

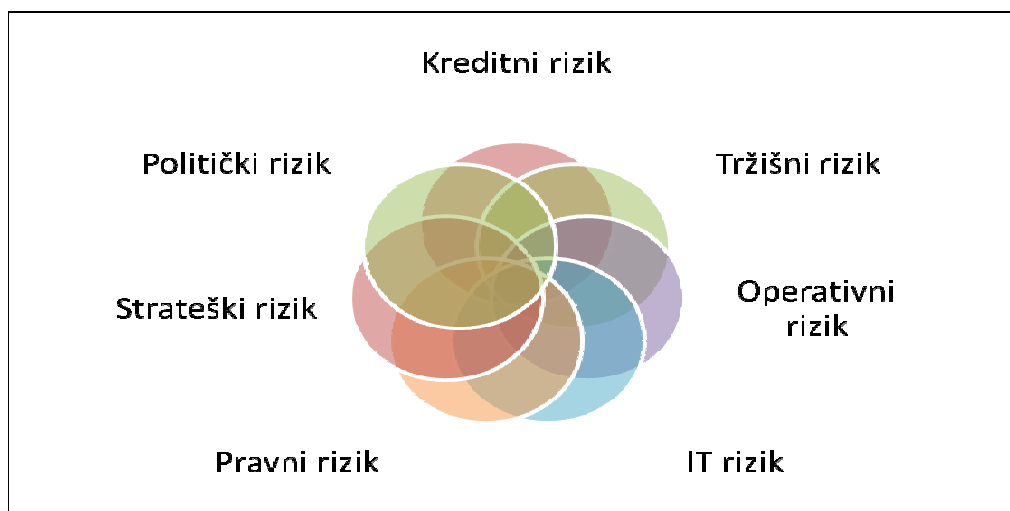
UPRAVLJANJE RIZICIMA – InfoTrend; Dalibor Uremović, KING ICT

Upravljanje rizicima nije nova stvar. Čak štoviše, mogli bi reći da je čovjek kao svjesno biće od prapovijesnih vremena upravljao rizicima. Zamislite primjerice rimskog vojskovođu Gaja Julija Cezara kako stoji na obalama rijeke Rubikon. Prelazak rijeke i napredovanje prema Rimu sa samo jednom legijom predstavlja velik rizik od mogućeg poraza. Ipak, Cezar prihvaća rizik, prelazi rijeku i govori legendarnu rečenicu *Alea iacta est!* („Kocka je bačena!“). Ostalo je povijest...

Naravno, ovdje nema ni govora o formalnim metodama upravljanja rizicima, koje se zapravo počinju pojavljivati u drugoj polovici prošlog stoljeća i to prvenstveno uz poslovne procese vezane uz financije i police osiguranja. Sredinom 80-tih godina prošlog stoljeća, velike kompanije koriste formalne metode upravljanja političkim i nacionalnim rizicima. Ovo dovodi i do postepenog formiranja organizacijskih jedinica zaduženih isključivo za rizike, a danas već imamo i zakonsku obvezu te razne regulative koje organizacijama ne ostavljaju mnogo prostora nego se uhvatiti u koštac s ovom problematikom.

IT rizici

Upravljanje rizicima se može generički definirati kao identifikacija, procjena i prioritizacija rizika nakon kojih slijedi koordinirana i ekonomična uporaba resursa kako bi se smanjila, nadzirala i bolje kontrolirala vjerojatnost i/ili utjecaj neželjenih događaja. Ono što stvara pomutnju pri razumijevanju i primjeni ove definicije u praksi je kontekst u kojem se upravljanje rizicima promatra, a u tom smislu pogleda na upravljanje rizicima ima pravo mnoštvo (vidi sliku 1).



Slika 1 – Neki od pogleda na rizike

U ovom članku ću se zadržati u okvirima IT rizika, iako se većina stvari o kojoj će biti riječi može preslikati i na ostale vrste rizika. IT rizici su ustvari rizici na poslovanje koji proizlaze iz korištenja informacijske i komunikacijske tehnologije. Primjeri takvih rizika su zastoji u radu aplikacija, gubitak administratorskih zaporki ili ključeva, neovlašteni pristup povjerljivim informacijama i sl.

