Sigurnosni i financijski aspekt informatičkih rizika poslovnih informacijskih sustava

Roso, Moris

VELEUČILIŠTE s pravom javnosti
BALTAZAR ZAPREŠIĆ
Zaprešić
Specijalistički diplomski stručni studij
Financijski menadžment

MORIS ROSO

SPECIJALISTIČKI DIPLOMSKI RAD

SIGURNOSNI I FINANCIJSKI ASPEKT INFORMATIČKIH RIZIKA POSLOVNIH INFORMACIJSKIH SUSTAVA

Zaprešić, 2020. godine

VELEUČILIŠTE s pravom javnosti
BALTAZAR ZAPREŠIĆ
Zaprešić
Specijalistički diplomski stručni studij
Financijski menadžment

SPECIJALISTIČKI DIPLOMSKI RAD

SIGURNOSNI I FINANCIJSKI ASPEKT INFORMATIČKIH RIZIKA POSLOVNIH INFORMACIJSKIH SUSTAVA

Mentorica:

izv. prof. dr. sc. Ivana Ogrizek Biškupić

Apsolvent:

Moris Roso

Naziv kolegija:

INFORMACIJSKI SUSTAVI ZA POSLOVNO UPRAVLJANJE

JMBAG studenta:

0234040787

SADRŽAJ

SAŽETAK

S ciljem zaštite poduzeća od mogućih rizika, ono mora upravljati njima kako bi ih maksimalno u svojem poslovanju preveniralo ili svelo na najmanju moguću mjeru. Informacijski sustav nekog poduzeća predstavlja njegovu okosnicu i u današnje vrijeme, temelj osiguranja provedbe poslovnih procesa i transakcija. Ranjivost informacijskog sustava predstavlja velik rizik za poduzeće pa su tako nastale metodologije i metrika čijom se primjenom nastoji spriječiti moguća šteta po tvrtku. Informacijski rizik implicira financijski rizik te se u tom kontekstu u ovome radu promatra važnost informacijskog sustava, rizici mogućih gubitaka uslijed pada pojedinih njegovih segmenata te metodologije koje se u svrhu sprječavanja istog u tvrtkama koriste.

KLJUČNE RIJEČI : Informacijski sustav, rizik, informacijski rizik, upravljanje rizikom

ABSTRACT

In order to protect companies from possible risks, it must manage them in order to prevent them to the maximum in its business or to minimize them. Information system of a company is its backbone and in this time, the basis for ensuring the implementation of business processes and transactions. The vulnerability of the information system represents a great risk for the company, so methodologies and metrics have been created and with their application, seek to prevent possible damage to the company. Information risk implies financial risk, and in this context the importance of the information system, the risks of possible losses due to the decline of some of its segments and the methodology used to prevent it in companies are observed in this paper.

KEY WORDS: Information system, risk, information risk, risk management

1. UVOD

Dakle, pod informacijskim sustavom podrazumijevamo sve postupke koji sakupljaju, analiziraju, pripremaju te pokazuju informacije i podatke koji su veoma važni za poduzeće. Danas se informacijski sustavi većinom ostvaruju uz pomoć suvremene informacijske i komunikacijske tehnologije.

Rizik u ekonomiji bio bi opasnost nastupa neželjena događaja i mogućnosti gubitka ili umanjenja imovine. Mogućnost donošenja pogrešne odluke u upravljanju poduzećem zbog nastupa iznenadnog neželjenog događaja i zakazivanja ljudskoga faktora po čemu nastaje šteta. Upravljanje rizikom je cjelokupan proces mjerenja i procjena strategija za kontrolu nad rizikom.

Informacijski rizici predstavljaju vjerojatnost nekog nepoželjnog događaja kao što su prijetnje koje u datim okolnostima uzrokuju štetu, umanjenje inteziteta rada informacijskog sustava, zastoj ili štetu na informacijama koje su u njemu spremljene. Informacijska sigurnost svodi se na sigurnost informacijskog sustava i samih informacija zasebno.

Cilj rada je ukazati na problem informacijskih rizika na poslovni informacijski sustav te kako se pripremiti, te ublažiti štetu. Ukazati na problem da potpuna zaštita informacijskih sustava ne postoji. Kako se razvija tehnologije informacijskoga sustava tako i raste broj rizika koji mogu bitno utjecati na samo poslovanja poduzeća.

