Upravljanje rizicima informacijskog sustava

Šalić, Antonela

SVEUČILIŠTE U ZAGREBU

FAKULTET ORGANIZACIJE I INFORMATIKE

VARAŽDIN

Antonela Šalić

UPRAVLJANJE RIZICIMA INFORMACIJSKOG SUSTAVA

ZAVRŠNI RAD

Varaždin, 2022.

SVEUČILIŠTE U ZAGREBU

FAKULTET ORGANIZACIJE I INFORMATIKE

VARAŽDIN

Antonela Šalić

Matični broj: 1007998345004

Studij: Primjena informacijske tehnologije u poslovanju

UPRAVLJANJE RIZICIMA INFORMACIJSKOG SUSTAVA

ZAVRŠNI RAD

Mentorica: Dr. sc. Aleksandra Sobodić

Varaždin, 2022.

Antonela Šalić

Izjava o izvornosti

Izjavljujem da je moj završni rad izvorni rezultat mojeg rada te da se u izradi istoga nisam koristio drugim izvorima osim onima koji su u njemu navedeni. Za izradu rada su korištene etički prikladne i prihvatljive metode i tehnike rada.

Autor/Autorica potvrdio/potvrdila prihvaćanjem odredbi u sustavu FOI-radovi

---

Sažetak

Često mi sami svjesno ili ne upravljamo rizicima, možda smo nekada želeći postići neki cilj odabrali neku od metoda za rukovođenje rizicima poput prihvaćanja, smanjivanja, prijenosa ili izbjegavanja. Cilj ovog rada je upoznati se sa rizicima informacijskog sustava i kako se njima upravlja, objasniti pojam rizika, te njegovu podjelu, isto tako objasniti analizu rizika i njenu podjelu. Zatim objasniti informacijsku sigurnost i Cyber napade, te kritički analizirati smjernice za upravljanje rizicima poslovnih subjekata.

Ključne riječi: rizik, upravljanje rizicima, informacijski sustav, analiza rizika, informacijska sigurnost, informacijska imovina

Sadržaj

1. Uvod

Tema mog završnog rada je upravljanje rizicima informacijskog sustava. Odabrala sam ovu temu kako bih nadogradila znanje o informacijskom sustavu i upoznala se sa njegovim rizicima. U ovom završnom radu objasnit ću pojam rizika i podjelu rizika. Zatim ću u drugom poglavlju predstaviti upravljanje rizikom i analizu rizika, te ću objasniti kvantitativnu i kvalitativnu analizu rizika. Definirat ću informacijsku sigurnost i nabrojati njezina područja, a nakon toga objasniti i Cyber napade. Zatim slijedi poglavlje upravljanje rizikom informacijskog sustava gdje ću pojasniti metodologiju upravljanja rizicima IS-a, proces vrednovanja rizika IS-a i norme informacijske sigurnosti. I na kraju slijedi kritička analiza smjernica za upravljanje rizicima poslovnih subjekata.

2. Rizik

U današnje vrijeme puno toga predstavlja rizik. Rizik je za studenta koji se nije dobro pripremio izaći na ispit, rizik je pokrenuti vlastiti posao u koji će se uložiti veliki novac, a na kraju ne ostvariti očekivanu dobit. Postoji puno definicija rizika, pa tako neki kažu da rizik predstavlja potencijalni problem ili potencijalnu priliku, drugi pak tvrde da je rizik kalkulirana prognoza, odnosno vjerojatnost moguće štete, gubitka ili opasnosti (Andrijanić, Gregurek i Merkaš, 2016, str. 17). Postoji definicija koja kaže „da je rizik šansa da se dogodi nešto što će imati utjecaja na naše ciljeve“ (Andrijanić i sur., 2016, str. 17), no, opća definicija rizika nam kaže da je rizik sposobnost da se prilikom ostvarivanja nekog cilja taj cilj ne ispuni u cijelosti ili jednim dijelom; mogućnost opasnosti, pogibelji, nesreće, izloženost nezgodi... („Rizik“, bez dat.)

2.1. Podjela rizika

Rizike nije moguće razvrstati na jedinstven način, pa tako imamo više podjela: podjela rizika ne vezano na veličinu i djelatnost, specifične rizike obzirom na veličinu entiteta, poslovne rizike obzirom na djelatnost. Opće je poznato da rizici mogu biti pozitivnog, negativnog ili neutralnog ishoda. Rizik je kod pozitivnih ishoda prezentiran kao prilika, a u situaciji gdje se može očekivati negativan ishod je obično definiran pojmovima neutralnih djelovanja (ako se događaj ne dogodi) ili gubitka. Pa tako imamo rizike događaja čije posljedice daju samo negativne ishode. Primjer takvih rizika su hazardni ili čisti rizici, koji predstavljaju osnovni predmet osiguranja. Najjednostavniji primjer čistog rizika s kojim se susreće većina organizacije je požar ili krađa.

Kontrolne rizike povezujemo s neočekivanim i nepoznatim događajima. Uglavnom se takvi rizici ne mogu predvidjeti, posebno preko tehnika distribucije i povijesnih podataka. Postoje i organizacije koje svjesno preuzimaju rizike, posebno tržišne, s ciljem da postignu pozitivan povrat investicije. Takvi rizici nude mogućnost ostvarenja prinosa i zovu se špekulativni rizici. Postoje dva aspekta povezana sa špekulativnim rizicima, jedan označava rizik propuštanja prilike, a drugi predstavlja opasnost preuzimanja mogućnosti. (Andrijanić i sur., 2016, str. 43 i 44)

Ali rizike možemo podijeliti i bez obzira na veličinu entiteta i djelatnosti, pa tako imamo rizike obzirom na (Andrijanić i sur., 2016, str. 45-56):

