

# Úvod do informačnej bezpečnosti

## Bezpečnosť v organizácii

*Daniel Olejár*

# Použité zdroje a autorské práva

- V prednáške bol použitý obrázok a časť tabuľky zraniteľností z normy ISO/IEC 27005
- Prednášku možno používať za podmienok licencie Creative Commons CC-BY-NC

# Terminologická poznámka

- V slovenskej legislative – naprv informačná bezpečnosť
- Po roku 2015 pribudla kybernetická bezpečnosť
- Pojem nie je dobre definovaný (smernica NIS, ktorej implementáciou je zákon o kybernetickej bezpečnosti – CIA informačných systémov a sietí – čiže informačná bezpečnosť kybernetického priestoru)
- Nezáleží na pomenovaní (Rómeo a Júlia), dôležité je, aby spoločnosť, organizácia, osobný počítač dobre fungovali
- Pojem informačná bezpečnosť je lepšie definovaný, budeme ho používať a ako kompromis – kybernetická a informačná bezpečnosť – KIB (tento prístup - aj Zákon o ITVS)

# Prečo potrebujeme riešiť IB v organizácii?

- Legislatívne požiadavky; za ich nespĺnenie hrozia organizácii sankcie (zákon o kybernetickej bezpečnosti, zákon o ITVS, GDPR, zákon o kritickej infraštruktúre, zákon o utajovaných skutočnostiach,...) podrobnejšie v ďalšej prednáške
- Elektronická komunikácia, obchodovanie, požiadavky partnerov, štátnych orgánov
- Obavy z bezpečnostných incidentov alebo skúsenosti organizácie s nimi a snaha vyhnúť sa problémom v budúcnosti

# Kde začať?

- **Scenár:** Absolvent matfyzu sa v organizácii stane manažérom informačnej bezpečnosti (a/alebo osobou zodpovednou za ochranu osobných údajov)
- ak rieši nejaký akútne problém (napr. opatrenia uložené pri kontrole, hroziace závažné bezpečnostné incidenty, zákon), nemá čas na analýzy potrebné na komplexné riešenie v organizácii
  - Okamžité riešenie bezpečnostného incidentu
  - Bezpečnostný projekt pre postihnutý alebo ohrozený systém, alebo časť organizácie
  - Implementácia opatrení
  - Správa vedeniu organizácie a návrh postupu pri riešení IB v organizácii
- Návody a postupy na riešenie akútneho problému – iné prednášky, normy, podpora CSIRT, či iných externých organizácií
- Ale riešenie problémov *ad-hoc* nie je dobrá stratégia

# Systematické riešenie IB v organizácii (1)

- Ľahko sa povie, ťažšie realizuje (a nezáleží to len od vás)
- k čomu smerujeme –
  - Ucelená koncepcia riešenia informačnej bezpečnosti v organizácii (ISMS), ktorá zohľadňuje potreby a možnosti organizácie a implementácia tejto koncepcie
- ISO/IEC normy 27001, 27002, 27005
- V reálnom živote budeme musieť kombinovať oba prístupy
  - systematický
  - s riešením akútnych problémov

# Systematické riešenie IB v organizácii (2)

- Najprv prehľad o organizácii a riešení IB v nej
  - Kto zodpovedal za IB v organizácii (manažér, garant)
  - Ďalšie relevantné osoby (ochrana osobných údajov, utajované skutočnosti, personálne oddelenie, právne oddelenie, správa budov, vedúci IT oddelenia,...)
  - Externí spolupracovníci
  - Aké dokumenty týkajúce sa IB/súvisiace s IB v organizácii existujú (bezpečnostná politika, bezpečnostné štandardy, vnútorné predpisy, bezpečnostné projekty, správy auditu, záznamy kontrol, správy o bezpečnostných incidentoch, zmluvy s dodávateľmi a pod.)
  - Základné dokumenty o organizácii (štatút, organizačný poriadok) – aký je účel organizácie, právna forma, aké zákony upravujú jej činnosť (povinnosti, ale napr. aj dôvody pre spracovanie osobných údajov)
  - Organizačná štruktúra organizácie
  - Geografické rozmiestnenie organizácie (jedna budova, plán, centrum a pobočky na Slovensku,...)
  - Hlavné aktíva organizácie (bez ktorých by nemohla plniť svoje poslanie)
  - Hlavné informačné aktíva (systémy, siete, databázy, aplikácie; kto za ne zodpovedá, na čo sa používajú a kto s nimi pracuje)