Rad se sastoji od 4 osnovnih dijelova: Informacijski sustav, rizik, informacijski rizik te financijski aspekt upravljanja istim.

2. INFORMACIJSKI SUSTAV

Dakle, pod informacijskim sustavom podrazumijevamo sve postupke koji sakupljaju, analiziraju, pripremaju te pokazuju informacije i podatke koji su veoma važni za poduzeće. Danas se informacijski sustavi većinom ostvaruju uz pomoć suvremene informacijske i komunikacijske tehnologije. Navedene prikupljene informacije te i podaci se čuvaju u bazama podataka. Poslovni sustav mora sadržavati informacijski sustav, radi lakšeg vođenja poslovnih projekata. Neke od glavnih sastavnica informacijskog sustava:[1]

1. Sustav upravljanja izvještajima
2. Sustav upravljanja informacijama
3. Sustav koji pomaže pri odlučivanju

Učinkovito obavljanje poslova u poslovnom sustavu, praćeno je podacima i informacijama. Zbog sve veće uporabe informacijske tehnologije u poslovnim projektima, informacijski sustav postaje značajan za bilo kakav posao kojom se poduzeće bavi. Sama svrha informacijskog sustava je sakupljanje važnih informacija potrebne za procese poslovanja te i samo vođenje poslovnog sustava. Može se reći da informacijski sustav pokazuje poslovnu realnost, razrađujući poslovne aktivnosti te pomaže poduzeću u ostvarivanju poslovnih ciljeva. Fizička osoba spada isto kao faktor informacijskog sustava, izvršava poslovne zadaće, daje podršku informacijskom sustavu te ga unaprijeđuje, koristeći se informacijskom tehnologijom. Modeli informacijskog sustava su:[2]

1. Model procesa – utvrđuje procese iz samog poslovnog sustava
2. Model podataka – utvrđuje podatke koji se koriste u poslovnom sustavu
3. Model izvršitelja – utvrđuje elemente koji su uključeni u izvršavanju procesa

[1] https://www.enciklopedija.hr/natuknica.aspx?id=27410 (pristupano 24.05.2020)
[2] http://www.ss-strukovna-vvlatkovica-zd.skole.hr/images/pages/Nastavni_materijali/Spahic/Upotreba_IT/inf.doc (pristupano 24.05.2020)

2.1. Svrha informacijskog sustava

Svrha informacijskog sustava je ta da kao podsustav poslovnog sustava obrađuje korisne i nove informacije te na taj način komunicira sa okolinom, preuzima informacije koje obrađuje i tako prerađene prezentira poslovnom sustavu. U poslovni sustav izlaze i ulaze informacijski tijekovi. Informacijski sustav može biti tehnološki podložan modernizaciji ili ručan. Kao što je već rečeno prije, sama svrha informacijskog sustava je sakupljanje važnih informacija potrebne za procese poslovanja te i samo vođenje poslovnog sustava. Postoji više razina na kojima se obavlja rukovođenje a to su:[3]

1. Strateška

2. Taktička

3. Operativna

Strateško rukovođenje spada pod najviši menadžment koji donosi dugoročne strateške poslovne odluke.

Taktičko rukovođenje spada pod srednji menadžment koje analizira aktivnosti na duže razdoblje jer informacije imaju oblik periodičkih izvještaja.

Operativno rukovođenje spada pod niži menadžment koji kontrolira dnevne poslovne aktivnosti i donosi odluke taktičkog menadžmenta. Informacije izgledaju kao dnevni izvještaj.

Razine upravljanja:[4]

1. Sustav za potporu odlučivanja (DSS - Decision Support System) – ovaj sustav za potporu koristi informacije iz prošlosti kako bi na temelju njih izvukao nove informacije koje bi bile veoma važne u procesu odlučivanja. Kao takav može biti složen sustav koji uz razne tehnike uključuje i tehnike obrade informacija , upitnih jezika , modeliranje proračunskih tablica i ekspertnih sustava pa i umjetne inteligencije. (eng.Al-Artificial Intelligence).