- Pristup – koje dijelimo na opće i specifične. U opće spadaju čisti rizici, špekulativni rizici, osnovni rizici, pojedinačni rizici, politički rizici, statički rizici... A u specifične spadaju bankarski, rizici poslovnih organizacija, rizici osiguravajućih društava...
- Vezivanje – u njih spadaju poslovni i neposlovni rizici. Poslovni rizik je rizik ostvarivanja bruto financijskog rezultata poduzeća, a neposlovni rizik nije vezan uz rezultat poslovanja.
- Porijeklo – dijele se na vanjske i unutarnje. Unutarnji rizici nastaju u samoj organizaciji i vezani su uz njezinu strukturu, način upravljanja, zaposlenike i dijelimo ih na rizike upravljanja, strategijske, financijske i operativne. Vanjski rizici predstavljaju sve utjecaje koji dolaze izvan organizacije i dijele se na rizike elementarnih nepogoda, tržišne, političke i društvene.
- Očekivanja – s obzirom na očekivanja, rizike dijelimo na realne koji se relativno lako uočavaju i prepoznaju kao stvarni ili realan gubitak i na oportunitetne koji se ne uočavaju lako kao ni gubitak koji proistječe iz njega.
- Stvaranje – tu imamo špekulativne i hazardne rizike. Primjer špekulativnih rizika je klađenje, kockanje, kartanje... A primjer hazardnih rizika je požar u stanu, elementarna nepogoda, otuđenje stvari...
- Prenošenje – ove rizike dijelimo u dvije grupe, a to su prenosivi i neprenosivi rizici. Prenosivi se mogu prenijeti na drugu stranu, a neprenosivi rizici se u pravilu ne mogu prenijeti.
- Mjerenje – u njih spadaju mjerljivi i nemjerljivi rizici. Kod mjerljivih je moguće izračunati eventualnu nastalu štetu, dok se kod nemjerljivih štetna posljedica ne može kvantificirati.
- Utjecaj – subjektivni rizici predstavljaju rizike vezane uz utjecaj ljudskog faktora unutar organizacije, usko su vezani s poslovnim odlukama i radnim procesima zaposlenika, a objektivni rizici predstavljaju rizike koji su vezani uz događaje izvan aktivnosti zaposlenika.
- Nastup – ovdje rizike dijelimo na direktne i indirektne. Direktni su oni koji nanose štetu direktno i ta je šteta unutar organizacije vezana za nastup određenog događaja. Indirektni rizici su složeniji i uvijek postoji nekoliko načina pomoću kojih se određeni rizik pretvara u štetu unutar organizacije.
- Pojavnost – dijelimo ih na tipične i atipične. Pri tome su tipični oni koje možemo svesti unutar određenih kategorija i grupa, češće se pojavljuju i moguće ih je pratiti, a

atipični se rijetko pojavljuju i predstavljaju događaj koji nije moguće predvidjeti prilikom donošenja poslovnih odluka.

- Brzinu – tu imamo katastrofične rizike koji se uglavnom svode na elementarne nepogode, i imamo tzv. puzajuće rizike koji su stalno prisutni unutar poduzeća i nanose neznatne, ali kontinuirane štete.

2.2. Upravljanje rizikom

Postoje razne definicije za upravljanje rizicima (Krakar i sur., 2014, str. 282):

- Prema COSO (2004.) upravljanje rizicima je proces za koji je odgovorna uprava, menadžment i osobe koje su odgovorne za strategiju poslovnog sustava i analizu potencijalnih događaja koje mogu imati neželjene posljedice na njenu realizaciju.
- Prema ISO/IEC 31000:2009, upravljanje rizicima je koordinirana aktivnost kojom se cijeli poslovni sustav promatra preko rizika.
- Prema ISO/IEC 27005:2011 upravljanje rizicima predstavlja koordinirane aktivnosti usmjeravanja i nadzora organizacije s obzirom na rizike.

Iako postoji još definicija upravljanja rizicima, zajedničko im je to da je upravljanje rizicima sistematičan analitički proces kojim poslovna organizacija pronalazi, identificira, reducira i kontrolira moguće rizike i gubitke kojima je izložena.

Prema ISO/IEC 31000:2009 proces upravljanja rizicima čine sljedeće faze:

- Procjena rizika
    - Identifikacija rizika
    - Analiza rizika
    - Vrednovanje rizika
- Postupanje rizicima
- Nadzor i pregleda rizika
- Komunikacije i konzultiranje o rizicima

Procjena rizika je cjelokupni proces prepoznavanja, analize i ocjenjivanja rizika. Prepoznavanje rizika je otkrivanje, identificiranje i objašnjavanje rizika. Analiza rizika je

shvaćanje prirode rizika i određivanje razine rizika. Ocjenjivanje rizika je definirano kao usporedba postavljenih kriterija i ishoda analize rizika, da bi se procijenilo da li je razina rizika prihvatljiva ili ne.

„Postupanje s rizicima je faza njegove modifikacije koja može uključiti izbjegavanje rizika, donoseći odluku o nepokretanju ili prekidu aktivnosti koje doprinose povećanju rizika, povećanje ili preuzimanje rizika u svrhu ostvarenja potencijalne prilike, uklanjanje izvora rizika, mijenjanje mogućnosti pojave rizika, prenošenje rizika na treću stranu (uključujući ugovaranje i financiranje rizika), mijenjanje posljedica i svjesno prihvaćanje rizika.“ (Krakar i sur., 2014, str. 281).

Kako bi se prepoznale tražene i očekivane promjene, potrebno je nadzirati rizik stalnim provjerama, kritičkim razmatranjem i određivanjem njegovog statusa. Aktivnost kojom se utvrđuje prikladnost i učinkovitost primijenjene mjere s ciljem da se ostvare postavljeni ciljevi naziva se pregled rizika. Organizacija provodi aktivnost komunikacije i savjetovanja o rizicima kako bi dobila informacije nužne da se uključe dionici koji su zainteresirani u proces upravljanja rizicima.

2.3. Analiza rizika

Metode analize rizika koriste se za ocjenjivanje kvalitete, postavki, prijetnji, te za predlaganje promjena arhitekture sustava. To je osnovni alat izrade sigurnosti poslovnog sustava, menadžerski alat koji pruža pomoć za donošenje poslovnih odluka koje su vezane uz moguće gubitke poslovnog sustava. Analizu rizika čine metode koje mogu ugroziti poslovanje sustava kao i zadati štetu sustavu. Da bi analiza rizika bila ostvariva treba:

- prepoznati imovinu sustava koju je potrebno zaštititi,
- prepoznati tipove prijetnji koje mogu utjecati na imovinu,
- računati statističku mogućnost da bi se rizik mogao ostvariti, uz napomenu da statistika nije egzaktna znanost te se uz procjenu računa i procjena pogrešaka,
- odrediti negativne učinke, gubitke koji mogu zahvatiti poslovni sustav.