Kako upravljati IT rizicima?

Danas u svijetu postoje mnoge metodologije ili okviri (vidi tablicu 1), koje daju smjernice ili konkretne upute za uporabu najboljih praksi za procese upravljanja rizicima. Neke od njih odnose se isključivo na IT rizike, neke govore o rizicima informacijske sigurnosti, a neke od njih možemo primijeniti u bilo kojem kontekstu upravljanja rizicima. Svima je zajedničko to da se upravljanje rizicima grubo može podijeliti u dvije glavne faze:

- procjena rizika,
- obrada rizika.

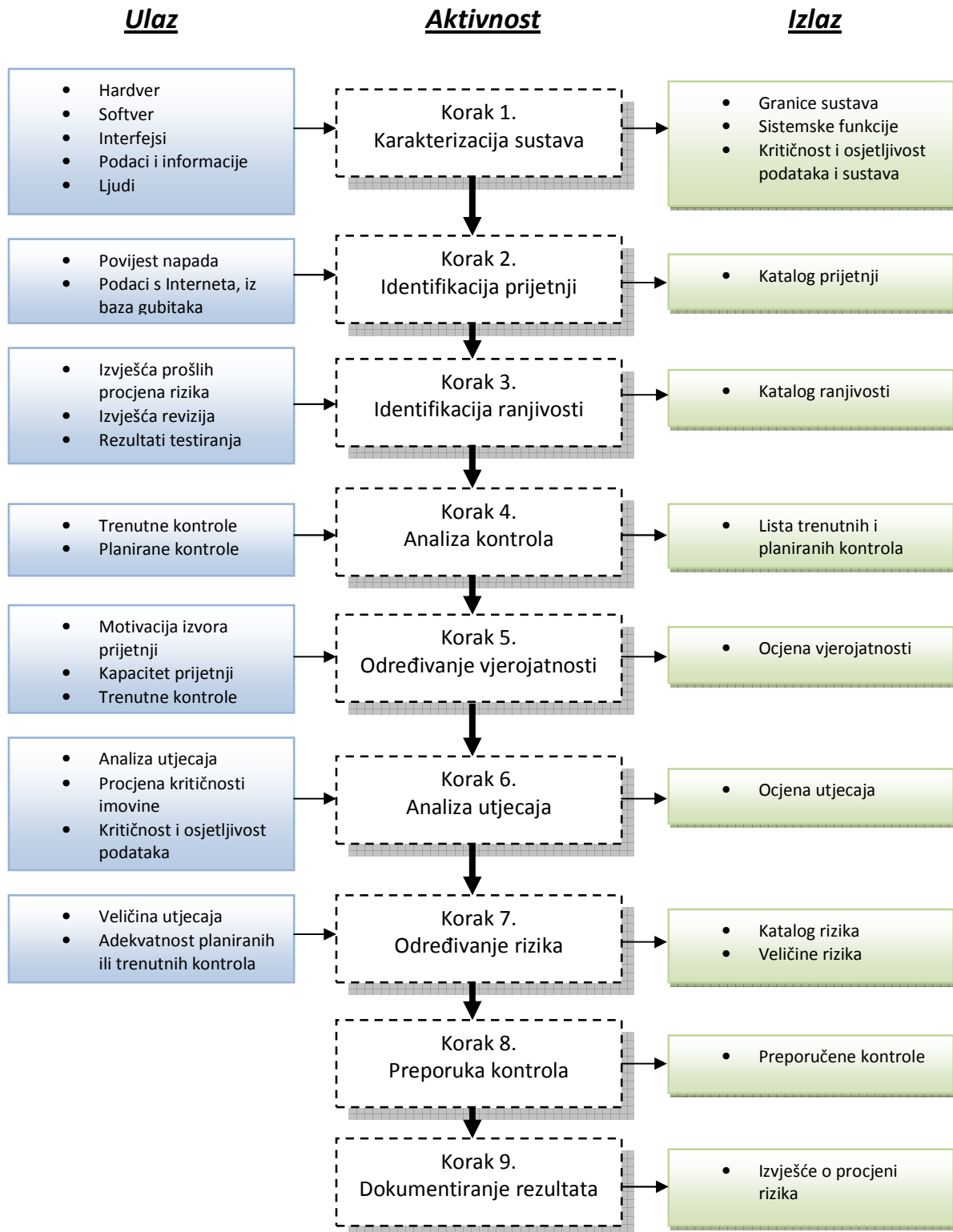
	Zemlja porijekla	Cijena	Primjenjivost na vrstu organizacije	Mogućnost certificiranja
CRAMM	Velika Britanija	N/A	velike	Ne
BS 7799-3:2006	Velika Britanija	cca 80 £	sve	U sklopu ISO 27001
ISO/IEC 27005:2008	Velika Britanija	cca 90 £	sve	U sklopu ISO 27001
IT-Grundschutz	Njemačka	besplatno	sve	Ne
Mehari 2007	Francuska	besplatno	sve	Ne
Octave	SAD	besplatno	srednje i male	Ne
SP800-30 (NIST)	SAD	besplatno	sve	Ne