[3] http://tecajevi.freeservers.com/isuvod.htm (pristupano 24.05.2020)
[4] http://tecajevi.freeservers.com/isuvod.htm (pristupano 24.05.2020)

2. Transakcijski informacijski sustav - daje potporu dnevnom objavljanju aktivnosti poslovanja koje uključuje iz vanjskih izvora obradu podataka unutar sustava koja može biti osim automatska i elektronska.

3. Upravljački informacijski sustav - koristi srednjem poslodavstvu koje opskrbljuju kategoriziranim i sintetiziranim podacima iz transakcijskog dijela informacijskog sustava.

2.2. Poslovni sustav

Poslovni sustavsluži za izvršavanjeposlovnih procesa unutar nekog poduzeća i svako poduzećenastoji izgraditi svoj informacijski sustav kojičini podlogu za kvalitetno i brzo odlučivanje i upravljanje odlukama . Informacijski sustav poslovnom sustavu omogućava komunikaciju unutar sebe i okoline. Pod materijalnim faktorima spadaju:[5]

1. Sirovina

2. Materijal

3. Energija

Glavne aktivnosti poslovnog sustava su:[6]

1. Izvršavanje poslovnih procesa

2. Upravljanje poslovnim sustavom

U poslovni proces spada osnovna poslovna djelatnost. U proizvodnji nekog poduzeća poslovni proces sastoji se od raznih poslova a to su nabava potrebnih sirovina, nabava energije, proizvodnja i plasman proizvoda i dr. U bankama poslovni proces dijeli se na obavljanje transakcije financija, štednje, kreditiranja i mnoga druga.

[5] http://www.ss-strukovna-vvlatkovica-zd.skole.hr/images/pages/Nastavni_materijali/Spahic/Upotreba_IT/inf.doc (pristupano 24.05.2020)
[6] http://www.ss-strukovna-vvlatkovica-zd.skole.hr/images/pages/Nastavni_materijali/Spahic/Upotreba_IT/inf.doc (pristupano 24.05.2020)

Upravljanje poslovnim sustavom , odnosno svakim stvarnim sustavom u koje ubrajamo poduzeća, privredu, društvo, ustanove i dr., donose važne odluke za efikasnost odvijanja poslovnog procesa pomoću informacijskog sustava i informacijske tehnologije bez kojih bi bilo nemoguće obavljati posao. Uz pomoć informacijskog sustava obje aktivnosti osnažene su na način da transformiraju informacije u odluke a tako i efikasnije ,brže stvaranje poslovnih odluka i djela.

2.3. Sustavski pristup (pojam sustava, elementi sustava, veze u sustavu)

Sustavnim pristupom istražuju se i riješavaju svi problemi sa svom složenošću i cjelovitošću obuhvačajući sve odnose i veze između okoline i djelova sustava. Čini cjelinu koja se rastaviti ne može zato što pri tome gubi osnovna svojstva. Sustavni pristup spaja sve dosadašnje razdvojene predmete znanstvenog proučavanja i područja razdvojenih ljudskih aktivnosti. Ta sustavna cjelina je sređena povezana na određeni način svojih elemenata. Za opis nekog sustava treba odrediti koje veze pripadaju samom sustavu, elementi koji pripadaju sustavu te koje veze postoje unutar samog sustava prema elementima sustava i okoline te samo međusobno funkcioniranje sustava. Elementi su dio stvarnog objekta koji tvori realni sustav:[7]

1. Društveni
2. Fizički
3. Mehanički
4. Biološki

2.4 Pojmovi vezani uz informacijski sustav

Pojam podatak, je pojam kojim kvantificiramo odnosno mjerimo elementarnu ili simboličnu funkciju realnog sustava u odredjenom trenutku.[8] Njime se izgrađuje informacija. Danas se podaci

[7] http://www.ss-strukovna-vvlatkovica-zd.skole.hr/images/pages/Nastavni_materijali/Spahic/Upotreba_IT/inf.doc (pristupano 24.05.2020)
[8] http://www.ss-strukovna-vvlatkovica-zd.skole.hr/images/pages/Nastavni_materijali/Spahic/Upotreba_IT/inf.doc (pristupano 24.05.2020)

pohranjuju u računalima kao bitovi, njihov načini pohranjivanja su standardizirani te najčešći je kod ASCII (ISO-7)[9].