Analiza rizika proučava rizike koji se izvode unutar neke radnje. Dva su elementa od kojih se sastoji rizik: vjerojatnosti da se događaj dogodi i novčanog iznosa štete prouzročene događajem. Analiza mora osigurati integritet, korisnost i tajnost podataka i aplikaciju koje će analizirati. (Dvorski, Dobrinić, Hutinski i Vrček, 2005, str. 18 i 19)

Iako postoje razni načini analize rizičnosti sustava, analitičke metode rizika grupiramo u dvije skupine, a te dvije skupine su kvalitativne metode analize rizika i kvantitativne metode analize rizika. Njihova ključna razlika je, da se kvantitativna analiza rizika temelji na procjeni vjerojatnosti da će se uočeni rizik ostvariti, a kako bi ta analiza bila moguća treba znati opasnosti koje predstavljaju prijetnju poslovnom sustavu. Kvalitativna analiza se temelji na procjeni rizika koju određuje tim koji obavlja analizu. Subjektivne prirode jer njezin rezultat ovisi o procjeni članova tima. (Andrijanić i sur., 2016, str. 162)

2.3.1. Kvantitativna analiza rizika

Kvantitativna analiza je izražavanje rizika u planiranim novčanim izdatcima na godišnjoj razini. Neke organizacije preferiraju takav način analize jer im je tako dopušteno planiranje novčanih sredstava, pa tako uprava ima mogućnost da bez tehničkih pojedinosti donosi adekvatne odluke. Čista kvantitativna analiza uglavnom se primjenjuje samo u financijskim institucijama poput banaka i osiguravajućih društava. (Andrijanić i sur., 2016, str. 162)

Kao i svaka druga, tako i ova analiza ima svoje dobre i loše strane, pa su dobre strane kvantitativne analize (Dvorski i sur., 2005, str. 19):

- rezultati dobiveni analizom temelje se na objektivnim procesima i mjerenjima,
- statističku vjerojatnost računamo pomoću matematičkih formula,
- procjena potrebnih ulaganja je precizna,
- za prikaz rezultata analize može se koristiti menadžerska terminologija (npr. cijenama, postocima i vjerojatnošću).

A loše strane kvantitativne analize su (Dvorski i sur., 2005, str. 19):

- kompleksno računanje jer analitičar mora dobro razumjeti statističke izraze koje primjenjuje za izradu analize poput pojma vjerojatnosti, pojma odstupanja od vjerojatnosti,

- dobri rezultati ostvaruju se ukoliko je znana baza znanja,

- korištenje analize je kompleksno, zahtjeva više vremena za analizu rizika,

- uvijek postoji mogućnost da neki statistički rezultati nisu točni što ukazuje na neispravnost vjerojatnosti, a uz vjerojatnost se uvijek računa odudaranje vjerojatnosti od stvarnih vrijednosti,

- kako bi bila kompletna treba znati one rizike koji predstavljaju prijetnju sustavu, te ih sve procijeniti,

- objekte analize nije moguće izmijeniti,

- prikladna za prosudbu rizika u okolini koja nije izmjenjiva.

2.3.2. Kvalitativna analiza rizika

Subjektivnije pristupanje pri kojem se rizici, protumjere i resursi promatraju relativno obzirom na sustav čine kvalitativnu analizu rizika. Kako bi se kvalitativna analiza mogla provesti nije potrebno egzaktno poznavati materijalnu vrijednost resursa, ali kako bi se mogli vrednovati bitno je poznavati važnost za poslovne procese koji ih koriste. Ishod kvalitativne analize je relativan odnos vrijednosti šteta uzrokovanih djelovanjem neke prijetnje i uvođenjem protumjera. (Andrijanić i sur., 2016, str. 162)

Dobre karakteristike kvalitativne analize su (Dvorski i sur., 2005, str. 20):

- jednostavno računanje,

- cijenu procjene objekata analize nije potrebno definirati,

- učestalost rizika se ne računa,

- u procjenu uključuje i ostalo osoblje tvrtke,

- fleksibilnog je karaktera,
- jednostavno uklopi novi rizik u analizu,
- procjena rizika ne zahtjeva puno vremena,
- manja cijena implementacije.

Loše karakteristike kvalitativne analize su (Dvorski i sur., 2005, str. 20):

- ishod ovisi o kakvoći tima koji je izrađuje,
- kvaliteta rezultata ovisi o kvaliteti tima,
- o mjerama zaštite ovisi procjena troškovnika.

„Kvalitativna analiza zahtijeva manje vremensko razdoblje za analizu nego kvantitativna, fleksibilnija je na promjene okoline. Kvantitativna analiza rizika zahtijeva veliku bazu znanja o rizicima; ukoliko je rizik nov, nije moguće odrediti učestalost događaja te kvantitativnom analizom rizika nije moguće doći do procjene. Ukoliko u sustavu postoji metoda praćenja rizika koji prijete poslovnom sustavu, pogodnija će biti kvantitativna analiza rizika.“ (Andrijanić i sur., 2016, str. 162).

Ako znamo sve rizike koji predstavljaju prijetnju poslovnom sustavu može se izraditi analiza kvantitativnom metodom, tada ćemo dobiti dobre rezultate. U situaciji kada nisu poznati svi rizici, kvantitativna metoda je nepotpuna, pa je bolje odabrati kvalitativnu analizu rizika kako bi procijenili sigurnost kao temelj odabira mjera zaštite. (Andrijanić i sur., 2016, str. 162)

2.4. Informacijska sigurnost i područja

„Informacijska sigurnost je stanje povjerljivosti, cjelovitosti i raspoloživosti podataka, koje se postiže primjenom propisanih mjera i standarda informacijske sigurnosti te organizacijskom potporom za poslove planiranja, provedbe, provjere i dorade mjera i standarda. Mjere informacijske sigurnosti su opća pravila zaštite podataka koja se realiziraju na fizičkoj, tehničkoj ili organizacijskoj razini. Standardi informacijske sigrunosti su organizacijske i tehničke procedure i rješenja namjenjena sustavnoj i ujednačenoj provedbi

propisanih mjera informacijske sigurnosti.“ („Ured vijeća za nacionalnu sigurnost [UVNS]“, bez dat.)

