2. mednarodna znanstvena konferenca
Znanje in poslovni izzivi globalizacije v letu 2010
Fakulteta za komercialne in poslovne vede,18. - 19. november 2010 Celje, Slovenija

Mateja Škornik
Univerza v Mariboru, Fakulteta za logistiko, Slovenija
mateja.skornik@fl.uni-mb.si

Vladislav Škornik
Fakulteta za komercialne in poslovne vede, Slovenija
slavko.skornik@t-2.net

Proces upravljanja informacijskih tveganj

Povzetek
Proces upravljanja z informacijskimi tveganji je poslovni proces, ki podpira upravljanje odločanja. Omogoča upravljanje lastnih sredstev za izvajanje zaščite premoženja podjetja na razumen in preudaren način. Proces naj nebi bil dolgotrajen – za dosego rezultatov moramo hitro in učinkovito izvršiti analizo in oceno tveganja. Mednarodna organizacija za standardizacijo (ISO) je razvila standard ISO 27005, ki opisuje proces upravljanja s tveganji in njegove aktivnosti, s katerimi zagotavljamo informacijsko varnost v okviru splošnih konceptov, ki jih podaja ISO 27001. Seveda ISO 27005 predstavlja samo enega od pristopov k reševanju problematike ocenjevanja tveganj. Podaja splošna priporočila za analizo in ocenjevanje informacijskih tveganj tako, da ne predpisuje posamezne metode ali orodja, ki bi bilo primerno za uporabo v neki organizaciji. Ena izmed najbolj razširjenih metod za obvladovanje informacijskih tveganj je metoda NIST SP 800-30. Proces je izredno celovit, saj zajema vse – od identifikacije grožnje do sprotnega vrednotenja ter ocenjevanja.

Ključne besede: tveganje, upravljanje IT tveganj, informacijska varnost, ISO/IEC 27005:2008, ISO/IEC 27001:2005, NIST SP 800-30

Information security risk management process

Abstract
IT risk management process is a business process that supports management decision-making. It provides managing company's own resources to implement the asset for business protection in a reasonable and circumspect way. The process should not be time consuming - to achieve results we need to perform analysis and risk assessment quickly and efficiently. International Organization for Standardization (ISO) developed standard ISO 27005 which provides guidelines for information security risk management. It supports the general concepts specified in ISO 27001 and is designed to assist the satisfactory implementation on information security based on a risk management approach. ISO 27005 is one of many approaches of risk assessment. It gives general recommendations for the analysis and assessment of information risk and does not provide specific methods or tools that may be suitable for use in an organization. One of the most common methods to manage information risks is NIST SP 800-30. The process is extremely comprehensive - it covers everything, from threats identification to ongoing evaluation and assessment.

Keywords: risk, IT risk management, information security, ISO/IEC 27005:2008, ISO/IEC 27001:2005, NIST SP 800-30

1 Uvod in ozadje

Upravljanje tveganj pomeni ukvarjati se z negotovostjo. Definicija strokovnega združenja COSO, katerega temeljno poslanstvo je postavljanje standardov na področju upravljanja tveganj, ga opredeljuje kot nenehni proces, ki poteka v podjetju in sestoji iz prepoznavanja negotovosti (tveganj in priložnosti), ocenjevanja tveganj z vidika verjetnosti, pomembnosti in časa njihovega nastajanja ter vrednotenja možnih posledic in s tem povezanega določanja prednosti tveganj (razvrščanje in prednostno obravnavanje tveganj), odločanja o tem kako ravnati s prepoznanimi tveganji, ter njihovega nadzora.

Upravljanje s tveganji je ena pomembnejših disciplin pri načrtovanju in vodenju projektov. V bistvu želimo z ustreznimi metodami in tehnikami določiti strategijo razvoja projekta v prihodnosti ob upoštevanju različnih motilnih dejavnikov.

Za izvedbo učinkovitega sistema upravljanja informacijske varnosti (ISMS) morajo organizacije poskrbeti za sistematično upravljanje informacijskih tveganj, ki mora biti skladno s potrebami, usmeritvami in okoljem v katerem organizacija deluje. Navsezadnje mora biti upravljanje informacijskih tveganj v skladu z upravljanjem vseh tveganj, s katerimi se organizacija srečuje. Varnostne usmeritve se nanašajo na pravočasno in učinkovito upravljanje s tveganji na področjih in v času, kjer in ko je to potrebno. Gre za proces, ki ga je potrebno vzpostaviti in ga po vzpostavitvi stalno izvajati in dopolnjevati.

Tveganje je verjetnost za morebitno škodo, ki lahko nastane zaradi nekaterih trenutnih procesov ali dogodka v prihodnosti. Tveganja so prisotna v vsakem vidiku našega življenja. Z IT varnostnega vidika je upravljanje s tveganji proces razumevanja in odzivanja na dejavnike, ki lahko vodijo do okvare pri zaupnosti, celovitosti oz. razpoložljivosti informacijskega sistema. Informacijsko tveganje je tako verjetnost škode v procesu informacijske pridobitve oz. izgube le-te.