Pojam informacija, označuje dio podataka sa određenim značenjem te nam one povećavaju znanje kada ih koristimo kao glavni temelj u komunikaciji[10]. Često pojmove podatak i informaciju smatraju sinonimima no njihovo se značenje razlikuje. „Informacija ili obavijest proizlazi iz podatka kao zapis na nekom mediju, informacija odnosno obavijest je određeno značenje tj.činjenica s određenim značenjem“.[11]

Sam primatelj informacije odredit će njenu vrijednost . Što je informacija točnija i novija toliko je i vrijednija pri odlučivanju. Svaku informaciju sačuvat ćemo u obliku podatka. Sva područja u određenom vremenskom trenutku organiziraju utvrđivanjem svoje znanje, medusobnih odnosa i ograničenja prikladnih kategorija koncepata. Ima niz načina prikaza znanja. U obliku pravila je najpoznatiji (npr. teorema. matematici aksioma i dr.). Najviše distribucije dobivaju na internetu i kooperacijskim mrežama. Ujedno se sve više razvijaju i skladišta podataka iz svih izvora te se pohranjuju.[12]

2.5 Informacijski sustav u poslovnom sustavu

Informacijski je sustav podsustav poslovnog sustava. Glavni cilj informacijskog sustava je opskrbljivati poslovni sustav svim njemu korisnim i potrebnim podacima nužno potrebnim za donošenje raznih poslovnih odluka i odlučivanja tj. donositi pretpostavke o upravljanju poslovnim sustavom. Pozitivni rezultati nastaju primjenom informacijskog sustava. Pojedinac kao dio informacijskog sustava, formalizira poslovno okruženje u podatke, algoritme, procedure i informacije primjenom informacijske tehnologije i programsku podršku, ispunjava poslovne funkcije i zadatke[13].

[9] https://www.enciklopedija.hr/natuknica.aspx?id=48887 (pristupano 26.10.2020)
[10] https://www.enciklopedija.hr/natuknica.aspx?id=27405 (pristupano 26.10.2020)
[11] http://www.ss-strukovna-vvlatkovica-zd.skole.hr/images/pages/Nastavni_materijali/Spahic/Upotreba_IT/inf.doc (pristupano 24.05.2020)
[12] http://www.ss-strukovna-vvlatkovica-zd.skole.hr/images/pages/Nastavni_materijali/Spahic/Upotreba_IT/inf.doc (pristupano 24.05.2020)
[13] http://www.ss-strukovna-vvlatkovica-zd.skole.hr/images/pages/Nastavni_materijali/Spahic/Upotreba_IT/inf.doc (pristupano 24.05.2020)

Sustavi egzistiraju radi ostvarivanja poslovnih ciljeva. Za njihovo ostvarenje važno je upravljati sustavom na način da se donose adekvatne odluke, a kako bi se one donijele potrebne su informacije koje proizlaze iz informacijskog sustava. Informacijski sustav sakuplja važne informacije potrebne za procese poslovanja te i samo vođenje poslovnog sustava. Uspješan poslovni sustav mora imati pravi informacijski sustav koji ima najnoviju informatičku tehnologiju. U samom procesu odlučivanja, poslovni informacijski sustav pomaže u donošenju odluka pošto sadrži potrebne informacije na koje bi menađžeri trebali imati uvid. Upravljanje poslovnim sustavom:[14]

1. Funkcije informacija – pruža informacije o stanju sustava u određenom vremenu
2. Funkcija upravljanja – pruža informacijske podloge za upravljanje i odlučivanje
3. Funkcija dokumentiranja – pruža obradu poslovnih podataka o prijašnjim događajima

[14] http://www.efos.unios.hr/poslovni-informacijski-sustavi/wp-content/uploads/sites/216/2013/04/1.-POSLOVNI-INFORMACIJSKI-SUSTAVI.pdf (pristupano 26.10.2020)

3. RIZIK

Vjerojatnost da se određeni cilj ne ostvari. Rizik u ekonomiji bio bi opasnost nastupa neželjena događaja i mogućnosti gubitka ili umanjenja imovine. Mogućnost donošenja pogrešne odluke u upravljanju poduzećem zbog nastupa iznenadnog neželjenog događaja i zakazivanja ljudskoga faktora po čemu nastaje šteta. Rizik dijelimo na prenosivi i neprenosivi:[15]

1. Prenosivi rizik – kod ovih rizika može se ustanoviti kada bi mogli nastati i koliku štetu bi mogli napraviti
2. Neprenosivi rizik – kod ovih rizika se ne može utvrditi kada bi mogli nastati ni koliku štetu bu mogli napraviti

Pri donošenju poslovnih odluka, rizik je mogućnost procjene nesigurnosti. Radi mogućnosti procjene rizika, rizik se može uračunati u troškove poslovanja.