Tri su osnovna parametra informacijske sigurnosti (Spremić, 2017, str. 53 i 54):

- Povjerljivost (eng. confidentiality) – siguran pristup informacijskome sustavu i informaciji prvenstveno za to nadležnoj osobi.
- Integritet ili cjelovitost (eng. integrity) – zaštita cjelovitosti i ispravnosti informacija i podataka.
- Raspoloživost ili dostupnost (eng. availability) – nadležnoj osobi omogućiti stalan i pravodoban pristup informacijskim sustavima i informacijama.

Tri ključna svojstva informacija čije ugrožavanje označava rizik za poslovanje su (Spremić, 2017, str. 53 i 54):

1. Povjerljivost je informacijsko svojstvo da je na raspolaganju prvenstveno sustavima i osobama koje imaju ovlasti za to. Primjeri posljedica ugrožavanja povjerljivosti informacija: nedostatak povjerenja klijenata (propuštanjem privatnih informacija klijenata u javnosti), nedostatak konkurentne prednosti (otkrivanje podataka konkurenciji o odlikama novog proizvoda), financijski gubitci (propuštanje privatnih informacija može inicirati tužbe klijenata i uroditi isplatom novčanih sredstava kako bi se pokrili odštetni zahtjevi), kršenje mjerodavnih propisa (propuštanje privatnih podataka klijenata može označavati nepoštivanje regulative u području očuvanja privatnih podataka).
2. Cjelovitost je obilježje informacije da postoji racionalno vjerovanje u njezinu točnost, tj. da namjernim ili slučajnim djelovanjem nije nedopušteno ili neplanirano izmijenjeno, što podrazumijeva i naknadno izmjenjivanje, brisanje ili dodavanje informacija bez dokaza o provedenim aktivnostima. Primjeri posljedica ugrožavanja sveobuhvatnosti informacija mogu biti: gubitak povjerenja klijenata (zbog krivo izračunate i naplaćene cijene proizvoda ili usluge), kršenje mjerodavnih propisa, donošenje pogrešnih poslovnih odluka.
3. Dostupnost je obilježje informacije da u određenom roku i po potrebi bude dostupna sustavima i ovlaštenim osobama. Neke posljedice koje narušavaju dostupnost informacija su: onemogućavanje isporuke usluga i proizvoda klijentima, nemogućnost ispunjavanja ugovornih obaveza, kršenje mjerodavnih propisa.

Tri ključna parametra informacijske sigurnosti možemo zaštititi koristeći sljedeće mjere zaštite (Spremić, 2017, str. 53 i 54):

- Povjerljivost ostvarujemo tako da primjenjujemo zaštitne kontrolne mjere koje pristupaju informacijskome sustavu koristeći kontrolne mjere autorizacija i identifikacije korisnika (fizičke, biometrijske, geolokacijske mjere zaštite, logičke metode, dodjele ovlasti)
- Integritet se postiže osiguranjem podataka kod transporta (dinamički podaci) i osiguranjem podataka koji miruju (statički podaci) pri tome primjenjujući metode poput šifriranja podataka, sigurnosnih protokola transporta podataka, poput https, ssl, end-to-end enkripcija i drugi.
- Dostupnost (raspoloživost) koja se ostvaruje korištenjem revizija karakterističnih za rukovođenje kontinuitetom poslovanja, pristupačnosti sustava i resursa sustava i tehnikama oporavljanja poslovanja nakon neželjenog događaja.

Klasifikaciju informacijske sigurnosti na pet područja prikazuju područja informacijske sigurnosti, a cilj klasifikacije je učinkovita i sustavna realizacija donošenja, provedbe i kontrole standarda i mjera informacijske sigurnosti. Takav način pristupanja informacijskoj sigurnosti tipičan je za državni sektor i standardan u zemljama članicama NATO-a i EU-a.

Segmenti informacijske sigurnosti su:

a. sigurnosna provjera
b. fizička sigurnost,
c. sigurnost podataka,
d. sigurnost informacijskog sustava,
e. sigurnost poslovne suradnje.

„Informacijska sigurnost definirana je Zakonom o informacijskoj sigurnosti (NN79/07) i kao takvu obvezna su je provoditi državna tijela, tijela jedinica lokalne i područne (regionalne) samouprave, pravne osobe s javnim ovlastima, koje u svom djelokrugu koriste klasificirane i neklasificirane podatke, te pravne i fizičke osobe koje ostvaruju pristup ili postupaju s klasificiranim i neklasificiranim podacima.“ („UVNS“, bez.dat.)

2.5. Cyber rizici

„Cyber rizici (informatički rizici, IT rizici) su poslovni rizici koji proizlaze iz intenzivne uporabe informacijskih sustava i tehnologije u okruženju digitalne ekonomije kao važne podrške odvijanju i unaprjeđenju poslovnih procesa i poslovanja uopće.“ (Spremić, 2017, str. 38).

Cyber rizici odnose se na prijetnje i opasnosti da intenzivno korištenje informacijskih sustava može prouzročiti neočekivane ili neželjene posljedice kao i financijske ili druge štete u organizaciji, kao i na njezino neposredno i šire okruženje. Iako su podskup informatičkih rizika, cyber rizici su rizici korištenja digitalne tehnologije u osmišljavanju, provedbi, nadzoru i upravljanju digitalnim poslovnim modelima.

Dvije važne značajke cyber rizika uvijek su prisutni i imaju dualnu narav. Uvijek su prisutni se odnosi na to da bez obzira je li ih tvrtka svojim mehanizmima korporativnog upravljanja informatikom otkrila i prihvatila ili nije, i svladavanje takvih rizika predstavlja prilične izazove u dostizanju strateških ciljeva poslovanja. Kada kažemo da cyber rizici imaju dualnu narav mislimo na to da informatičke inicijative koje su dobro vođene kreiraju konkurentsku prednost koja je održiva, novu vrijednost i nove poslovne prilike, a informatičke inicijative koje su loše vođene razaraju poslovanje ne kreiraju novu vrijednost, a troše resurse poslovanja, zaposlenicima stvaraju frustracije i gubitke, stvaraju probleme i štete. (Spremić, 2017, str. 61 i 62)

3. Upravljanje rizikom informacijskog sustava

Rizik informacijskog sustava podrazumijeva mogućnost da prijetnja iskorištavanjem slabosti resursa IS utječe negativno na poslovanje subjekta.