Mednarodna organizacija za standardizacijo je razvila standard ISO/IEC 27005:2008 (ISO 27005). Ta opisuje proces upravljanja s tveganji in njegove aktivnosti, s katerimi zagotavljamo informacijsko varnost v okviru splošnih konceptov, ki jih podaja ISO/IEC 27001:2005 (ISO 27001). Seveda ISO/IEC predstavlja samo enega od pristopov k reševanju problematike ocenjevanja tveganj. Podaja splošna priporočila za analizo in ocenjevanje informacijskih tveganj tako, da ne predpisuje posamezne metode ali orodja, ki bi bilo primerno za uporabo v neki organizaciji. Organizacije morajo same prepoznati metodologijo, ki najbolj ustreza njenemu SUIV (Sistem upravljanja informacijske varnosti) in ugotovljenim zahtevam za varovanje poslovnih informacij ter pravnim in zakonskim zahtevam. Prav tako morajo organizacije same razviti kriterije za sprejem tveganj in določiti sprejemljive ravni tveganj. Izbrana metodologija mora zagotoviti, da bo ocena tveganj dala primerljive rezultate, ki jih bo mogoče v bodočnosti reproducirati.

V članku B. Jereb in M. Škornik je v Dodatku A zbranih 66 orodij, metodologij in pristopov za ocenjevanje in obvladovanje tveganj. Gre za zbir, kjer posamezne rešitve niso medsebojno primerjane ali kakor koli drugače ocenjene. Za ocenjevanje in obvladovanje informacijskih tveganj so razvite naslednje metode in orodja:

- NIST (Razvit s strani *National Institute of Standards and Technology*, ZDA, določa skupne temelje za izkušene in neizkušene, tehnično in netehnično osebje, ki podpira ali upravlja proces upravljanja informacijskih tveganj.);
- OCTAVE;
- FRAP;
- COBRA;
- Risk Watch;
- CRAMM;
- FMEA.

Proces upravljanja tveganj, ki jih predvideva ISO 27005 je mogoče uporabiti pri:

1. celotni organizaciji ali samo v enem od njenih delov (kot je oddelek, fizična lokacija ali celo storitev),
2. kateremkoli informacijskem sistemu in
3. pri obstoječih, planiranih ali pri posameznih vrstah kontrol v organizaciji (na primer pri načrtovanju neprekinjenega poslovanja).

Upravljanje informacijskih tveganj zajema opravila, ki med drugim zajemajo:

1. prepoznavanje tveganj;
2. ocenjevanje tveganj prek vplivov na poslovanje podjetja in morebitne verjetnosti, da se pojavijo;
3. komuniciranje in razumevanje verjetnosti za tveganja in posledice tveganj;
4. vzpostavitev prioritetnega vrstnega reda ukvarjanja s tveganji;
5. vzpostavitev vrstnega reda akcij za zmanjševanje tveganj;
6. vključevanje vseh deležnikov organizacije v odločanje o upravljanju s tveganji in o stalnem informiranju o stanju glede tveganj;
7. učinkovit nadzor in spremljanje tveganj in samega upravljanja tveganj;
8. zajemanje informacij s katerimi lahko upravljanje tveganj izboljšujemo;
9. izobraževanje zaposlenih - še posebej vodij - glede tveganj in načinov za izogibanje tveganjem.

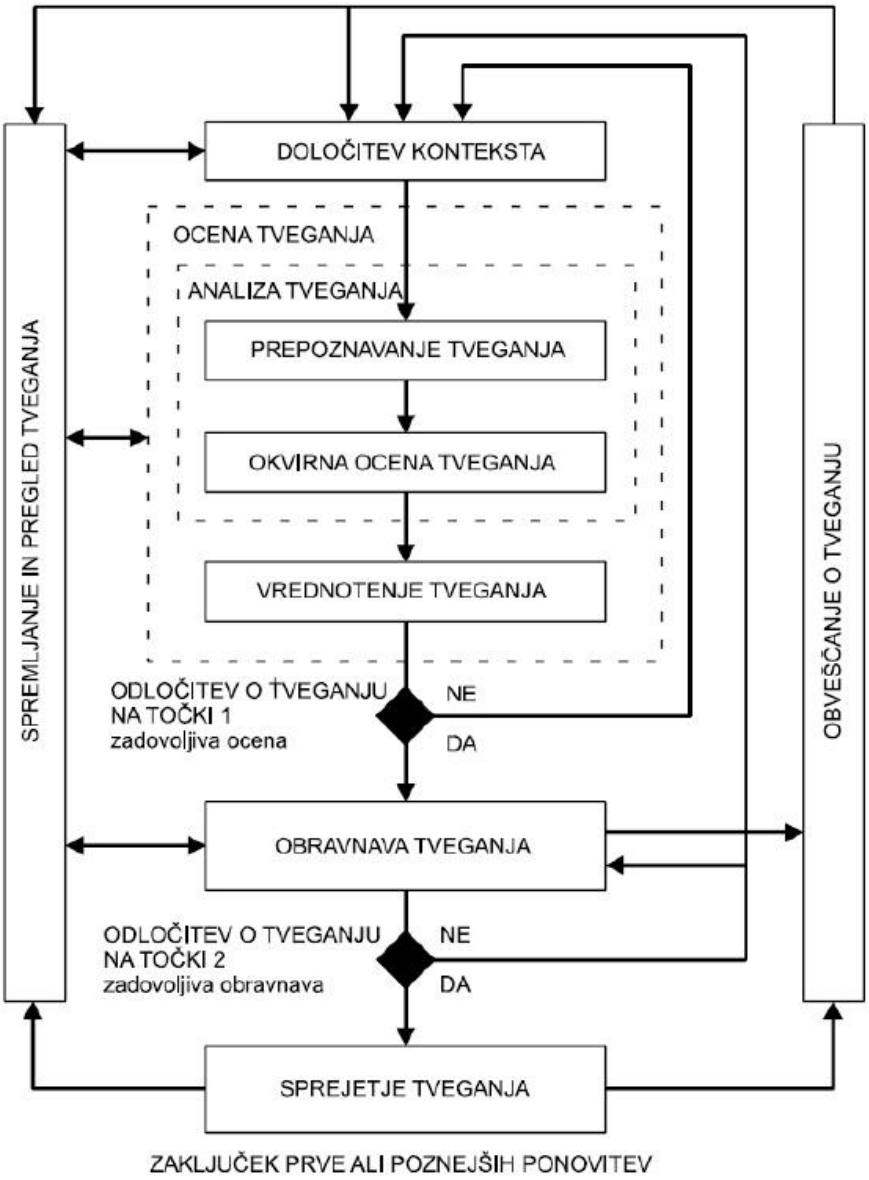
2 Upravljanje informacijskih tveganj po ISO 27005