Nemogučnost podmirenja obaveza je kreditni rizik, dakle govori se o uloženim sredstvima za koje postoji rizik da se neće vratiti.[16]

Rizik likvidnosti je onaj rizik kada poduzeće nije sposobno u kratkom vremenskom razdoblju pretvoriti dio unovčive imovine u novac.

Tržišni rizik je kada se zbog kretnje cijena na tržštu može ostvariti gubitak[17].

Osiguratelj ugovorom ili uvjetima utvrđuje:[18]

1. Rizike koji se preuzimaju kod stanovitih povećanih premijskih stopa
2. Rizike koji obuhvaćaju određeno standardno osiguranje,
3. Rizike koji su ograničavani
4. Rizike koji su isključeni

[15] https://www.enciklopedija.hr/natuknica.aspx?id=53028 (pristupano 06.06.2020)
[16] https://www.hnb.hr/temeljne-funkcije/medunarodne-pricuve/rizici (pristupano 27.10.2020)
[17] https://capital.com/hr/trzisni-rizik-definicija (pristupano 27.10.2020)
[18] https://www.enciklopedija.hr/natuknica.aspx?id=53028 (pristupano 06.06.2020)

Osiguratelji vode statistiku o preuzetim rizicima, te na osnovi dobivenih podataka te uporabom teorije o rizicima zasnivaju svoju poslovnu politiku, mogu ih prihvatiti ili odbaciti u svoje osiguranje.[19]

3.1. Upravljanje rizicima

Rizicima se može upravljati tako da se:[20]

1. Izbjegavaju – primjerice promjenom tehnologije
2. Preuzimaju – znaći da se ne poduzima ništa pošto je rizik malen
3. Umanjuju – klasičan pristup
4. Prebacuju – djeli se odgovornost na treću stranu

Subjekti koji sudjeluju u upravljanju rizicima su:[21]

1. Nositelj aktivnosti (eng. risk action owner)
2. Potencijalni nositelj (eng. risk owner)
3. Direktor projekta (eng. project director)
4. Osoba koja upravlja rizicima (eng. risk manager)

Odredbe koje definiraju funkciju kontrole rizika , većinu poslova veže kontrola rizika jer sukladno zakonu obavlja sljedeće:[22]

1. Praćenje rizika,
2. Analiza rizika,
3. Izvještavanje svih o riziku,
4. Sudjelovanje u funkcioniranju i izradi metoda i modela za kontrolu nad rizikom i
5. Proučavanje stanja

Upravljanje rizikom je cjelokupan proces mjerenja i procjena strategija za kontrolu nad rizikom. Širi pojam menadžmenta rizika uključuje procjene, analize i identifikaciju rizika. Menađžeri

[19] https://www.enciklopedija.hr/natuknica.aspx?id=53028 (pristupano 06.06.2020)
[20] https://www.safu.hr/datastore/filestore/332/Upravljanje_rizicima_1.pdf (pristupano 06.06.2020)
[21] https://repozitorij.unin.hr/islandora/object/unin%3A1969/datastream/PDF/view (pristupano 06.06.2020)
[22] https://repozitorij.unin.hr/islandora/object/unin%3A1969/datastream/PDF/view (pristupano 06.06.2020)

moraju sagledati informacije dobivenih iz istraživanja stanja u kojemu se poduzeće nalazi, te potom dati zahtjev za eliminiranje rizika.[23]

Klasični menadžment rizika se odnosi na one rizike koji su proizašli prirodnim putem (požar, poplava) te i na pravne čimbenike. Menadžment rizika poduzeća usmjerava se prema okolnostima i događajima koji negativno utječu na samo poduzeće. Tako imamo i menadžment rizika koji se odnosi na financijske rizike.[24]

Strategijski problem razvoja, upravljanja, promatranja i organizacijskih teorija čine rizici. Zbog mogućnosti mjerljivosti, postoji mogućnost i upravljanjem nad jedinicom nesigurnosti koju predstavlja sam rizik. (Perhot, 2011).