Upravljanje rizikom informacijskog sustava je neprekidni proces koji uključuje („Hrvatska agencija za nadzor financijskih usluga [HANFA]“, 2014):

- Identifikaciju resursa IS,
- Identifikaciju prijetnji resursima IS,
- Identifikaciju ranjivosti resursima IS,
- Procjenu rizika IS i njihovog potencijalnog štetnog učinka,
- Odabir mjera za postupanje s procijenjenim rizicima IS,
- Primjenu mjera za postupanje s procijenjenim rizicima IS,
- Praćenje procijenjenih rizika IS te primijenjenih mjera i postupaka za njihovo smanjenje te
- Unaprjeđenje procesa upravljanja rizicima.

Rukovođenje rizicima informacijskog sustava možemo raščlaniti na dva glavna koraka, proces ublažavanja rizika koji obuhvaća izbor zaštitnih kontrola i njihovu implementaciju, te proces procjene rizika koji obuhvaća identifikaciju, analizu i procjenu rizika. Glavni cilj je da se otkriju i prepoznaju slabosti u sustavu, da se procjeni razina opasnosti kojoj su izloženi resursi i pružiti razuman i izvediv princip smanjenja njihove jačine. (Spremić, 2017, str. 70)

3.1. Metodologija upravljanja rizicima informacijskog sustava

Danas u svijetu postoji puno metoda koje usmjeravaju na upotrebu najboljih praksa za procese upravljanja rizicima. Pojedine se odnose na rizike informacijske sigurnosti, dok se neke odnose samo na IT rizike, a neke su primjenjive u svim aspektima upravljanja rizicima. Zajednička im je podjela rukovođenja rizicima u dvije najvažnije faze: procjena rizika i obrada rizika.

Neke od tih metodologija za rukovođenje rizicima su CRAMM, zatim ISO/IEC 27005:2008, Mehari 2007, Octave, SP800-30 (NIST)... Za neke od ovih metodologija postoje razni softverski alati koji znatno pospješuju postupke rukovođenja rizicima, pružajući kompletnost pri prepoznavanju slabosti i prijetnji, osiguravajući brže i jednostavnije matematičke pokazatelje veličina rizika i pružajući različite vrste izvještaja za visoki menadžment ili osobe nadležne za procese rukovođenja rizicima. Nijedan od tih alata ne funkcionira sam, uglavnom se mora prilagoditi organizaciji, poslovnim procesima organizacije, željama menadžmenta ili različitim zakonskim i regulacijskim kriterijima karakterističnim za pojedinu državu ili poslovnu vertikalu u kojoj organizacija funkcionira. (Uremović, bez dat.)

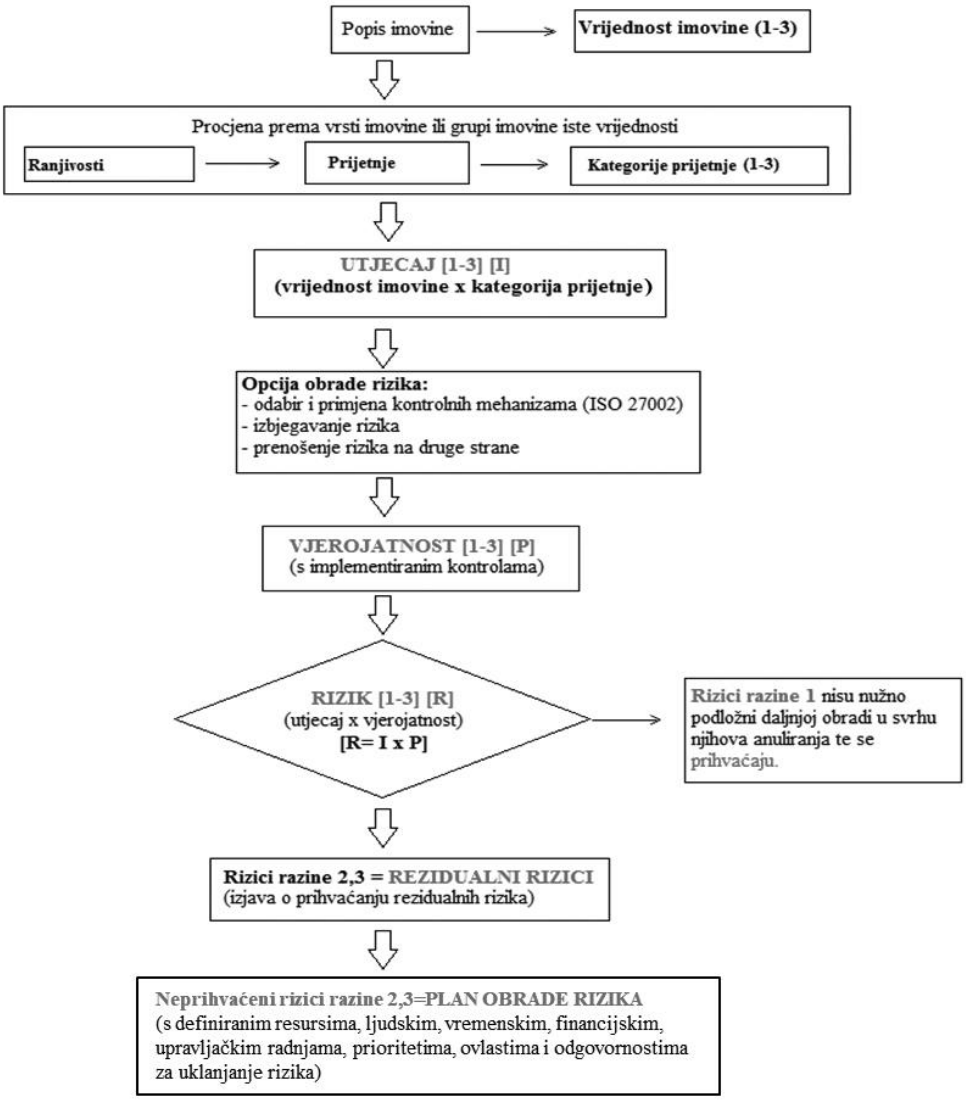
Ovdje je važno spomenuti i PDCA (eng. Plan – Do – Check - Act) krug, poznatiji i kao Demingov krug, a on se koristi kako na cijelom sustavu, tako i na svim elementima sustava upravljanja informacijskom sigurnošću. Faze upravljanja informacijskom sigurnošću su (Žderić i Labaš, bez dat.):

- Planiranje – to je faza pomoću koje se uspostavlja sustav koji će upravljati informacijskom sigurnošću. Pomaže organizacijama da odaberu mjere sigurnosti.
- Implementacija – to je faza pomoću koje se upravlja sustavom informacijske sigurnosti, tako da se ono što je isplanirano u fazi planiranja provede u ovoj fazi.
- Provjera – faza pomoću koje se nadzire i ispituje sustav informacijske sigurnosti kako bi se provjerilo da li dobro funkcionira informacijska sigurnost i da li ispunjava ciljeve.
- Djelovanje – faza pomoću koje se poboljšava sustav informacijske sigurnosti i to tako da se poboljšaju nedostaci faze provjere.