# Systematické riešenie IB v organizácii (3)

- Máme základný prehľad o organizácii, chceme postupne prejsť od ad-hoc prístupu k systematickému riešeniu (systém manažmentu informačnej bezpečnosti, v angličtine ISMS)
- Pri poverovaní funkciou bezpečnostného manažéra sa treba dohodnúť na vypracovaní správy o stave IB a návrhu riešenia pre Vedenie organizácie (dokedy, s kým z Vedenia môžete konzultovať)
- Návrh pre vedenie (forma business case) stav IB v organizácii, legislatívne požiadavky a možné sankcie, potreba ochrany informačných aktív organizácie (príklady bezpečnostných incidentov doma, alebo v podobných organizáciách), stručný obsahový návrh, rozpočet, harmonogram riešenia, požiadavky na zloženie pracovnej skupiny
- Požiadavka zaviesť ISMS – zákon o ITVS a bezpečnostné štandardy (vykonávací predpis) k nemu, implicitne GDPR
- <https://www.workfront.com/blog/how-to-write-a-business-case-4-steps-to-a-perfect-business-case-template>



# Politika informačnej bezpečnosti

- Začnime Politikou informačnej bezpečnosti, skrátene Bezpečnostnou politikou
- Obsah BP - normy ISO/IEC 27001 a 27002
- Základný koncepčný dokument IB v organizácii
- Vytvára rámec pre budovanie IB v organizácii
  - Čo organizácia potrebuje chrániť
  - Na akej úrovni
  - Povinnosti jednotlivých ľudí
  - Organizačné zaistenie IB
  - Riešenie bezpečnostných incidentov
  - Kde sa ciele IB rozpracujú podrobnejšie
  - Kontrola plnenia úloh v IB
  - Revízie politiky IB
- Politika IB je určená všetkým zamestnancom aj návštevníkom a externým spolupracovníkom

# Čo dať do Bezpečnostnej politiky?

- Úvod politiky IB (verejný prísľub vedenia organizácie a zdôraznenie významu IB zamestnancom a spolupracovníkom organizácie)
  - Čo je IB
  - Význam IB pre organizáciu
  - Čo organizácia hodlá spraviť pre zaistenie IB
  - Význam politiky IB
  - Deklarácia vedenia organizácie (povinná) v ktorej vedenie
    - (a) deklaruje význam informačnej bezpečnosti pre organizáciu,
    - (b) stotožní sa s cieľmi stanovenými v bezpečnostnej politike,
    - (c) dá prísľub, že bude presadzovať realizáciu bezpečnostnej politiky a vytvárat' na to podmienky.
- Deklarácia vedenia organizácie, aj ako samostatný dokument, Bezpečnostný zámer

# Obsah Bezpečnostnej politiky

- **Pôsobnosť politiky IB** (celá organizácia, nejaká oblasť, systém)
- Aj **hlavné aktíva organizácie**
- **Na koho sa vzťahuje** (domáci zamestnanci a externisti)
- Čo s externistami
  - Nemáme na nich bezprostredný dopad, ale
  - Politika riadenia prístupu a
  - Klasifikačná schéma a pravidlá pre narábanie s klasifikovanými informáciami
- **Špeciálne podsystémy** – potrebujeme vyššiu úroveň IB – vyčlenenie z pôsobnosti „obyčajnej“ politiky IB
- Elektronická, alebo aj papierová forma?
- Jedna politika alebo viac politík – problém s koordináciou, rozsahom bezpečnostnej politiky

# Obsah Bezpečnostnej politiky

- **Roly a povinnosti** (kategorizácia ľudí podľa ich vzťahu k IKT a IB, aby sme sa nemuseli zaoberať každým jednotlivo)
- Politika IB sa týka všetkých ale primerane ich postaveniu. V Politike všeobecná deklarácia a konkretizácia rolí a povinností buď ešte v samotnej politike, alebo v dokumentoch nižšej úrovne
- Aké roly treba rozlišovať a aké povinnosti sú na ne viazané?
- Štandardy definujú príliš veľa rolí, v našich podmienkach na špeciálne bezpečnostné roly nemáme dosť ľudí
- Ale úlohy ostávajú