U širi pojam menadžmenta rizika spadaju procesi analize i procjene rizika, proces identifikacije . Glavni cilj smanjenje i upravljanje rizikom jest taj da očuva učinkovitost djelovanja. Da bi upravljanje rizikom bio što kvalitetniji proces treba se pazljivo i stručno analizirati i identificirati svaki rizik. Proces upravljanja rizikom:[25]

1. Procijeniti težinu mogućih gubitaka
2. Utvrditi sve izvore rizika
3. Izraditi metodu i kontrolu rizika
4. Primijeniti metode
5. Nadgledavati djelotvornost metoda

U svakom poduzeću svim zaposlenim menadžerima i rukovoditeljima posao se dijeli na više ili manje bitno. Može imati velik učinak ili nema nikakav učinak na rezultat posla. „Tako na temelju iskustva 90% poslova koje neki menadžer obavlja može imati važnosti svega 10%, tako preostalih 10% ostalih poslova mogu imati vrlo visok značaj od čak 90% važnosti. Menadžere još okružuju poslovi koji se dijele na van kontrole i pod kontrolom, sve što je pod kontrolom može se utjecati odlukama o promjeni, dok će se stvari van kontrole dogoditi a možda i ne.“ (Srića, 2003).

[23] Analiza rizika upravljanja poduzećem; Ana Udovičić, univ.spec.oec., Željka Kadlec, struč.spec.oec.; https://hrcak.srce.hr/file/175103 (pristupano 20.06.2020)
[24] Analiza rizika upravljanja poduzećem; Ana Udovičić, univ.spec.oec., Željka Kadlec, struč.spec.oec.; https://hrcak.srce.hr/file/175103 (pristupano 20.06.2020)
[25] Analiza rizika upravljanja poduzećem; Ana Udovičić, univ.spec.oec., Željka Kadlec, struč.spec.oec.; https://hrcak.srce.hr/file/175103 (pristupano 20.06.2020)

Kako bi upravljanje rizikom bilo što uspješnije koristi se sto brže i točnije mjerenje same izloženosti riziku, tehnike i metode koje su najčešće u primjeni su dinamičke i statičke, odnosno modeli. (Deželjin, 2007).

Proces upravljanja rizikom započinje strategijskim ciljevima organizacije, od izvještaja preko procjene i odlučivanja, postupanja prema riziku do samog krajnjeg nadzora. „Potreban je prevoditelj strategije poduzeća u taktičkim i operacijskim objektima kako bi menadžer i svi zaposlenici snosili odgovornost za rizik u cjelokupnom krugu poslovanja“[26]. Upravljanje rizikom nastavlja se razvijati proces pomoću kojeg se analizira strategija poduzeća i njena primjena. Sam proces mora biti ugrađen u poduzeće te zagarantiran.[27]

„Proaktivno ponašanje, poznato kao ponašanje pobjednika, dosegnut će svoju najveću učinkovitost ukoliko se usmjeri na bitno i pod kontrolom. Ako je strategija poduzeća usmjerena samo na bitno ali izvan kontrole, tada je najbolje biti prilagodljiv situaciji. Upravljanje rizikom zasniva se na analizi rizika čiji je plan rezultat djelovanja kako bi se izbjegle posljedice (Karić, 2009)“.[28]

Rizik se ne može eliminirati nego se može umanjiti. Kada upravljamo rizikom ne izbjegavamo time sami rizik već se to odnosi na unaprijed donesene odredbe za prihvaćanje rizika. Takav način donosi organizaciji dodanu vrijednost i njenim sudionicima. „Prema UK standardu postoji nekoliko točaka u svom procesu realiziranja upravljanja rizikom:“[29]

1. Stvaranje okvira za buduću aktivnost (kontrola),
2. Unaprijeđivanje odlučivanja (planiranje , projektne prilike i opasnosti , sveoobuhvatno poimanje poslovnih aktivnosti),
3. Doprinosi učinkovitijem korištenju resursa,
4. Umanjenje manje bitnih područja poslovanja
5. Čuvanje i očuvanje imovine i imidž organizacije
6. Optimizira provedbu aktivnosti

