]
  - Prepojenie medzi systémami [typ linky, prenosová rýchlosť, sieťové protokoly]
  - Prepojenie na vonkajší svet [+ provider]
  - Časti siete s rozličnými požiadavkami na ochranu
  - Kontrola aktuálnosti popisu (plánu) siete

Príklad plánu siete (BSI Štandard 100-2)



Analýza IT štruktúry 2/3

- Zber informácie o IT systémoch
- Zber informácie o IT aplikáciách (stačí tabuľková forma) na ktorých IT systémoch beží a aké citlivé údaje sa v nej spracovávajú
- Nasledujúca tabuľka je prebratá zo BSI Štandardu 100-2

Description of the IT applications			IT systems						
Applic. no.	IT application / information	Personal data	S1	S2	S3	S4	S5	S6	S7
A1	Processing of HR data	X	X						
A2	Benefits processing	X	X						
A3	Travel expense accounting	X	X						
A4	User authentication	X		X				X	
A5	System management			X					
A6	Exchange (E-mail, appointment calendar)	X			X				
A7	Central document administration					X			

Analýza IT štruktúry 3/3

- Dokumentácia miestností v podobe tabuľky [meno, typ, umiestnenie, čo je v nej, požiadavky na ochranu, CIA, vyplnia sa neskôr]

- Kategorizácia
  - Kvôli redukcii zložitosti
  - Zoskupenie podobných aktív a typ namiesto triedy:
    - Rovnaký typ
    - Rovnaká konfigurácia
    - Pripojenie k sieti
    - Rovnaké administratívne a infraštrukturálne podmienky
    - Tie isté aplikácie
    - Tie isté požiadavky na ochranu

Definovanie požiadaviek na ochranu 1/4

- Najprv definícia úrovní ochrany

- Aké dôsledky bude mať narušenie CIA (na proces, aplikáciu, údaje)
  - Scenáre (čo sa stane keď...?)
    - Porušenie zákonov, nariadení, zmlúv
    - Ohrozenie osobných údajov
    - Fyzické zranenie
    - Znemožnenie vykonávania povinností
    - Negatívne vnútorné a vonkajšie efekty
    - Finančné následky

- Tabuľka [aplikácia, údaje, požadovaná úroveň ochrany vzhľadom na CIA, zdôvodnenie]

Definovanie požiadaviek na ochranu 2/4

- Význam aplikácie voči procesu
  - Normálny: proces sa dá vykonať iným spôsobom a náklady na tento spôsob sú akceptovateľné
  - Vysoký: alternatívne riešenie s vysokými nákladmi
  - Veľmi vysoký: proces sa bez aplikácie nedá vykonať

- Definovanie požiadaviek na ochranu IT systémov
  - Máme zoznam systémov s aplikáciami
  - Ohodnotenie aplikácií
  - Ohodnotenie systému na základe všetkých aplikácií, ktoré na ňom bežia; princíp maxima
  - Závislosť aplikácií (výstup jednej = vstup druhej) – prenesenie úrovne ochrany na inú aplikáciu aj IT systém
  - Kumulatívny efekt (viac aplikácií na jednom systéme)
  - Aká časť aplikácie beží na systéme (vysoká úroveň ochrany, ale len nepodstatná časť aplikácie)

Definovanie požiadaviek na ochranu 3/4

- Požiadavky na ochranu komunikačných liniek

- Kritické linky
  - Spojenie s externým prostredím (prechádzajú nechráneným prostredím)
  - Prenášajúce informáciu s (veľmi) vysokými požiadavkami na ochranu
  - Cez ktoré sa nemôže prenášať veľmi citlivá informácia

- Ochrana kritických liniek – šifrovanie, redundancia

- Požiadavky na ochranu miestností
  - Odvodené od IT systémov v miestnosti
  - Princíp maxima
  - Zohľadniť aj závislosť systémov a aplikácií a kumulatívny efekt
  - zdokumentovať

Definovanie požiadaviek na ochranu 4/4

- Princíp maxima zvyšujú sa požiadavky na ochranu

- Bezpečnostné zóny
  - Geografické
  - Technické
  - Personálne

Výber bezpečnostných opatrení 1/3

- Pri klasickej analýze rizík
  - Identifikácia relevantných hrozieb
  - stanovenie rizík
  - Ohodnotenie rizík
  - Výber bezpečnostných opatrení
- IT-Grundschutz má veľa vecí pripravených v predstihu v podobe modulov
- Modul
  - Hrozby
  - Opatrenia
- Predpokladá sa typické prostredie (štandardné aktíva, spôsob použitia a pravdepodobnosť naplnenia hrozby)