Upravljanje informacijskih tveganj po ISO 27005 sestavljajo naslednje aktivnosti:

1. Določitev konteksta, v katerem skušamo definirati okvir za upravljanje tveganj.
2. Oceno tveganja, kjer skušamo ovrednotiti nivo tveganja. Ta sklop vsebuje še aktivnosti:
   a) Analizo tveganja, ki se deli na:
      a. prepoznavanje tveganja in
      b. okvirno oceno tveganja.
   b) Vrednotenje tveganja.
3. Obravnava tveganja, kjer je potrebno sprejeti ustrezne ukrepe tako, da se tveganjem izognemo, jih zmanjšamo, prenesemo na druge ali se odločimo, da jih v danem trenutku sprejmemo takšne, kot so.
   Sprejetje tveganja; sprejmemo odločitve za sprejetje ukrepov, povezanih s tveganji, in določimo odgovornost za identifikacijo tveganj z utemeljitvami.
4. Obveščanje o tveganjih, kjer zagotavljamo, da poteka stalna kakovostna izmenjava informacij med vsemi zainteresiranimi javnostmi in upravljalci tveganj o obstoju, naravi, obliki, verjetnosti, resnosti, sprejemljivosti in podobne dejavnike tveganj.

5. Spremljanje in pregled, kjer tveganja in njegove dejavnike spremljamo in pregledujemo, da zaznamo vse spremembe v okviru organizacije ter vzdržujemo celosten pogled v tveganje.

Zgoraj naštete procese in njihove medsebojne odvisnosti prikazuje Slika 1.



Slika 1: Proces pri upravljanju informacijskih tveganj
Vir: ISO 27005:2008

Kot kaže Slika 1, najprej določimo kontekst upravljanja. Temu sledi ocena tveganja. Če ne zberemo dovolj informacij, je potrebno ciklično izvesti aktivnosti določanja konteksta in ocenjevanja tolikokrat, da je zbranih dovolj informacij za obravnavo tveganj. Ciklični pristop omogoča manjše vložke za dosego želenega in potrebnega o stanju tveganj (Slika 1, Odločanje o tveganju na točki 1).

Učinkovitost obravnave tveganja je odvisna od rezultatov ocene tveganja. Možno je, da obravnava tveganja ne bo v prvi iteraciji zagotovila sprejemljive ravni preostalega tveganja. V tem primeru je treba, podobno kot je opisano zgoraj, ciklično ponoviti aktivnosti določanja konteksta in ocenjevanja. Večkrat pa je potrebno samo ponoviti celostno obravnavo tveganj na osnovi danih rezultatov ocene tveganj (Slika 1, Odločanje o tveganju na točki 2).

Pri sprejemanju tveganj moramo zagotoviti, da vodilni v organizaciji izrecno sprejmejo preostala tveganja. To pomeni, da sprejemajo vsa tveganja, ki niso bila predmet obravnave tveganj ali pa smo se pri obravnavi tveganj odločili, da jih v danem trenutku sprejmemo takšna kot so.

Ker ISO 27001 predvideva cikel PDCA (*Plan – Do – Check – Act*) v okviru ISMS, je temu ciklu podvržen tudi ISO 27005. Tabela 2 povzema aktivnosti obvladovanja tveganja pri varovanju informacij.

Proces ISMS	**Aktivnosti pri procesu obvladovanja tveganja pri varovanju informacij**
Načrtuj (*Plan*)	Določitev konteksta Ocena tveganja Razvoj načrta za obravnavo tveganja Sprejetje tveganja
Stori (*Do*)	Vpeljava načrta za obravnavo tveganja
Preveri (*Check*)	Stalno spremljanje in pregledovanje tveganj
Ukrepaj (*Act*)	Vzdrževanje in izboljševanje procesa obvladovanja tveganja pri varovanju informacij

Tabela 1: Prekrivanje ISMS procesov z aktivnostmi procesa obvladovanja informacijskih tveganj

2.1 Določitev konteksta

Pri določanju konteksta zberemo informacije o organizaciji, ki so relevantne za obvladovanje tveganj v okviru informacijske varnosti. Sem spada:

1. Določanje osnovnih meril, potrebnih za varnost pri upravljanju informacijskih tveganj. Izbrati je potrebno ustrezen pristop k obvladovanju tveganja ali ga razviti. Razviti in določiti je potrebno merila za vrednotenje:
    a) tveganja, ki ogroža varnost informacij organizacije;
    b) učinka v smislu stopnje škode ali stroškov za organizacijo, ki jih povzroči informacijski varnostni dogodek;
    c) sprejeta tveganja, ki so pogosto odvisna od politike in ciljev organizacije ter interesov interesnih skupin.
2. Merila za sprejetje tveganja se lahko razlikujejo glede na to, kako dolgo pričakujemo obstoj tveganja. Poleg tega mora organizacija oceniti, ali so na voljo ustrezna sredstva.
   Opredelitev področja uporabe in mej vseh ustreznih sredstev, poslovnih ciljev, poslovnih procesov, strategij, pravnih in regulativnih zahtev, ki veljajo za organizacijo ter vmesnikov. Področje uporabe procesa obvladovanja tveganja pri varovanju informacij mora biti opredeljeno za zagotovitev, da se pri oceni tveganja upoštevajo vsa sredstva. Poleg tega je treba določiti meje, da se lahko obravnavajo tveganja, ki lahko prestopijo meje. Informacije o organizaciji je treba zbrati za določitev okolja, v katerem deluje, in njegove pomembnosti pri procesih obvladovanja tveganja. Poleg tega mora organizacija utemeljiti vsako izključitev s področja uporabe.

3. Organiziranje obvladovanja tveganja, tj. vzpostavitev ustreznega delovanja zaposlenih v organizaciji na področju varnosti pri upravljanju informacijskih tveganj (vloge in odgovornosti). Takšno organiziranje mora odobriti vodstvo organizacije. Bistveno je tudi, da določimo namen obvladovanja tveganja pri varovanju informacij, ker ta vpliva na celoten proces in zlasti na določitev konteksta.

2.2 Prepoznavanje tveganja

Namen prepoznavanje tveganja je, da določimo, kaj lahko povzroči potencialno izgubo ter kako, kje in zakaj lahko ta izguba nastane.
Sama aktivnost določa prepoznavanje sredstev, možnih groženj in šibkih točk, ki obstajajo (ali bi lahko obstajale) ter prepoznavanje že obstoječih kontrol, njihov vpliv na prepoznavanje tveganj in morebitne posledice. Prepoznavanje tveganja tako temelji na naslednjih opravilih:

1. Prepoznavanje sredstev. Prepoznavanje moramo izvesti tako podrobno, da zagotovimo dovolj informacij za oceno tveganja. Stopnja natančnosti vpliva na splošno količino informacij, zbranih med oceno tveganja. Stopnjo je mogoče v nadaljnjih ponovitvah ocene tveganja ponovno določiti kako drugače.
2. Prepoznavanje groženj. Opredeliti moramo splošne nevarnosti oz. grožnje in jih razvrsti po tipu (npr. nedovoljene dejavnosti, materialna škoda in tehnične napake). Upoštevati je potrebno tudi interne izkušnje iz preteklih incidentov ter pretekle ocene nevarnosti. Pri obravnavi groženj moramo upoštevati še vidike okolja in kulture.
3. Prepoznavanje obstoječih kontrol. Znova moramo identificirati in preveriti obstoječe kontrole z namenom zagotavljanja njihovega pravilnega delovanja. Kontrole, katerih vpeljava se načrtuje v skladu z načrti za vpeljavo obravnave tveganja, je treba upoštevati na enak način kot že vpeljane kontrole. Za identifikacijo obstoječih oz. načrtovanih kontrol morajo biti zbrane informacije preverjene še pri osebah, odgovornih za varovanje informacij, in pri uporabnikih, da ugotovimo, katere kontrole so resnično vpeljane za informacijske procese ali informacijske sisteme. Opravimo še izvedbo fizičnih kontrol na mestu samem in pregled rezultatov internih presoj.
4. Prepoznavanje ranljivosti. Prepoznati moramo ranljivosti, ki jih lahko izkoristijo grožnje, da škodujejo sredstvom oz. organizaciji. Sama prisotnost ranljivosti še ne povzroči škode, ker je potrebna grožnja, ki bi jo uresničila.
5. Prepoznavanje posledic. Ta dejavnost določa škodo ali posledice za organizacijo, ki jih lahko povzroči z negativni scenarijem (incident). Negativni scenarij opisuje grožnje, ki jim je organizacija izpostavljena zaradi pomanjkljivosti oz. niza pomanjkljivosti v informacijskem varnostnem sistemu. Učinek negativnega scenarija moramo determinirati ob upoštevanju meril učinka, opredeljenih v aktivnosti določitev konteksta.

2.3 Okvirna ocena tveganja

Ocenjevanje tveganja je aktivnost dodeljevanja vrednosti verjetnostim in posledicam vsakega identificiranega tveganja. Sestavljajo jo naslednja opravila:

1. Izbira metodologije za okvirno oceno tveganja glede na specifičnost zahtev in specifičnost samega tveganja: Tveganja lahko analiziramo različno natančno, odvisno od pomembnosti sredstva, obsega znanih ranljivosti in preteklih incidentov, ki so prizadeli organizacijo. Lahko je – odvisno od okoliščin – kvalitativna ali kvantitativna analiza ali kombinacija obeh. Kvalitativna okvirna ocena uporablja kvalifikacijske atribute za opis resnosti potencialnih posledic (npr. nizko, srednje, visoko) in verjetnost njihovega pojava. Prednost kvalitativne okvirne ocene je v preprostosti razumevanja, medtem ko je slaba lastnost odvisnost od subjektivne izbire ocene. Kvantitativna okvirna ocena uporablja ocenjevalno lestvico z numeričnimi vrednostmi (namesto opisnih ocenjevalnih lestvic) za posledice in verjetnost, pri čemer se uporabljajo podatki iz različnih virov. Kvaliteta analize je

odvisna od pravilnosti in popolnosti numeričnih vrednosti in veljavnosti uporabljenih modelov.