Metodologijom koja osigurava usporedive i ponovljive rezultate vrši se procjena rizika. Kod pojedine imovine rizik se procjenjuje odnosom (Hofer, 2014):

- Vrijednosti pojedine imovine;
- Ranjivosti imovine;
- Prijetnji koje imaju mogućnost da iskoriste ranjivosti;
- Vjerojatnost da će se prijetnje ostvariti;
- Posljedicama koje mogu nastati ako se neka prijetnja ostvari.

Autor navodi da je slika 1. isključivo primjer i da se metodologija procjene rizika radi u skladu s normom ISO 31000 upravljanje rizikom koja utvrđuje niz načela koja treba zadovoljiti za djelotvorno upravljanje rizikom.



Slika 1. Primjer metodologije rizika (Izvor: Hofer, 2014)

3.1.1. Informacijska imovina

Dva ključna koraka u rukovođenju rizicima informacijskog sustava su proces procjene rizika i proces ublažavanja rizika. Prvi korak procesa procjene rizika je utvrđivanje popisa imovine zbog toga što se rizici manifestiraju nepovoljnim učincima upravo na imovini. Ta je faza često kritična jer ima apstraktno razmišljanje o tome što je uistinu imovina. „Informacijska imovina nadilazi imovinu koja se odnosi na računala, poslužitelje, aplikacije i slično, te uključuje sve ono što je vrijednost za organizaciju, a sadržava informaciju ili jest informacija, ili se koristi u procesima podrške uslugama koje počivaju na tim informacijama“ (Čular, bez dat.). Razumijevajući imovinu na taj način, u registru informacijske imovine mogu se pronaći i aplikacije, fizička računala, djelatnici, vanjski partneri, poslovni procesi i drugi. Faza procjene rizika ima fazu izrade registra informacijske imovine koja je jako osjetljiva jer postoji opasnost od krivog shvaćanja izraza imovina, a postoji i mogućnost da se poneka imovina izuzme iz registra. U slučaju da se izuzme imovina iz registra, svi oni rizici koji su vezani za tu imovinu neće biti prepoznati, vrednovani ni obrađeni. Tako da se kreiranjem registra informacijske imovine zapravo definira opseg procesa rukovođenja rizicima. Poslije utvrđivanja opsega sustava za koji se vrši procjena rizika, iduća se faza fokusira na prepoznavanje ranjivosti i prijetnji svih elementa u registru imovine. S obzirom na vrstu imovine, prepoznaju se prijetnje koje možemo pronaći na pojedinoj vrsti imovine, ali i ranjivosti koje se nalaze kod nekih vrsta imovine. (Čular, bez dat.)

3.2. Proces vrednovanja rizika informacijskog sustava

Prvu fazu upravljanja sigurnosnim rizicima nazivamo procjena rizika. Identifikacija, analiza, periodičko ispitivanje i uklanjanje rizika su uključeni u cjelokupni proces rukovođenja sigurnosnim rizicima, a za proces procjene rizika vežemo određeno utvrđivanje sigurnosnog rizika i pojedini resurs. Organizacije upotrebljavaju proces procjene rizika da rizik uključe u svoj IT sustav i kako bi odredile veličinu mogućih prijetnji. Podaci koji predstavljaju ishod procjene rizika kao i oni koji su nužni za odlučivanje vezano za investiranje u sigurnosna rješenja i proizvodnju daju se na pregled menadžmentu organizacije. Procjena rizika je jako složen proces, pa ga najbolje mogu provoditi iskusni stručnjaci koji su dobro upoznati sa sustavom za koji provode procjenu rizika. Proces procjene rizika zasniva se na devet koraka (Zorčec, 2006):

1. Sustavna identifikacija i klasifikacija (eng. Asset Identification);
2. Identifikacija prijetnji (eng. Threat Identification);
3. Identifikacija ranjivosti (eng. Vulnerability Identification);
4. Analiza postojećih kontrola (eng. Control Analysis);
5. Vjerojatnost pojave neželjenih događaja (eng. Likelihood Determination);
6. Analiza posljedica (eng. Impact Analysis);
7. Određivanje rizika (eng. Risk Determination);
8. Preporuka kontrola za umanjivanje rizika (eng. Control Recommendation);
9. Dokumentacija rezultata (eng. Result Documentation).

3.3. Norme informacijske sigurnosti

U Velikoj Britaniji kreiran je standard BS 7799 naziva „Industry Code of Practice“ sa svrhom da se organizacijama privatnog i javnog poslovnog sektora pomogne kako bi se uveo sustav informacijske sigurnosti s ciljem prevencije od oštećenja, zlouporabe ili gubitka nekih podataka ili informacija. Iz tog standarda proizlaze ISO/IEC 17799, tj. ISO/IEC 27001 i ISO/IEC 27002 kao međunarodne norme. „Razlog usvajanja standarda BS 7799 kao međunarodne norme je taj što osigurava fleksibilnost, definira upravljački okvir, a ne zadire u konkretnu tehničku implementaciju što je čini primjenjivom u organizacijama različitih tehničkih sustava bez obzira na njihovu veličinu.“ (Bogati, bez dat.).