Výber bezpečnostných opatrení 2/3

- Moduly
  - Generické aspekty IB (týkajú sa skoro všetkých aktív)
  - Bezpečnosť infraštruktúry
  - Bezpečnosť IT systémov
  - Bezpečnosť sietí
  - Bezpečnosť aplikácií

- Hrozby (detailný popis)
  - Vis major
  - Organizačné nedostatky
  - Ľudské chyby
  - Technické poruchy
  - Zámerná činnosť

Výber bezpečnostných opatrení 3/3

- Bezpečnostné opatrenia
  - Infraštruktúra
  - Organizačné
  - Personálne
  - Hardvér a softvér
  - Komunikácia
  - Plánovanie kontinuity činnosti

- Porovnanie s ISO 27002 a 27005
  - Kompatibilné ale podstatne podrobnejšie (existuje analýza)
  - Metodika sa dá použiť aj pre plánované systémy

Kontrola existujúcej úrovne IB 1/2

- Máme:
  - Prehľad o aktívach
  - Bezpečnostných požiadavkách na ne
  - Porovnanie ochrany so štandardom (ISO 27002 alebo IT-Grundschutz alebo niečo iné) = opatrenia, ktoré by postačovali bezpečnostným požiadavkám

- Potrebujeme zistiť, ktoré opatrenia nepostačujú
  - Neboli implementované alebo boli zle implementované
  - Nevyhovujú súčasným bezpečnostným požiadavkám

- Zdroj: bezpečnostná dokumentácia, zodpovední ľudia (neráta sa zatiaľ s auditom)

Kontrola existujúcej úrovne IB 2/2

- Porovnanie cieľového a aktuálneho stavu (opatrenia)

- Identifikované bezpečnostné opatrenie
  - Nie je potrebné
  - Bolo úplne implementované
  - Bolo implementované len čiastočne
  - Nebolo implementované