# Obsah Bezpečnostnej politiky

- prístup k ochrane aktív organizácie, založený na analýze rizík
- V bezpečnostnej politike – aká analýza rizík – kvantitatívna alebo kvalitatívna, hranica akceptovateľného rizika
- Riešenie bezpečnostných incidentov, vrátane disciplinárnych postihov
- Plány kontinuity činnosti
- Audit
- Zodpovednosť za Bezpečnostnú politiku
- Revízie Bezpečnostnej politiky
  - Pravidelné
  - Veľké zmeny
  - Závažné bezpečnostné incidenty

# Ďalší postup

- BP musí schváliť vedenie organizácie a vydať ako záväzný predpis (na UK smernica rektora)
- Zamestnanci sú povinní oboznámiť sa s BP a dodržiavať ju
- Povinnosť stanovená v pracovnej zmluve
- Školenia – ochrana osobných údajov, bezpečnosť pri práci + informačná bezpečnosť
- Aj externisti a dočasní pracovníci
- Rozpracovanie v podobe dokumentácie nižšej úrovne a kontrola dodržiavania

# Bezpečnostné politiky, štandardy, praktiky

- Bezpečnostná politika je všeobecná a dlhodobu platná
- Nemala by sa často meniť
- Nemôže byť príliš konkrétna
- Politiky, resp. dokumenty nižšej úrovne
- Špeciálne bezpečnostné politiky – buď na konkrétny systém alebo oblasť činnosti (bezpečnostné štandardy)
- Bezpečnostné praktiky – 3. stupeň – praktické návody ako postupovať v konkrétnych situáciách

# Špeciálne bezpečnostné politiky

- (a) Politika pre riadenie prístupu
- (b) Politika pre klasifikáciu informácie a narábanie s (klasifikovanou ) informáciou
- (c) Štandardy fyzickej bezpečnosti,
- (d) Štandardy upravujúce činnosť používateľov pri používaní IKT (pravidlá používania IKT); napr.
  - i) pre opustenie pracoviska (čistý stôl a obrazovka),
  - ii) pre sťahovanie softvéru,
  - iii) pre používanie mobilných zariadení (notebook, tablet, mobil,...),
  - iv) obmedzenia na inštaláciu a používanie softvéru a pod.
- (e) Politika pre zálohovanie a obnova systémov zo záloh
- (f) Politika pre prenos a výmenu informácií



# Špeciálne bezpečnostné politiky

- (g) Politika ochrany pred škodlivým softvérom
- (h) Politika pre inštaláciu bezpečnostných záplat (patching)
- (i) Politika pre uchovávanie a archivovanie informácie
- (j) Politika pre používanie kryptografických funkcií
- (k) Politika pre prevádzku počítačových sietí
- (l) Politika pre prácu na diaľku (teleworking)
- (m) Politika ochrany údajov a súkromia,
- (n) Politika pre softvérové licencie,
- (o) Politika pre outsourcing.

# Analýza rizík

- Bezpečnostná politika je len rámcová, potrebujeme ju konkretizovať na jednotlivé systémy/oblasti činnosti organizácie
- Manažment IB v organizácii sa zakladá na **manažmente rizík**
- Začíname analýzou bezpečnosti informačného systému – **analýzou rizík**
- Popisuje norma ISO/IEC 27005 **Information technology – Security techniques – Information security risk management**
- **information security risk** = potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization
- Definícia sa približuje k definícii hrozby, zaujímajú nás hodnota rizika, čo je stredná hodnota dopadu hrozby
- Nasledujúci obrázok je prebratý z normy ISO/IEC 27005 – analýza rizík je len malá časť manažmentu rizík