IEC i ISO predstavljaju sustav za međunarodnu standardizaciju. ISO je objavila norme vezane za sigurnost i zaštitu informacijskog sustava (Bogati, bez dat.):

- ISO 27000 – Pregled normi iz ISO 27000 serije
- ISO 27001 – Sustav upravljanja informatičkom sigurnošću (ISMS, 2006.)
- ISO 27002 – Kodeks postupka za upravljanje sustavom informacijske sigurnosti (2007.)
- ISO 27003 – Vodič za uvođenje sustava informacijske sigurnosti
- ISO 27004 – Mjerenje i metrika efikasnosti sustava informacijske sigurnosti
- ISO 27005 – Upravljanje rizicima informacijske sigurnosti
- ISO 27006 – Zahtjevi za postupkom analize i certificiranja standarda
- ISO 27011 – Upute za uspostavu sustava informacijske sigurnosti u telekomunikacijskom sektoru

Kod spomenutih normi najvažnije su ISO/IEC 27001 i ISO/IEC 27002. Korištenje tih normi omogućava ujednačenost aktivnosti u organizaciji s valjanom zakonskom regulativom, povećano pouzdanje sustava u trenutku katastrofe, te omogućava povećanje svijesti o bitnosti obuke i osviještenosti djelatnika vezano za informacijsku sigurnost. (Bogati, bez dat.)

4. Kritička analiza smjernica za upravljanje rizicima poslovnih subjekata

Kritička analiza strateškog upravljanja kritički procjenjuje sve aspekte procesa upravljanja. Potrebno je sagledati posao koji se radi u tvrtci kako bismo vidjeli približava li nas svaka aktivnost našim ciljevima. Takav kritički pristup omogućava da se poboljšaju naše strategije kako bi se bolje uskladili sa svojim ciljevima. Menadžeri koji su odgovorni za razvoj strategija se usredotočuju na ciljeve kao što su povećanje dobiti ili prihoda. Kritička analiza uključuje ciljeve tvrtke i društvene ciljeve. Kritička analiza želi da se u obzir uzme doprinos svih dionika i da ih se smjesti u kontekst osnovnih vrijednosti i krajnjih rezultata. Takav pristup mogao bi dovesti do strateškog cilja pružanja veće vrijednosti kupcima, a ne postizanja tržišnog udjela smanjenjem cijena (Markgraf, bez dat.). Na sljedećoj stranici je prikazana Tabela 1. kritičke analize HANFA-e i HNB-a, napravljena na temelju „smjernica za primjereno upravljanje rizicima informacijskih sustava subjekata nadzora Hrvatske agencije za nadzor financijskih usluga“ („Hrvatska agencija za nadzor financijskih usluga [HANFA]“, 2014) i „smjernica za upravljanje informacijskim sustavom u cilju smanjenja operativnog rizika Hrvatske narodne banke“ („Hrvatska narodna banka [HNB]“, 2006). U Tabeli 1. napravljena je analiza pomoću sljedećih kriterija: opis institucije, broj zaposlenih, ciljevi, temeljna načela, prijetnje, načini upravljanja rizikom, upravljanje lozinkama, zaštita od malicioznog koda.

Tabela 1. Kritička analiza HANFA-e i HNB-a

	HANFA	HNB
OPIS INSTITUCIJE	-Hrvatska agencija za nadzor financijskih usluga -nadzire financijska tržišta, financijske usluge, pravne i fizičke osobe koje pružaju financijske usluge	-Hrvatska narodna banka -središnja banka uRepublici Hrvatskoj -dio Europskog sustava središnjih banaka
BROJ ZAPOSLENIH	-182 zaposlenih -90% ima visoku stručnu spremu	-646 zaposlenih -većina ima visoku stručnu spremu
CILJEVI	-razviti svijest o rizicima IS-a -upoznati subjekte s načinima ublažavanja rizika IS-a	-uzeti u obzir organizacijska i druga -održavanje potreba organizacijskih jedinica u banci -osiguranje dosljednosti na svim razinama
TEMELJNA NAČELA	-povjerljivost -cjelovitost -dostupnost	-povjerljivost -integritet -raspoloživost -neporecivost -dokazivost -autentičnost -pouzdanost
PRIJETNJE	-Unutrašnje: neovlašteni pristup informacijama iznutra, interna prijevara, nesvjesno odavanje povjerljivih informacija, pogreške u unosu podataka u aplikacije, krađa resursa IS. -Vanjske: hakerski napadi, maliciozni kod, elementarne nepogode, socijalni inženjering, epidemije bolesti.	-Ljudske se dijele na namjerne kao što su: prisluškivanje, modifikacija informacija, hakiranje, maliciozni kod, krađa, te slučajne kao što su: pogreške i propusti, nenamjerno brisanje datoteka, pogrešno preusmjeravanje, nenamjerno fizičko uništenje. -A pored ljudskih postoje i prirodne prijetnje: potres, udar groma, poplava, požar.
NAČINI UPRAVLJANJA RIZIKOM	-izbjegavanje -smanjenje -prihvaćanje -prijenos	-procjena -smanjenje -održavanje prihvatljive razine
UPRAVLJANJE LOZINKAMA	-identificirati i koristiti minimalne standarde svojstava lozinki kako bi se pristupilo resursima IS-a -čuvati tajnost lozinki -lozinke moraju biti spremljene u obliku koji je nečitljiv -izbjegavati riječi iz riječnika, privatne podatke i ostale izraze koji se lako pogode	-sve lozinke moraju biti povjerljive -ne smiju biti pohranjene ni prikazane u čitljivom obliku -ne smije ih dijeliti više osoba -odrediti period nakon kojeg se lozinka mora izmijeniti i onemogućiti višekratno korištenje iste lozinke -lozinke treba izmijeniti ako se sumnja da su njihova povjerljivost i integritet narušeni
ZAŠTITA OD MALICIOZNOG KODA	-osigurati adekvatnu primjenu sustava zaštite komponenti IT od malicioznog koda -osigurati ažurnost sustava kako bi se zaštitile komponente IT-a od malicioznog koda -osigurati redovito korištenje sigurnosnih ispravaka operativnih sustava i aplikacija -osigurati odgovarajuću upotrebu preglednika internetskih stranica i klijenata elektroničke pošte korisnicima IS-a	- jednom dnevno provjeravati ažurnost sustava zaštite od malicioznog koda i neovlaštenih i neuobičajenih radnji - sustavi za otkrivanje malicioznog koda koji se temelje na identificiranju uzorka teže otkrivaju maliciozni kod u enkriptiranim podacima

(Izvor: smjernice HANFA-e i HNB-a)