2. Ocena posledic: Oceniti je potrebno vpliv na poslovanje organizacije, ki ga lahko ima možen ali dejanski incident pri varovanju informacij, pri tem je treba upoštevati kršitve varovanja informacij, kot so izguba zaupnosti, celovitosti ali razpoložljivosti sredstev. Vrednost vpliva na poslovanje se lahko izrazi v kvalitativni in kvantitativni obliki, vendar metoda določitve denarne vrednosti navadno zagotovi več informacij za odločanje in s tem olajša učinkovitejši proces odločanja.
3. Ocena verjetnosti incidenta: Oceniti moramo verjetnost uresničitve negativnih scenarijev (scenarijev incidenta). Po določitvi scenarijev incidenta je potrebno oceniti verjetnost pojava posameznega scenarija in vpliva, za kar ponovno uporabimo kvalitativne in kvantitativne ocenjevalne tehnike. Pri tem je potrebno upoštevati, kako pogosto se grožje uresničijo in kako lahko je izkoristiti ranljivost.
4. Raven ocene tveganja: Z okvirno oceno tveganja določimo vrednosti verjetnosti in posledic tveganja (kvantitativne ali kvalitativne vrednosti). Okvirna ocena tveganja temelji na ocenjenih posledicah verjetnosti. Poleg tega se pri tem lahko upoštevajo stroškovne koristi, skrbi interesnih skupin in druge spremenljivke, kot je to primerno za vrednotenje tveganja.

2.4 Vrednotenje tveganja

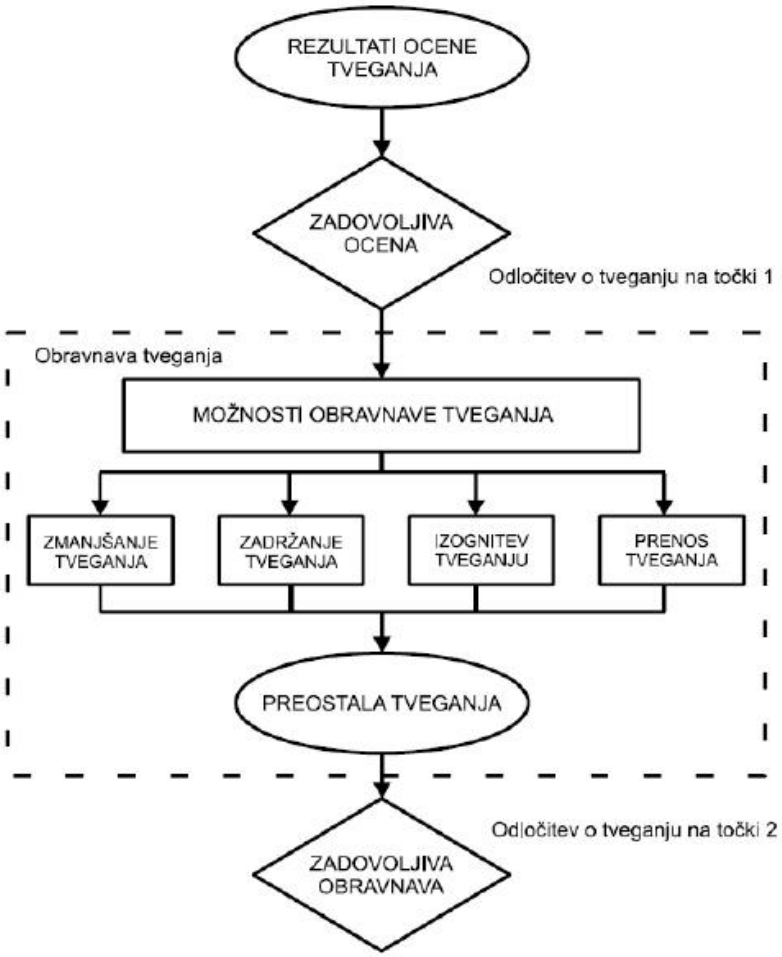
Pri aktivnosti vrednotenje tveganja primerjamo nivo tveganja z merili za oceno tveganja ter merili sprejemljivosti (opredeljenih pri aktivnosti določitev konteksta). Merila za vrednotenje tveganja, ki se uporabijo za sprejemanje odločitev, morajo biti skladna z opredeljenim eksternim in internim kontekstom obvladovanja tveganj pri varovanju informacij. Upoštevamo cilje organizacije, pomen poslovnega procesa oz. z določenimi sredstvi podprte dejavnosti ali niz sredstev, stališča interesnih skupin itn. Odločitve, sprejete med vrednotenjem tveganja, večinoma temeljijo na sprejemljivi ravni tveganja. Vendar moramo upoštevati tudi posledice, verjetnost in stopnjo zaupanja v določitev tveganja in analizo. Združitev več nizkih ali srednjih tveganj lahko povzroči precej višja skupna tveganja, zato jih obravnavamo v skladu s tem spoznanjem.