[26] Analiza rizika upravljanja poduzećem; Ana Udovičić, univ.spec.oec., Željka Kadlec, struč.spec.oec.; https://hrcak.srce.hr/file/175103 (pristupano 20.06.2020)
[27] https://hrcak.srce.hr/file/175103 (pristupano 20.06.2020)
[28] Analiza rizika upravljanja poduzećem; Ana Udovičić, univ.spec.oec., Željka Kadlec, struč.spec.oec.; https://hrcak.srce.hr/file/175103 (pristupano 20.06.2020)
[29] Analiza rizika upravljanja poduzećem; Ana Udovičić, univ.spec.oec., Željka Kadlec, struč.spec.oec.; https://hrcak.srce.hr/file/175103 (pristupano 20.06.2020)

3.2. Analiziranje rizika

Dakle, pod analizom rizika podrazumijevamo sve potrebne tehnike koje omogućavaju lakše prepoznavanje pojedinog problema te na temelju toga naći efikasnu strategiju. Za efikasnost strategije potrebno je najprije utvrditi o kakvom se riziku radi, kolika je mogućnost njegove štete te na temelju toga razvrstati vjerojatnosti bitnih faktora, njihovih utjecaja te na kraju donijeti rezultat.[30]

Analiziranje pojedinog rizika nam može pomoći u planiranju kako bi se bolje zaštitili, kategorizirati ih tako da se vidi koji od rizika se prvo treba umanjiti te koliko bi se trebalo izdvojiti za umanjenje tog rizika.[31]

Svaki moderni sustav koji se želi riješiti rizika, umanjiti ga, mora analizirati rizike pošto je to važan faktor svakog poduzeća ili organizacije[32]. Veoma je važno utvrditi postupak upravljanja rizicima na početku kako bi se moglo neprekidno baviti rizikom tokom cijelog vremenskog razdoblja. Proces analize rizika jest tehnika prepoznavanja prijetnji te se koristi izračunavanjem učinaka samih rizika te se koristi i kao instrument za upravljanje rizikom[33].

Kada se govori o investicijama koje mogu biti pod rizikom, odnosno, investicije u koje se ulaže dugoročno, potrebno je primijeniti tehniku analize rizika radi učinkovitog izvođenja kompleksnih postupaka unutar realizacije pojedine investicije.[34]

Analiza rizika uključuje:[35]

1. upravljanje rizikom,
2. komunikaciju rizika,

[30] Analiza rizika upravljanja poduzećem; Ana Udovičić, univ.spec.oec., Željka Kadlec, struč.spec.oec.; https://hrcak.srce.hr/file/175103 (pristupano 20.06.2020)
[31] Analiza rizika upravljanja poduzećem; Ana Udovičić, univ. spec. oec., Željka Kadlec, struč. spec. oec.; https://hrcak.srce.hr/118470 (pristupano 27.10.2020)
[32] https://sanitarac.pro/procjena-upravljanje-rizikom/ (pristupano 27.10.2020)
[33]Analiza rizika upravljanja poduzećem; Ana Udovičić, univ. spec. oec., Željka Kadlec, struč. spec. oec.; https://hrcak.srce.hr/118470 (pristupano 27.10.2020)
[34] Analiza rizika upravljanja poduzećem; Ana Udovičić, univ.spec.oec., Željka Kadlec, struč.spec.oec.; https://hrcak.srce.hr/file/175103 (pristupano 20.06.2020)
[35]Analiza rizika upravljanja poduzećem; Ana Udovičić, univ. spec. oec., Željka Kadlec, struč. spec. oec.; https://hrcak.srce.hr/118470 (pristupano 27.10.2020)

3. procjenu rizika.

Upravljanje rizicima je sustav koji ciljano identificira i upravlja svim učincima rizika, sa svrhom da sagleda sve pojedinačne i ukupne rizike, te ovisi o raznim činiteljima kao što su politička i ekonomska pitanja, poslovne linije i prirode poduzeća. (Olson, Wudash, 2008)

Dakle, kada se govori o komunikaciji rizika, tada se govori o razmjenjivanju informacija vezane uz štete koje bi neki rizik mogao proizvesti, dobivene informacije moraju biti nove kako bi menadžment koji odlučuje mogao vidjeti sve pozitivne te i negativne učinke.