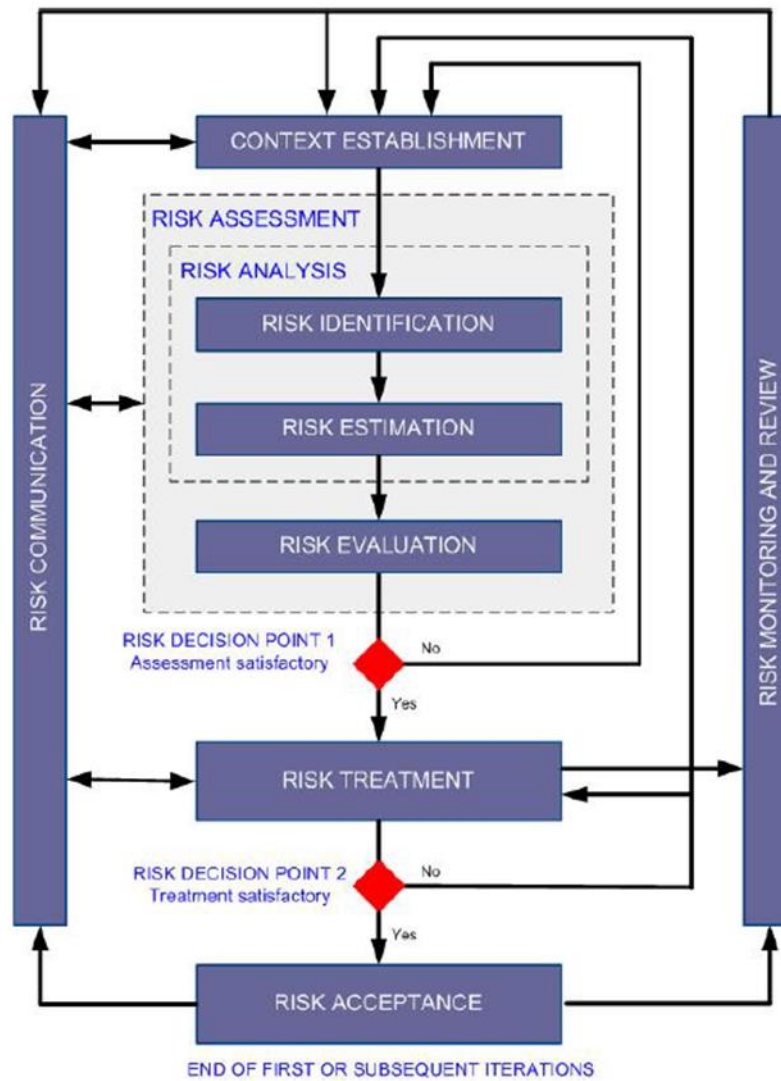


Figure 1 — Information security risk management process

# Popis systému

- Prostriedok na zistenie objektívnych bezpečnostných potrieb systému a stanovenie priorít ich riešenia
- Potrebujeme konkretizovať čo a pred čím máme chrániť a aké reálne sú hrozby
- Popis systému a jeho bezpečnostného okolia (celkový obraz systému a jeho okolia)
  - Slovný popis + podrobnejšie technické špecifikácie do príloh
  - čo to je (systém, sieť, databáza, aplikácia,..)
  - Na čo systém slúži
  - Na čom systém beží (hw, OS, databázový systém, aplikačný sw.)
  - Prepojenie vo vnútri a na iné systémy (obrázok s popisom)
  - Celková topológia siete, miesto systému v nej, pripojenie na externé siete (Internet, Govnet)
  - Kde systém je umiestnený (geografická lokalita, budovy, priestory)

# Popis systému

- Popis systému a jeho bezpečnostného okolia-pokračovanie
  - Kto systém spravuje (systémový administrátor a ďalší privilegovaní používatelia)
  - Prevádzka systému (aj údržba, outsourcing)
  - Vlastník systému
  - Používatelia
  - Roly
  - Správa používateľov
  - Aké údaje sa na systéme spracovávajú (tok údajov)
  - Klasifikácia informácie a systému
  - Bezpečnostné funkcie systému a jeho okolia
  - Iné
- Popis systému umožní zostaviť zoznam aktív systému,
- Pridáme nehmotné aktíva a aktíva organizácie závislé od systému, aktíva usporiadame a ohodnotíme

# Aktíva

- Aktíva (ISO/IEC 27005 aj v ďalšom)
  - Primárne
    - Procesy a aktivity organizácie
    - informácie
  - Sekundárne
    - Hardvér
    - Softvér
    - Personál
    - Budovy a priestory
    - Štruktúra organizácie
    - Podporná infraštruktúra a služby

# Ohodnotenie aktív

Kritériá pre ohodnotenie aktív (aké dopady by malo narušenie dôvernosti, integrity, dostupnosti, autentickosti aktív)

- Prerušenie poskytovania služieb
- Strata dôvery klientov
- Prerušenie interných operácií
- Prerušenie činností tretích strán
- Porušenie zákonných povinností
- Porušenie zmlúv
- Ohrozenie používateľov/personálu
- Útok na súkromie používateľov
- Finančné straty
- Finančné náklady súvisiace s mimoriadnymi situáciami
- Strata aktív, zdrojov
- Strata zákazníkov, dodávateľov