2.5 Obravnava tveganja

Zagotovimo seznam prednostnih tveganj z negativnimi scenariji glede na merila tveganj določenih v aktivnosti vrednotenje tveganja.
Standard definira 4 načine soočenja s tveganji:

1. Zmanjšanje tveganja: Raven tveganja je treba zmanjšati z izborom kontrol, tako da je preostala tveganja mogoče ponovno oceniti kot sprejemljiva. Izbrati je treba ustrezne in utemeljene kontrole, da se izpolnijo zahteve, ugotovljene med oceno tveganja in obravnavo tveganja. Na splošno lahko kontrole zagotovijo eno ali več naslednjih vrst zaščite: popravilo, odprava, preprečevanje, zmanjšanje vpliva, odvračanje, odkrivanje, obnova, spremljanje in ozaveščanje.
2. Zavestno in objektivno sprejetje tveganja: Odločitev brez nadaljnjih ukrepov mora biti odvisna od vrednotenja tveganja. Povsem mora ustrezati politikam organizacije in kriterijem za sprejem tveganj. Tveganja sprejmemo takšna, kot so.
3. Tveganju se izognemo: Dejavnosti ali pogoju, ki sproža določeno tveganje, se je treba izogniti.
4. Prenos tveganja: Tveganje je treba prenesti na drugo stranko, ki bo najučinkoviteje obvladala določeno tveganje glede na vrednotenje tveganja (npr. na zavarovalnico). Prenos tveganja lahko ustvari nova tveganja ali spremeni obstoječa, prepoznana tveganja.

Slika 2 kaže zgoraj naštete štiri dejavnosti pri obravnavi tveganja.
Možnosti za obravnavo tveganja izberemo na podlagi rezultata ocene tveganja, pričakovanih stroškov za vpeljavo teh možnosti in pričakovanih koristi teh možnosti.



Slika 2: Obravnava tveganja
Vir: ISO 27005:2008

2.6 Sprejetje tveganja

Pri tej aktivnosti se odločimo, da tveganje sprejmemo, določimo odgovornost za to odločitev in jo uradno zabeležimo. Načrti za obravnavo tveganj morajo opisati, kako obravnavamo ocenjena tveganja za izpolnitev meril za sprejetje tveganja. Pomembno je, da odgovorni pregledajo in odobrijo predlagane načrte za obravnavo tveganja in nastala preostala tveganja ter zabeležijo vse pogoje, ki so povezani s takšno odobritvijo.

2.7 Obveščanje o tveganju

Obveščanje o tveganju je dejavnost za sklenitev sporazuma o tem, kako obvladovati tveganja. Slednje storimo z izmenjavo in/ali delitvijo informacij o tveganju med osebami, ki sprejemajo odločitve, in drugimi interesnimi skupinami. Takšne informacije vključujejo obstoj, naravo, obliko, verjetnost, resnost, obravnavo, sprejemljivost tveganj in ostalo.
Oseba, ki sprejema odločitve, in zainteresirane javnosti, si morajo izmenjavati informacije o tveganju. Uspešna komunikacija med zainteresiranimi stranmi je pomembna, ker lahko odločilno vpliva na odločitve, ki jih je treba sprejeti. Sporočanje bo zagotovilo, da osebe, odgovorne za vpeljavo obvladovanja tveganja, in osebe, zainteresirane zanj, razumejo podlago, na kateri sprejemamo odločitve in določene ukrepe. Komunikacija mora biti dvosmerna.

2.8 Nadzor in ocenjevanje tveganja

Ocena tveganja določa vrednost informacijskih sredstev, prepoznava obstoječe grožnje in ranljivosti (ali tiste, ki bi lahko obstajale), prepoznava obstoječe kontrole in njihov vpliv na obstoječa tveganja, določa možne posledice in prednostni vrstni red ugotovljenih tveganj in jih razporedi v skladu z merili za vrednotenje tveganja, opredeljenimi pri določitvi konteksta.
Stalno spremljanje in pregledovanje sta nujna koraka, s katerima zagotovimo, da kontekst, rezultat ocene tveganja, obravnava tveganja in načrti za obvladovanje ostanejo ustrezni glede na okoliščine.
Organizacija se mora prepričati, da proces obvladovanja tveganj pri varovanju informacij in z njim povezane dejavnosti ostanejo ustrezne glede na obstoječe okoliščine in se upoštevajo. Vsako dogovorjeno izboljšavo procesa ali ukrepov, ki je potrebna za izboljšanje skladnosti s procesom, moramo sporočiti vodstvu, da bi zagotovili, da nobenega tveganja ali elementa tveganja ne spregledamo ali podcenimo, da ustrezno ukrepamo, tveganje razumemo in smo se sposobni nanj odzvati.
Poleg tega mora organizacija redno preverjati, da so ukrepi, ki se uporabljajo za merjenje tveganja in njegovih elementov, še vedno veljavni in v skladu s poslovnimi cilji, strategijami in politikami ter da se med obvladovanjem tveganja pri varovanju informacij ustrezno upoštevajo spremembe poslovnega okolja.