Tablica 1 - Neke od metodologija ili okvira za upravljanje rizicima

Za dio ovih metodologija postoji već mnoštvo raznih softverskih alata, koji bitno ubrzavaju postupke upravljanja rizicima, osiguravajući sveobuhvatnost pri identificiranju prijetnji i ranjivosti, omogućavajući brže i lakše matematičke izračune veličina rizika i dajući razne vrste izvještaja za visoki menadžment ili osobe odgovorne za procese upravljanja rizicima. Ono što je sigurno je da nijedan od tih alata ne radi svoj posao samostalno (princip „ključ u ruke i vozi“), već je često potrebno provesti određene prilagodbe samoj organizaciji, njenim poslovnim procesima, željama menadžmenta ili raznim regulatornim i zakonskim uvjetima specifičnim za pojedinu poslovnu vertikalnu ili državu u kojoj organizacija djeluje. Jedna od metodologija predstavljena je i kao regulatorna obveza Hrvatske narodne banke prema bankama koje posluju na tržištu Republike Hrvatske, a objavljena je u sklopu „Smjernica za primjereno upravljanje informacijskim sustavom u cilju smanjenja operativnog rizika“. Osnova metodologije je u američkom NIST standardu SP800-30.

Procjena rizika

Rekli smo da su, ugrubo, dvije grupe aktivnosti procjena rizika i obrada rizika. Ukoliko se ove grupe aktivnosti detaljnije razlože, proces procjene rizika je uglavnom slijedeći:



Slika 2 - Koraci procjene rizika (prema NIST-u)

Ostale metodologije imaju ponešto drugačije faze, ali se manje-više svode na isto.

Prvi korak je definirati sustav nad kojim će se promatrati rizici. Mnoge metodologije govore o registru informacijske imovine (eng. asset register) koji nije samo registar osobnih računala, poslužitelja i aplikacijskog softvera. Informacijska imovina je sve ono što predstavlja vrijednost za organizaciju, a sadrži ili jest informacija odnosno se koristi u procesima podrške uslugama koje počivaju na tim informacijama. U registru informacijske imovine će se tako naći poslovni procesi, računalne i komunikacijske usluge, aplikacijski i sistemski softver, računalna i komunikacijska oprema, mediji, izvori napajanja, klima uređaji, vanjski partneri, djelatnici organizacije i sl. NIST-ova metodologija navodi pojam „karakterizacija sustava“ (eng. system characterization) što se čini boljim pojmom za one organizacije koje se po prvi put susreću s procesom upravljanja rizikom. Naime, registar imovine često zna navesti na pogrešan korak sastavljanja neke vrste kataloga sve moguće informacijske i komunikacijske tehnologije, što zna biti dugotrajan posao, a neopipljiva imovina, poput procesa ili usluga se pri tom zaboravlja. Jedan takav registar više je plod upravljanja imovinom (eng. asset management) kao zasebnom disciplinom, iako nije zgoroga objediniti te dvije discipline oko te iste zajedničke točke.