# Ohodnotenie aktív - kritériá

Kritériá pre ohodnotenie aktív (aké dopady by malo narušenie dôvernosti, integrity, dostupnosti, autentickosti aktív)

- Súdne konania a právne postihy
- Strata kompetívnej výhody
- Strata vedúceho technologického postavenia
- Strate efektívnosti/dôvery
- Strata technickej reputácie
- Oslabenie vyjednávacej pozície
- Strata dobrého mena
- Materiálne straty
- Prepúšťanie/výpovede
- Priemyselná kríza (štrajky)
- Vládna kríza



# Ohodnotenie aktív

- Ohodnotenie aktív – kvantitatívne, kvalitatívne
- Kvôli kompatibilite - škálovanie
  - Od 3 do 10 úrovní
  - Tri úrovne: nízka, stredná, vysoká hodnota aktíva
- Pri posudzovaní hodnôt aktív
  - rôzne aspekty
  - Rôzne hodnoty
  - Berieme maximálnu z hodnôt
- Závislosti aktív
- Výsledok = zoznam ohodnotených aktív (+podrobnejšie informácie o každom aktíve)

# Ohodnotenie dopadov

- Narušenie aktíva má nejaký negatívny dôsledok (na aktívum, organizáciu)
- Potrebujeme posúdiť dopady
- Dopady priame a nepriame
- Priame
  - Cena za nahradenie aktíva
  - Náklady na obstaranie a inštaláciu
  - Strata v dôsledku zrušených operácií
  - Dopady narušenia IB
- Nepriame
  - Možné zneužitie prezradených informácií
  - Straty kvôli nutnosti presunúť zdroje na odstránenie narušenia aktíva
  - Porušenie zákonných, zmluvných povinností
  - Porušenie etického kódexu

# Ohodnotenie dopadov

- Prvý odhad dopadov
  - Neuvažuje sa s existenciou nejakých opatrení
  - Dopad je približne rovný hodnote dotknutého aktíva
- Ďalšia iterácia
  - zohľadnenie opatrení, hrozieb, zraniteľností, pravdepodobnosti narušenia
  - Realistickejší (nižší) odhad dopadov

# Hrozby

- Hrozby
  - Existujú rozsiahle katalógy hrozieb (niekoľko tisíc položiek)
  - Vybrať relevantné, netreba ísť do detailov
    - Veľká zložitosť analýzy rizík
    - Analýza rizík sa dá iterovať
    - Problematické veci možno analyzovať podrobnejšie neskôr
- Čo ďalšie potrebujeme zohľadniť
  - Bezpečnostné politiky organizácie, záväzné požiadavky na ochranu informácie a systému
  - Predpoklady o činnosti systému (napr. spoľahliví správcovia, fyzická ochrana)

# Hrozby

- Hrozby
- Len rámcovo (typy)
  - Fyzické poškodenie (požiar, unikajúca voda, prach, korózia, havária)
  - Prírodné udalosti (búrky, záplavy, zemetrasenia,...)
  - Strata podstatných služieb (klimatizácia, napájanie, telekomunikačné služby)
  - Poškodenie radiáciou (tepelnou, elektromagnetickou, emg. pulzmi)
  - Narušenie informácie
  - Technické poruchy
  - Neoprávnené činnosti
  - Kompromitácia funkčnosti
- Špeciálne ľudský faktor
  - Hacker
  - Počítačový zločinec
  - Terorista
  - Priemyselná špionáž
  - sabotáže
  - Vlastný zamestnanec

# Opatrenia a zraniteľnosti

- Existujúce opatrenia
  - Nemusia byť postačujúce, ale
  - Zabraňujú naplneniu niektorých hrozieb
  - Znižujú riziká
  - Bez nich – skreslený obraz
- zraniteľnosti
  - = Nutná podmienka naplnenia hrozby voči aktívu
  - Identifikácia zraniteľností aktív
- zoznam zraniteľností (ISO/IEC 27005)
- Typy
  - Hardvér
  - Softvér
  - Sieť
  - personál

# Zraniteľnosti

- Typy zraniteľností
  - Hardvér
  - Softvér
  - Sieť
  - Personál
  - Sídlo organizácie/systemu
  - Organizácie
- Na ilustráciu podrobnejší zoznam zraniteľností (zdroj ISO/IEC 27005)