2 Metoda NIST SP 800-30

Prva in najpomembnejša funkcija ocenjevanja in obvladovanja informacijskih tveganj je identifikacija tveganj. S pomočjo različnih metod in tehnik kot so planiranje scenarijev, viharjenja možganov, napovedovanje dogodkov s pomočjo časovnih serij, napovedovanje gibanj procesa in kritičnih mej, skušamo predpostaviti možna tveganja in njihove učinke na proces. Ta funkcija je močno odvisna od poznavanja tematike, t.j. znanja o procesu, njegovem okolju in medsebojnih vplivih med procesom in okoljem. Vsako grožnjo procesa skušamo predvideti, oceniti verjetnost pojavitve, njen vpliv na proces, časovne okvire pojavitve grožnje in nato vse grožnje urediti po stopnji kritičnosti. V nadaljevanju skušamo definirati strategije in scenarije možnih odgovorov na te grožnje. Z odgovori skušamo minimizirati vplive grožnje na proces oz. predvideti kakšna bo škoda v primeru neuspeha.

Metoda NIST narekuje devet korakov:

- korak 1: Karakterizacija sistema (*System Characterization*),
- korak 2: Identifikacija groženj (*Threat Identification*),
- korak 3: Identifikacija ranljivosti (*Vulnerability Identification*),
- korak 4: Analiza kontrole (*Control Analysis*),
- korak 5: Ocena verjetnosti (*Likelihood Determination*),
- korak 6: Analiza vpliva (*Impact Analysis*),
- korak 7: Določitev tveganja (*Risk Determination*),
- korak 8: Priporočila kontrole (*Control Recommendations*),
- korak 9: Dokumentiranje rezultatov (*Results Documentation*).

Koraki 2, 3, 4, in 6 se lahko izvajajo vzporedno po uspešno zaključenem koraku 1.

3.1 Karakterizacija sistema

Prvi korak pri ocenjevanju informacijskih tveganj je opredelitev obsega. V tem koraku določimo meje informacijskega sistema, vključno z viri in informacijami, ki predstavljajo sam

sistem. Določimo obseg ocene tveganja, zasnujemo učinkovite avtorizacijske meje podajanja informacij (tako programskih in strojnih, kot tudi informacije o sistemskih povezljivostih, ter o odgovornem podpornem osebju), ki so bistvenega pomena za opredelitev tveganja.

3.2 Identifikacija groženj

Pri prepoznavanju groženj je potrebno oceniti vire groženj, potencialne šibke točke ter obstoječe kontrole. Cilj tega koraka je identifikacija morebitnih virov groženj ter opredelitev potencialno nevarnih virov za vrednoten informacijski sistem.

3.3 Identifikacija ranljivosti

Analiza groženj informacijskega sistema mora vključevati analizo ranljivosti povezano s sistemom okolja. Cilj tega koraka je sestaviti seznam pomanjkljivosti sistema (šibkosti in pomanjkljivosti), ki bi jih viri groženj lahko izkoristili.

3.4 Analiza kontrole

Cilj tega koraka je analizirati kontrole, ki so bile izvedene oz. so načrtovane za izvajanje s strani organizacije, za zmanjšanje oz. odpravo verjetnosti uresničenja grožnje iz sistema ranljivosti. Za izpeljavo splošne ocene verjetnosti (korak 5), ki kaže potencialne ranljivosti je pri izvajanju že implementiranih oz. načrtovanih kontrol potrebno upoštevati še grožnje okolja.

3.5 Ocena verjetnosti

Ocenitev verjetnosti potencialne ranljivosti z upoštevanjem sledečih dejavnikov:

- motivacijo in zmožnost vira grožnje,
- naravno ranljivost,
- obstoj in učinkovitost sedanjih kontrol.

3.6 Analiza vpliva

Pomemben korak pri merjenju ravni tveganja – določitev škodljivih vplivov, ki izhajajo iz uspešno izvedenega koraka 2 (Identifikacija groženj) in 3 (Identifikacija ranljivosti). Pred začetkom izvajana tega koraka je potrebno pridobiti naslednje informacije:

- misija sistema (npr. procesi, ki se izvajajo s strani informacijskega sistema),
- kritičnost podatkov in sistema (npr. vrednost in pomembnost sistema za organizacijo),
- občutljivost sistema in podatkov.

3.7 Ocena tveganja

Namen tega koraka je oceniti stopnjo tveganja informacijskega sistema. Za merjenje groženj je potrebno determinirati lestvico obsega groženj in matriko ravni tveganja.

3.8 Priporočila kontrole

Zagotovijo se kontrole (primerne za poslovanje organizacije) za zmanjšanje in odpravo ugotovljenih tveganj. Cilj priporočitve kontrol je zmanjšati stopnjo tveganja informacijskega sistema in njegovih podatkov na sprejemljivo raven. Pri podajanju priporočil ali alternativnih rešitev za zmanjšanje ali celo odpravo tveganj je pametno upoštevati naslednje dejavnike:

- učinkovitost priporočljivih možnosti (npr. sistemska združljivost),
- zakonodajo in uredbo,
- politiko organizacij,
- operativni vpliv,
- varnost in zanesljivost.

Regulativna priporočila so rezultat procesa ocenjevanja tveganja in zagotavljajo prispevek k dodatku procesa zmanjševanja tveganja, pri katerem so priporočene proceduralne ter tehnične varnostne kontrole ocenjene, prioritizirane in izvedene. V zakup je potrebno vzeti, da vseh podanih kontrol ni vedno možno implementirati v proces.