Kad nam je poznat opseg sustava te informacijska imovina koja se nalazi u tom sustavu, potrebno je identificirati prijetnje koje mogu djelovati na tu imovinu te ranjivosti imovine koju takve prijetnje mogu iskoristiti. Slijedeća slika daje popis dijela prijetnji i ranjivosti na informacijsku imovinu.

Tip imovine	Ranjivost	Prijetnja
Hardver	Neredovito održavanje	Tehnički kvar na sustavu
	Nezaključani ormarići	Krađa medija i dokumenata
	Nekontrolirano odbacivanje medija	Krađa medija i dokumenata
Softver	Nedovoljno testiranje softvera	Greška u aplikaciji
	Poznate ranjivosti u softveru	Iskorištavanje poznatih ranjivosti
	Nedostatak operativnih i sistemskih zapisa	Neovlaštene promjene u sustavu
Mreža	Slabo upravljanje zaporkama	Napadi probijanjem zaporki
	Nekriptirani promet	Prisluškivanje prometa
	Neredundantna oprema	Kvar na mrežnom uređaju
Ljudi	Nedovoljna obučanost djelatnika	Greške pri korištenju

	Manjak obučenog kadra	Otkaz djelatnika
Lokacija	Blizina rijeke	Poplava
	Nedostatak agregata i/ili UPS-ova	Nestanak struje

Tablica 2 - Primjeri prijetnji i ranjivosti

Česta greška koje organizacije prilikom identifikacije prijetnji i ranjivosti čine je preslabo definiranje načina na koji će se one identificirati. Naime, pogrešno bi bilo uzeti samo gotove kataloge prijetnji i ranjivosti, primjerice s Interneta, iz raznih metodologija (poput IT-Grundschutz-a) ili ugrađenih u alate koji su dostupni na tržištu. Upravljanje rizicima je živi proces, a rizici se pojavljuju i nestaju svakodnevno. Ovu aktivnost potrebno je ugraditi u svakodnevni operativni posao organizacije, a izvori se mogu pronaći u bazama postojećih incidenata, rezultatima provjere ranjivosti i penetracijskih testiranja, projektnim rizicima, rezultatima testiranja softvera, postojećim bazama prijetnji i ranjivosti na Internetu i sl. Sve to je potrebno neprekidno unositi u kataloge prijetnji i ranjivosti te ga ažurirati jer mnoge prijetnje su najopasnije upravo u početnom razdoblju kad za njih još nisu razvijene kontrole obrane, poput servisnih zakrpa i slično.

Procjena i izračun rizika obavlja se kada definiramo koje prijetnje mogu djelovati na ranjivosti imovine, prikupimo podatke o već implementiranim sigurnosnim kontrolama te se koristimo nekim od mogućih načina vrednovanja ovih parametara. Među pravim morem načina procjenjivanja i izračuna rizika, danas su najpopularnija slijedeća dva:

a) Rizik = Imovina * Prijetnja * Ranjivost

pri čemu se parametrima Imovina, Prijetnja i Ranjivost dodjeljuju vrijednosti iz predefinirane, najčešće kvalitativne, skale. Znak množenja se formalno koristi u slučaju kvantitativne skale, u suprotnom se koristi matrica (vidi sliku 4, pod a).