# Príklad zraniteľností

Software	No or insufficient software testing	Abuse of rights
	Well-known flaws in the software	Abuse of rights
	No 'logout' when leaving the workstation	Abuse of rights
	Disposal or reuse of storage media without proper erasure	Abuse of rights
	Lack of audit trail	Abuse of rights
	Wrong allocation of access rights	Abuse of rights
	Widely-distributed software	Corruption of data
	Applying application programs to the wrong data in terms of time	Corruption of data
	Complicated user interface	Error in use
	Lack of documentation	Error in use
	Incorrect parameter set up	Error in use
	Incorrect dates	Error in use



# Stanovenie hodnôt rizík

- Risk = potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization (ISO/IEC 27005)
- Hodnota rizika = stredná hodnota dopadu vypočítaná na základe pravdepodobnosti naplnenia hrozby a dopadu
- Metodika pre odhad rizika (kvantitatívna, kvalitatívna) stanovená vopred, napr. v Politike IB
- Stanovíme riziká
  - Možnosti uplatnenia hrozieb voči aktívam (scenáre); zohľadňujeme zraniteľnosti a existujúce opatrenia
  - Priradíme rizikám hodnoty
- Tým je podľa normy ISO/IEC 27005 ukončená analýza rizík

# Vyhodnotenie rizík

- **Hranica akceptovateľného rizika** (býva stanovená v Politike IB) – čo je organizácia schopná/ochotná tolerovať
- Zohľadňujú sa aj
  - Bezpečnostné politiky organizácie, záväzné požiadavky na ochranu informácie a systému
  - Predpoklady o činnosti systému (napr. spoľahliví správcovia, fyzická ochrana)
- Posúdenie odhadnutých rizík vzhľadom na kritérium akceptovateľnosti rizika
- Výsledok = rozdelenie identifikovaných rizík na akceptovateľné a neakceptovateľné
- Rozhodnutie, čo sa bude robiť s príliš vysokými rizikami
  - Vyhnutie
  - Prenesenie
  - Prijatie opatrení

# Výber a implementácia opatrení

- Väčšinu problémov (neakceptovateľných rizík) budeme musieť riešiť
- Kde vziať riešenia?
- Pri analýze rizík: scenáre hrozieb (ktoré zraniteľnosti a ako sa dajú využiť)
- Opatrenia na pokrytie odhalených zraniteľností
  - Návrh (zoznam a plán implementácie)
  - Schválenie vedením organizácie
  - Implementácia

# Výber a implementácia opatrení

- Štandardné opatrenia
  - Systémy sú podobné a majú podobné bezpečnostné požiadavky
  - Experti spravili analýzu rizík pre typické systémy a navrhli štandardné opatrenia
  - Grundschatz nemeckého BSI (katalóg hrozieb, zraniteľností, opatrení)
- Súbory opatrení
  - USA – súbory minimálnych opatrení podľa úrovne klasifikácie systémov
  - ISO/IEC 27002 súbor cca 130 opatrení (povinných)
- Opatrenia je potrebné overiť (predpoklady) a konkretizovať

# Čo ďalej?

- Návrh opatrení a plán implementácie opatrení
- Schválenie vedením organizácie (peniaze, organizačné a legislatívne opatrenia)
- Implementácia opatrení
- Ostali zostatkové riziká
  - Akceptované
  - Zatiaľ nepokryté bezpečnostnými navrhnutými ale nerealizovanými opatreniami
  - Riziká znížené prijatými opatreniami
- Monitorovanie systému
- Vyhodnocovanie účinnosti opatrení
- Dodatočné analýzy rizík
- Bezpečnostné audity

# Ďalšie čítanie

## Normy ISO/IEC

- [ISO/IEC 27000](#) — Information security management systems — Overview and vocabulary
- [ISO/IEC 27001](#) — Information technology - Security Techniques - Information security management systems — Requirements.
- [ISO/IEC 27002](#) — Code of practice for information security controls
- ISO/IEC 27005 — Information security risk management

## BSI štandardy

- [https://www.bsi.bund.de/EN/Publications/BSIStandards/BSIStandards\\_node.html](https://www.bsi.bund.de/EN/Publications/BSIStandards/BSIStandards_node.html)

## NIST SP 800

- <https://csrc.nist.gov/publications/sp800>