3.9 Dokumentiranje rezultatov

Po zaključeni oceni tveganja (identifikaciji virov groženj, ugotovljenih šibkih točkah, ocenitvi tveganj in priporočitvi predvidenih kontrol) se morajo rezultati dokumentirati v uradno poročilo.

4 Zaključek

Uspešno in učinkovito upravljanje s tveganji je osnova za uspešno in učinkovito IT varnosti. Zaradi omejenih sredstev in skoraj neomejenega števila realnih groženj mora biti odločitev v zvezi z dodelitvijo sredstev za zaščito informacijskih sistemov sprejeta razumno in preudarno (ter sorazmerno s samo vrednostjo sistema). Za maksimalno učinkovitost obvladovanj tveganj, je treba tveganja dosledno in ponovljivo ocenjevati ter se osredotočati na njihovo zmanjševanje.

Tveganjem se tako v poslovnem življenju ne moremo v celoti izogniti. Sodobno tržno gospodarstvo in neusmiljena konkurenca pa od podjetij zahtevata, da tveganja prepoznavajo, proučujejo njihovo pomembnost in oblikujejo temelje za določanje ravnanja z njimi. Vodstvo se lahko različno odzove za tveganja, ki pretijo podjetju:

- lahko se jim izogne in se torej ne loti dejavnosti, ki določeno tveganje prinaša,
- lahko jih porazdeli (se zavaruje),
- lahko jih sprejme, ker ne presegajo sprejemljive ravni,
- lahko pa jih obvladuje.

Samo pri obvladovanju tveganj se srečujemo z notranjimi kontrolami. To so usmeritve in postopki, ki jih podjetje vzpostavi, in izvaja na vseh ravneh, da bi obvladovalo tveganja.
Standard ISO 27005 ne določa ali kako drugače predlaga metodo za načrtovanje in izvajanje načrta obvladovanja tveganj. To je dobrodošlo in skladno z usmeritvami za pisanje tovrstnih standardov. Odprt je za poljubne metode ocenjevanja tveganj in razlikuje med t.i. kvalitativnimi in kvantitativnimi metodami za diagnosticiranje tveganj. Obenem je razvidno, da pojem tveganja v standardu ni definiran. Čutiti je, da se izogiba srčiki problematike – diagnosticiranju tveganj. Uporabniku dopušča da sam izbere metode diagnosticiranja (in upravljanja) tveganj. Osnovna problematika upravljanja tveganj (to je njihovo diagnosticiranje) tako praktično v celoti ostaja nedorečena.

Ugotovimo lahko, da standard ISO 27005, predvsem v dodatkih, sicer govori o tem, da moramo definirati premoženje, ki je izpostavljeno tveganju, potencialne grožnje in njihove izvore, potencialne ranljivosti in posledice ali vplive, vendar je pojem tveganja definiran šele na 23. strani v poglavju, ki govori o ocenjevanju tveganj z naslednjo definicijo: 'Tveganje je kombinacija posledic, ki lahko sledijo pojavu neželenega dogodka, in verjetnosti pojava dogodka.' Gre za pičlo definicijo, ki ne odraža realnosti.

NIST SP 800-30 pojem ‘tveganje’ definira na 28. strani: ‘Tveganje je funkcija verjetnosti vira grožnje, ki kaže na možne ranljivosti in škodljive vplive na organizacijo.’

Seven J. Ross [6] meni, da ‘tveganje’ sploh ni definirano (ne glede na standard ISO 27005), temveč je definirana le izpostavljenost, ki je predstavljena kot izguba, ki se da predvideti v neki posamezni situaciji.

Dr. Borut Jereb [7] predlaga definicijo pojma ‘tveganje’. Tveganje opiše kot izpostavljenost negotovosti in poudari, da moramo pri izračunavanju tveganj nujno vključiti javnost kot definiran parameter.

Ostaja odprto vprašanje: 'Je možno natančno obravnavati problematiko, katere osnovni pojmi niso jasno definirani?'

Literatura

➡ STONEBURNER, Gary, GOGUEN, Alice, FERINGA, Alexis. 2002. NIST SP 800-30: Risk Management Guide for Information Technology Sytems. [Online]. Virginia. Dostopno na spletnem naslovu: http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf.

➡ JEREB, Borut, ŠKORNIK, Mateja. 2009. Upravljanje informacijskih tveganj po ISO/IEC 27005:2008. V: 17. Mednarodna konferenca o revidiranju in kontroli informacijskih sistemov. [Zbornik referatov].

➡ ISO/IEC 27005:2008, Information Technology – Security techniques – Information security risk management. [Standard.] 2008. International organization for Standardization. [Online.] Dostopno na spletnem naslovu: http://www.iso27001security.com/html/27005.html.

➡ PLEITER; Thomas R. 2010. Information Security Risk Analysis. 3. izd. New York: CRC Press. ISBN 978-1-4398-3956-0.

➡ ŠKORNIK, Mateja. 2010. Upravljanje informacijskih tveganj po NIST SP 800-30. V: Dnevi slovenske informatike 2010. [Zbornik referatov.]

➡ ROSS, Seven J. 2009. Gang Aft Agley. Vol 3. ISACA Journal.

➡ JEREB, Borut. 2009. Kaj so tveganja?. 17. mednarodna konferenca o revidiranju in kontroli informacijskih sistemov. [Zbornik referatov.]