b) Rizik = Vjerojatnost ostvarivanja prijetnje * Utjecaj na imovinu

I u ovom slučaju radi se o množenju odnosno matrici, a skala je i ovdje najčešće izražena kvalitativno (vidi sliku 4, pod b). Najbolje je ovo ocrtati primjerom iz prakse. Recimo da procjenjujemo vjerojatnosti ostvarivanja prijetnje poplave u server sobi u kojoj nam se nalaze svi bitni poslužitelji. Ukoliko su nam ranjivosti zastarjeli i neodržavani klima uređaji, stare i loše vodovodne cijevi u wc-u iznad server sobe te smještaj zgrade pored neke od naših rijeka, možemo reći da je vjerojatnost ostvarivanja prijetnje „umjereno velika“. Ukoliko nemamo dobro riješenu pričuvnu pohranu podataka, u slučaju ostvarivanja prijetnje utjecaj poplave u server sobi bit će „vrlo velik“. Moguće je ostati bez većeg dijela opreme te bez ključnih podataka o kojima ovisi poslovanje cijele organizacije. Prema tome, procijenjeni utjecaj je vrlo velik. Korištenjem b) načina izračuna rizika, izračunati rizik je u ovom slučaju „vrlo visok (60)“.

Ovaj postupak se ponavlja za sve „primjenjive“ parove imovina, prijetnja i ranjivost i time dobijemo popis rizika i njihovih veličina. Riječ „primjenjive“ može značiti više stvari. Primjerice, nećemo procjenjivati vjerojatnost prijetnje greška u kodu softvera na imovinu zgrade ili uredskih prostora

organizacije. Također je uputno grupirati pojedinu imovinu ukoliko ima slična svojstva te nad njom provoditi zajedničku procjenu rizika (npr. nećemo pojedinačno procjenjivati prijetnju kvara nad radnim stanicama djelatnika, pogotovu ukoliko su sve radne stanice istog proizvođača i jednake starosti).

Zapravo, može se reći da svaka metodologija ima svoje prednosti i mane i rješava neke od problema s kojima se susreću procjenitelji rizika pri primjeni neke od njih „na terenu“.