5. Zaključak

Iako postoji puno definicija rizika, ona kojom sam se vodila u radu je sposobnost da se prilikom ostvarenja nekog cilja taj cilj ne ispuni u cijelosti ili jednim dijelom. Isto tako kao što postoji puno definicija rizika, postoje i različite podijele rizika, ali ona kojoj sam posvetila više pažnje je podjela bez obzira na veličinu entiteta i djelatnosti. Analizom rizika ocjenjujemo kvalitetu, postavke, prijetnje, a u tome pomažu kvantitativna i kvalitativna analiza rizika. Imamo i cyber rizike koji nam dokazuju da i u IT-u postoje prijetnje i opasnosti s kojima se možemo suočiti. Informacijski sustavi su važni za svako poduzeće. Kako bi mogli sigurno upravljati informacijskim sustavima treba upravljati mogućim rizicima samog tog informacijskog sustava, a to činimo dvama glavnim koracima procjenom rizika i ublažavanjem rizika. Glavni cilj je prepoznati slabosti informacijskog sustava kako bi mogli pružiti prihvatljiva rješenja. Kritičkom analizom vidimo da su smjernice HANFA-e i HNB-a slične u pogledu temeljnih načela, načina kako upravljaju rizikom i lozinkama i kako štite od malicioznog koda, ali isto tako imaju i svoje razlike u broju zaposlenih, ciljevima i prijetnjama. Za upravljanje rizicima informacijskog sustava razvili su se razni standardi i metodologije koji ubrzavaju sam postupak upravljanja rizicima. Vjerujem da će se i u budućnosti razviti niz novih načina koji će pospješiti sigurnost informacijskog sustava i upravljanje njegovim rizicima.

Popis literature

1. Andrijanić, I., Gregurek, M., i Merkaš, Z. (2016). *Upravljanje poslovnim rizicima*. Zagreb: Libertas – Plejada.

2. Bogati, J. (bez dat.). *Norme informacijske sigurnosti ISO/IEC 27K* (Stručni rad, Ministarstvo obrane Republike Hrvatske, Virovitica, Odsjek za poslove obrane Virovitica). Preuzeto s https://hrcak.srce.hr/76462

3. CCTA Risk Analysis and Management Method [CRAMM] (1985) *European union agency for cybersecurity*

4. Čular, J. (bez dat.). *Razina prihvatljivosti*. Preuzeto 10.5.2021. s http://www.infotrend.hr/clanak/2012/4/razina-prihvatljivosti,72,912.html

5. Dvorski, S., Dobrinić, D., Hutinski, Ž., i Vrček, N. (2005). *Izravni marketing: Poglavlje „Sigurnost informacijskog sustava" iz obvezne literature kolegija „Poslovna informatika"*. Tiva tiskara, Varaždin.

6. Eaton, W., J. (Octave) (1988) *European union agency for cybersecurity*

7. Hofer, D. (2014). *Implementacija sustava upravljanja informacijskom sigurnošću prema ISO 27001:2013* (Stručni rad, Hrvatska konferencija o kvaliteti i 5. znanstveni skup hrvatskog društva za kvalitetu), Baška, otok Krk. Preuzeto s https://vdocuments.mx/implementacija-sustava-upravljanja-informacijskom-sigurnoscu-prema-iso-270012013.html

7. Hrvatska agencija za nadzor financijskih usluga [HANFA] (2014) *Objave sa sjednice upravnog vijeća*. Preuzeto 10.5.2021. s https://www.hanfa.hr/objave-sa-sjednica/24102014_-66-sjednica-upravnog-vijeca-hanfe/

8. Hrvatska agencija za nadzor financijskih usluga [HANFA] (2014) *Smjernice za primjereno upravljanje rizicima informacijskih sustava subjekata nadzora*. Preuzeto 1.7.2021. s https://www.hanfa.hr/getfile/41377/Smjernice%20za%20primjereno%20upravljanje%20rizicima%20IS%20subjekata%20nadzora%20Agencije%20-%20PRIJEDLOG.pdf

9. Rizik. (bez dat.). U Hrvatska enciklopedija. Preuzeto 12.02.2021. s https://www.enciklopedija.hr/natuknica.aspx?id=53028

10. Hrvatska narodna banka [HNB] (2006) *Smjernice za upravljanje informacijskim sustavom u cilju smanjenja operativnog rizika*. Preuzeto 1.7.2021. s https://www.hnb.hr/-/smjernice-za-upravljanje-informacijskim-sustavom-u-cilju-smanjenja-operativnog-rizika

11. International Organization for Standardization (2008) *ISO/IEC 27005:2008*

12. Krakar, Z., Tomić Rotim, S., Žgela, M., Arbanas, K., i Kišasondi T. (2014). *Korporativna informacijska sigurnost.* Fakultet organizacije i informatike, Varaždin.

13. Markgraf, B. (bez dat.). *Critical Analysis of Strategic Management*. Preuzeto 15.07.2021. s https://smallbusiness.chron.com/critical-analysis-strategic-management-65195.html

14. Method for Harmonized Analysis of Risk [Mehari 2007] (2007) *European union agency for cybersecurity*

15. National Institute of Standards and Technology [NIST] (2012) *SP 800-30 (NIST)*

16. Spremić, M. (2017). *Sigurnost i revizija informacijskih sustava u okruženju digitalne ekonomije.* Sveučilište u Zagrebu Ekonomski fakultet, Zagreb.

17. Ured vijeća za nacionalnu sigurnost [UVNS] (bez dat.) *Koja su područja informacijske sigurnosti?* Preuzeto 12.02.2021. s https://www.uvns.hr/hr/koja-su-podrucja-informacijske-sigurnosti

18. Uremović, D. (bez dat.). *Kako upravljati IT rizicima?* Preuzeto 10.5.2021. s

http://www.infotrend.hr/clanak/2009/6/kako-upravljati-it-rizicima,37,767.html

19. Zorčec, M. (2006). *Upravljanje sigurnosnim rizicima* (Diplomski rad, Sveučilište u Zagrebu, Fakultet elektrotehnike i računarstva), Zagreb. Preuzeto s http://sigurnost.zemris.fer.hr/ISMS/rizik/2006_zorcec/marinjo_diplomski/diplomski_marinjo.pdf

20. Žderić, M., i Labaš, D. (bez dat.). Upravljanje rizicima sukladno s ISO normama sigurnosti – područje informacijske sigurnosti, sigurnosti na radu i sigurnost hrane. *Međunarodna znanstveno-stručna konferencija.*

Popis slika

Popis tablica