- Štandard popisuje aj
  - Organizáciu kontroly
  - Dokumentáciu výsledkov

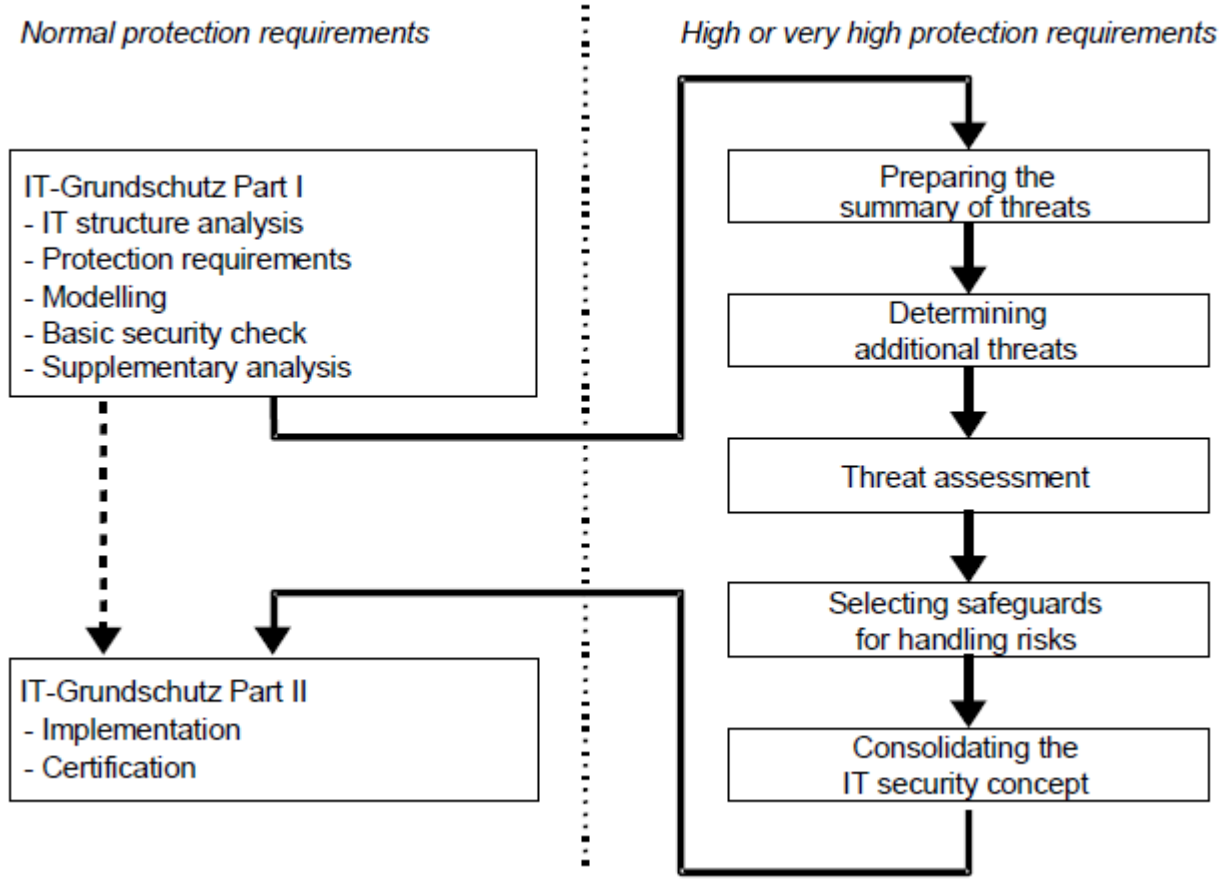
Doplňujúca bezpečnostná analýza 1/2

- Štandardné/existujúce bezpečnostné riešenia nemusia stačiť pre všetky systémy
  - Vyššie bezpečnostné požiadavky
  - Nedajú sa použiť hotové riešenia

- Je potrebná dodatočná analýza rizík

- Metodika BSI Štandard 100-3

Doplňujúca bezpečnostná analýza 2/2



Implementácia bezpečnostných opatrení

- Bezpečnostné opatrenia
  - Ktoré neboli alebo boli zle implementované
  - Zodpovedajúce vyšším požiadavkám
- Zosúladiť s existujúcimi riešeniami IB
- Postup
  - Sumarizácia potrebných opatrení (kvôli celkovému prehľadu, prioritám, zdrojom)
  - Konsolidácia bezpečnostných opatrení (odstránenie duplicít)
  - Odhad potrebných zdrojov (ľudia, financie; jednorazové aj náklady na udržiavanie)
  - Stanovenie poradia implementácie
  - Stanovenie úloh a zodpovedností
  - Podporné opatrenia (oboznamovanie dotknutých osôb)

Udržiavanie zlepšovanie úrovne IB

- Účinnosť a efektívnosť ISMS súčasť bezpečnostnej stratégie

- Základ pre posúdenie ISMS
  - Analýza bezpečnostných incidentov
  - Simulácia bezpečnostných incidentov (napr. penetračné testovanie)
  - Výsledky auditov
  - Certifikácia

- Kontrola IT bezpečnostného procesu na všetkých úrovniach

- Kontrolné mechanizmy
  - Kontrola (implementácie a dodržiavania bezpečnostných opatrení)
  - Monitoring
  - Správy o stave bezpečnosti (pre vedenie)
  - Audit

Záver 1/2

- 2 body: ISMS, štandardizácia IB
- Pre dôležité systémy potrebujeme IB riešiť systematicky, zaviesť ISMS
- ISMS je podrobne špecifikovaný v ISO štandardoch 27001 a 27002
- Až na organizačné zabezpečenie, formalizáciu postupov, dokumentáciu neobsahuje nič k čomu by sa nedalo logicky dospieť
- Hodnota štandardov: ucelená podoba ISMS, opatrenia a závislosti medzi nimi
- Problém: realizácia
- ISO 27003 rozsiahly, ale teoretický
- BSI štandardy:
  - kompatibilné s ISO Štandardami + praktické skúsenosti z implementácie (náklady, využitie existujúcich opatrení)
  - Vysoká metodická úroveň
  - Podporené katalógmi hrozieb a opatrení
  - Ale založené na IT-Grundschutz, ktorá u nás nie je známa

Záver 2/2

- Individuálne riešenie IB je náročné
- Štandardy ako návody nestačia (nedokážeme ich ani preložiť a zaviesť do STN)
- Aj na Slovensku budeme musieť poskytnúť zrozumiteľnú a použiteľnú metodiku (štátnym aj súkromným inštitúciám)
- BSI má asi 1000 zamestnancov a na IT-Grundschutz robí takmer 20 rokov, BSI manuál má 4000 strán, podobne NIST (SP-800, FIPS)
- Nemáme dosť odborníkov na vytvorenie vlastných riešení
- Budeme musieť preberať zahraničné riešenia