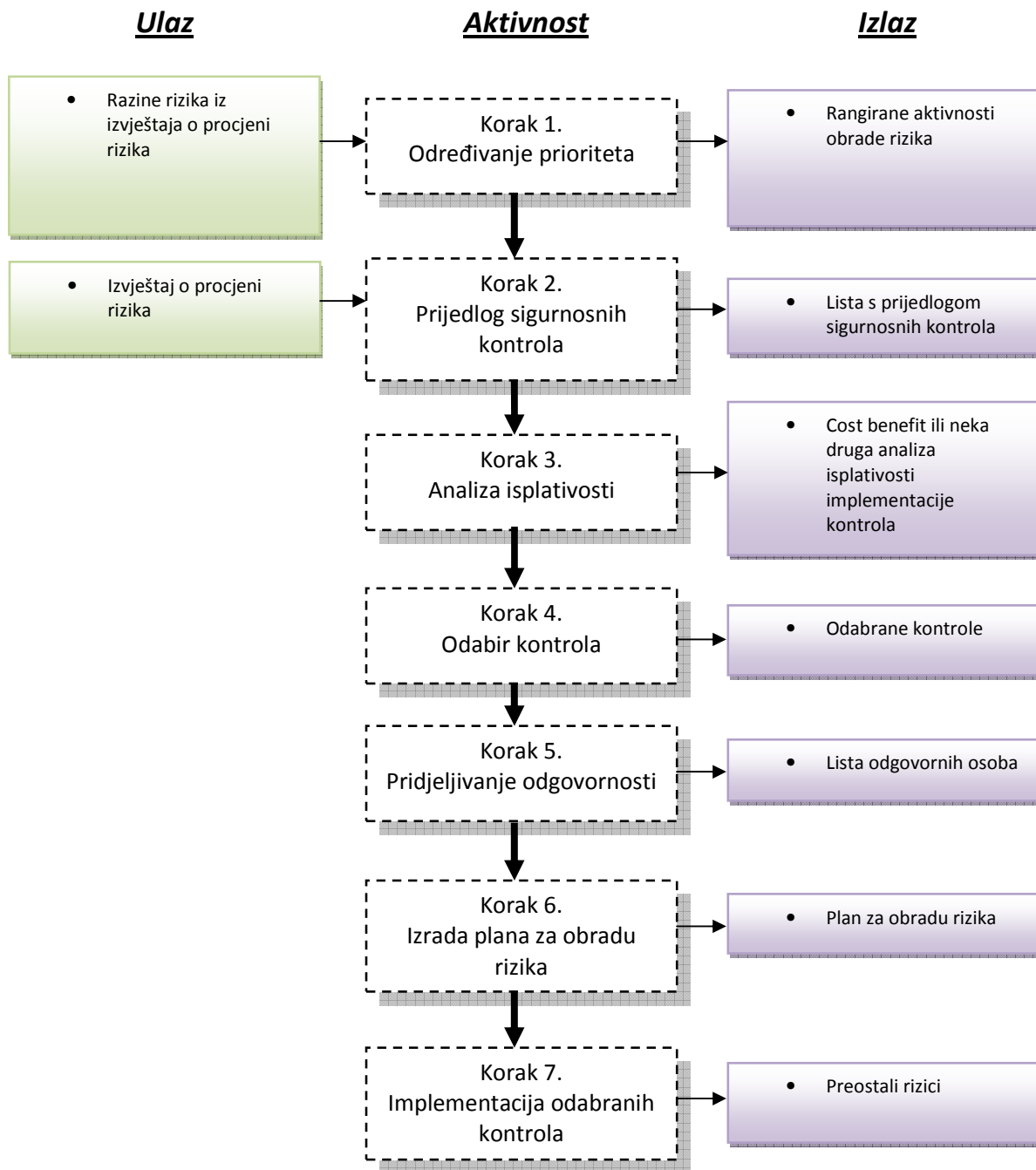
Obrada rizika

Nakon procjene rizika, slijede aktivnosti obrade rizika (vidi sliku 3). Ove aktivnosti uključuju određivanje prioriteta, procjenu, odabir i provođenje sigurnosnih kontrola za smanjivanje rizika. Smanjivanje rizika se uglavnom radi na jedan od 3 moguća načina:

- **Smanjivanje provođenjem sigurnosnih kontrola** – ovim načinom se implementiraju sigurnosne kontrole koje smanjuju vjerojatnost ostvarivanja prijetnje ili smanjuju utjecaj ukoliko dođe do ostvarivanja prijetnje,
- **Izbjegavanje rizika** - bilo koja akcija kod koje dolazi do promjene poslovnih aktivnosti ili načina vođenja poslovanja da bi se spriječila pojava rizika, primjerice nekorištenjem e-trgovine ili Interneta za određene poslovne aktivnosti izbjegava se čitav niz prijetnji koje vrebaju uslijed ovakvog načina poslovanja,
- **Prenošenje rizika** – ovim načinom se uglavnom pokrivaju rizici kod kojih bi implementacija sigurnosnih kontrola bila neekonomična pa se pribjegava prenošenju rizika na drugu organizaciju, primjerice ugovaranjem polica osiguranja i sl.

Zadnja opcija koja ostaje, a ne odnosi se na smanjivanje rizika je svjesno prihvaćanje rizika. Odabirom ove opcije organizacija svjesno prihvaća vrednovani rizik i ne namjerava poduzimati dodatne radnje kako bi ga smanjila. Npr. organizacija može u procesu upravljanja rizicima u kojem su rizici iskazani skalom od 1-5, odlučiti da prihvaća rizike 1 i 2, a za sve rizike koji su viši od 2 primijeniti neke od mogućih načina smanjenja rizika.

Nakon što se rangira katalog rizika, za one rizike koji se žele smanjiti, potrebno je predložiti mjere odnosno kontrole kojima će se to i uraditi. Naravno, neke mjere mogu biti tehnološki vrlo kompleksne i skupe te je stoga potrebno izraditi neku vrstu analize isplativosti. Naime, čemu potrošiti nekoliko milijuna kuna u visokokvalitetni hardver i softver za pohranu podataka, ako rizici koji djeluju nad pričuvnom pohranom nisu visoko rangirani. Analiza isplativosti se može raditi brojnim metodama, a danas je jedana od najkorištenijih, metoda „očekivanog godišnjeg gubitka“ (eng. **ALE – annual loss expectancy**). Ovom metodom se procjenjuje koliki je očekivani gubitak jednog ostvarivanja prijetnje (npr. pola sata zastoja u radu aplikacije A zbog „prljavih“ odnosno nevjerođostojnih podataka košta B kuna). To se množi s procijenjenim brojem takvih događaja godišnje te se dobije očekivani godišnji gubitak C. Ukoliko je za implementaciju kontrole koja smanjuje pojavu ovakvog događaja potrebno utrošiti D kuna, lako je izračunati da li se implementacija takve kontrole isplati ili ne.



Slika 3 - Koraci obrade rizika (prema NIST-u)

Analizom isplativosti organizacija dolazi do konačnog broja sigurnosnih kontrola koje je potrebno implementirati te se na osnovu toga stvara plan obrade rizika, koji jasno komunicira potrebne aktivnosti, odgovornosti u njihovom provođenju, datume početka i kraja implementacije, prioritete aktivnosti i sl.

Implementacijom sigurnosnih kontrola odabrani rizici se smanjuju, ali najčešće nikad u potpunosti. Ono što je cilj jest doći do preostalih rizika nakon implementacije koji su dovoljno niski da ih organizacija može prihvatiti.

Kako odabrati sigurnosne kontrole?

Najbolji odgovor na to su zakoni, standardi, najbolje prakse odnosno smjernice i okviri prema kojima se danas *de facto* vrše upoređivanja (eng. benchmarking) u području informacijske sigurnosti. U svjetskim okvirima to je svakako **ISO/IEC 27001:2005** norma za uspostavu sustava upravljanja informacijskom sigurnošću koja u svom dodatku A ima referencu na ISO 27002 (bivši 17799) standard najboljih praksi primjene sigurnosnih kontrola raspoređenih u 11 poglavlja. Po ovoj normi je moguće i certificirati sustav upravljanja informacijskom sigurnošću organizacije. Trenutno je u Republici Hrvatskoj certificirano 10 organizacija po ovoj normi (ili prethodnim), među kojima su i banke, telekom operateri, informatičke privatne tvrtke pa i jedinice lokalne samouprave. Ovo dokazuje da je ova norma primjenjiva na sve vrste organizacije, raznih veličina ili raznih vertikalala.

Od zakonskih i regulatornih obveza implementacije procesa upravljanja rizicima, danas u Hrvatskoj imamo **Odluku HNB-a o primjerenom upravljanju informacijskim sustavom** u cilju smanjenja operativnog rizika iz 2007. godine, proizašlog iz Basel II zahtjeva koji je napokon malo više pažnje posvetio operativnom riziku te time i IT rizicima kao podskupu operativnih rizika. Odluka HNB-a je obvezujuća za sve naše banke te se i posljednji članci odluke moraju zadovoljiti do sredine 2010. godine. Bankama je tako dan rok od nekoliko godina da prilagode svoje poslovanje sukladno ovim odredbama, a dio vezan za upravljanje rizicima teče upravo u ovom polugodištu.

S druge strane, za tijela državne i javne uprave te sve organizacije koje razmjenjuju klasificirane podatke od značaja za RH, obavezna je primjena **Zakona o informacijskoj sigurnosti** (NN 79/07) koja kroz članke podzakonskog akta Uredba o mjerama sigurnosti, daje jasne zahtjeve za uspostavom procesa upravljanja rizicima.

Što trebaju učiniti organizacije?

Odgovor na ovo pitanje nije jednostavan inače bi sve organizacije primijenile i uspostavile procese upravljanja IT rizicima već davno. Naime, ova disciplina je relativno mlada u Republici Hrvatskoj, i mora se priznati da su veći pomaci napravljeni upravo izbacivanjem odgovarajućih zakona i regulative. Ovim se natjeralo organizacije da se napokon pozabave upravljanjem IT rizicima na metodološki način te smanje gubitke koje su imale, a možda ih nikad nisu dostojno računale. Skupina znanstvenika koja je radila na Basel II direktivi je istraživanjem došla do podatka da operativni rizici (uključujući IT rizike) nose trećinu od ukupnih gubitaka svih ostvarenih rizika.

Danas je primjetan trend da organizacije upravljanje svojim IT rizicima eksternaliziraju (eng. outsourcing) vanjskim tvrtkama koje im pružaju usluge savjetovanja pri uspostavi procesa i realizacije pripadajućih aktivnosti. Ovo nije slučajno. Iako se proces upravljanja rizicima, kako je opisan u prethodnim poglavljima, čini jednostavan, on sadržava brojne zamke prilikom implementacije u praksi. Vanjski savjetnici osiguravaju da se upravljanje rizicima radi na sveobuhvatan način te pridonose i stručnim

ekspertizama za koje organizacije često nemaju dovoljno sredstava i vremena. Naravno, ova priča ima i svoju drugu stranu jer se na tržištu pojavljuje sve veći broj priučenih savjetnika sa sumnjivom stručnom pozadinom. Time organizacija ne dobiva dovoljno kvalitetno rješenje, a pri tom gubi šansu da sama osposobi kadrove za samostalno provođenje procesa upravljanja rizicima.

IT GRC alati

Kao podršku upravljanju rizicima, pojavljuje se sve više softverskih alata iz tzv. IT GRC (G-Governance, R-Risk Management, C-Compliance) sfere. Ovi alati daju podršku onim aktivnostima upravljanja IT rizicima odnosno upravljanju IT-em i sukladnošću, koji rade s velikim skupinama podataka (primjerice registar imovine, katalozi prijetnji i ranjivosti, katalozi sigurnosnih kontrola i sl.) te time ubrzavaju cijeli proces i vode djelatnike putem raznih čarobnjaka (eng. wizards) ili definiranih tijekova rada (eng. workflows).

I ovdje je, kao i kod odabira vanjske tvrtke, potrebno voditi računa o raznim parametrima poput cijene, podrške pri problemima, frekvencije ažuriranja internih kataloga, broja podržavajućih standarda i sl. Za većinu alata je zajedničko to da upravljanju rizicima pristupaju kroz više razina i s bogatim bazama znanja. Cijena ovakvih alata može biti prepreka za mnoge organizacije, ali ukoliko se kvalitetno provede analiza isplativosti, a uzimajući u obzir istraživanja o gubicima uslijed neupravljanja rizicima, često se dolazi do opravdanih iznosa investicija u njih.

Vrijednost imovine	Razina prijetnje								
	Mala			Srednja			Velika		
	Razina ranjivosti								
	M	S	V	M	S	V	M	S	V
0	0	1	2	1	2	3	2	3	4
1	1	2	3	2	3	4	3	4	5
2	2	3	4	3	4	5	4	5	6
3	3	4	5	4	5	6	5	6	7
4	4	5	6	5	6	7	6	7	8

a) Imovina * Prijetnja * Ranjivost

Vjerojatnost ostvarivanja prijetnje	Utjecaj				
	Vrlo veliki (100)	Umjereno veliki (60)	Srednji do mali (30)	Vrlo mali (10)	
Vrlo velika (1)	Vrlo visok (100)	Vrlo visok (60)	Visok (30)	Srednji (10)	
Umjereno velika (0,6)	Vrlo visok (60)	Visok (36)	Srednji (18)	Nizak (6)	
Srednja do mala (0,3)	Visok (30)	Srednji (18)	Nizak (9)	Nizak (3)	
Vrlo mala (0,1)	Srednji (10)	Nizak (6)	Nizak (3)	Nizak (1)	

b) Vjerojatnost ostvarivanja prijetnje * Utjecaj na imovinu

Slika 4 - Dva najčešća načina izračuna rizika