Kada se govori o procijeni samog rizika, to znači da se mora utvrditi sam izvor od kuda bi šteta mogla nastati te kakve bi posljedice mogla izazvati[36].

3.3. Upravljanje rizicima u poduzeću

Svako poduzeće mora imati neke ciljeve ako želi uspješno poslovati, oni se mogu mijenjati ako su postavljeni na kratkoročno vremensko razdoblje. Postavljeni ciljevi poduzeća razvrstani su po hijerarhijskom modelu, tim načinom kratkoročni ciljevi vodit će prema ispunjenju dugoročnih a time i glavnih ciljeva samog poduzeća. Određen broj teoretičara smatra za prioritetan cilj poduzeća maksimalizaciju dobiti, dok drugi dio to poriče, s razlogom kako nije moguće ostvarenje takvog cilja bez dodatnih ciljeva koji ne bi ograničavali uspješnost poduzeća kao što su dobri međuljudski odnosi u poduzeću , osiguranje solventnosti, odnosno sposobnost poduzeća da podmiri sve svoje dospjele obaveze, ispunjenje društvenih obaveza i dr.. Utvrđeni ciljevi za određeni vremenski period mogu biti: (Karić, 2001)

1. Dobit koja je iskazana na uložena sredstva
2. Položaj na tržištu prikazan opsegom prodaje,
3. Proizvodnost prikaz kroz količinu usluga ili proizvoda, usluga po radniku,
4. Novi planirani razvoj proizvoda,
5. Novo planiranje o osvajanju novih tržišta i dr..

[36]Analiza rizika upravljanja poduzećem; Ana Udovičić, univ. spec. oec., Željka Kadlec, struč. spec. oec.; https://hrcak.srce.hr/118470 (pristupano 27.10.2020)

Što je poduzeće više pozicionirano na samom tržistu i samo dobro poslovanje i osiguranje privlače investitore. Kako bi poduzeće upješno poslovalo mora investirati te imati na umu rizike koji bi se mogli zadesiti te uzrokovati neku štetu na poslovanje poduzeća. Veoma je važno da menadžeri, kao glavni voditelji, razumno upravljaju investicijima te rizicima koji mogu iz njih nastati, dakle, u najekonomičnijoj mjeri. Potrebno je naglasiti ako poduzeće posluje uspješno, ako se može supotstaviti rizicima u pojedinim investicijama, biti će lakše razvijati odnose sa partnerima. U sve većoj mjeri menadžeri se moraju koristiti upravljačkim tehnikama s kojima maksimalno i racionalno iskorištavaju resurse koji su nedodirljivi. U nedodirljive resurse ubrajaju se: (Horvat i dr., 2007)

1. Podatak
2. Informacija
3. Znanje
4. Povjerenje izmedju zaposlenika i menadžera
5. Brzina
6. Fleksibilnost
7. Image (slika gospodarskog objekta u javnosti)
8. Licenca
9. Patent
10. Kvaliteta

Svako poduzeće da bi bilo uspješno mora donositi važne odluke koje se dijele na:

1. Taktičke
2. Operativne
3. Strategijske

Navedene strategije se dijele na razine menadžmenta upravlja, tako na primjer strategijskim odlukama u poduzeću upravlja glavni menađžment, a ostalima, dakle, operativnim i taktičkim odlukama upravlja menadžment za razinu niži, znaći srednjem menadžmentu, te se odluke odnose na dnevne zadaće poduzeća. Kod upravljanja poduzeća veliku ulogu imaju i kontrolori. Servisna

djelatnost glavnog, provedbenog i srednjeg menadžmenta je kontroling koja se bavi provedbenim i strateškim odlukama.[37]

Svako ulaganje donosi i neki rizik, tako postoji i rizik ulaganja glavnice u neku investiciju. Važnu sastavnicu poduzetničke djelatnosti predstavlja sama vještina vođenja menadžerstva. (Žugaj i dr., 1999).

Dakle, kada se govori o poslovnim procesima u poduzeću, bitno je znati da su oni glavni dio svakog poduzeća te da se njihovom analizom mogu ostvariti zadani ciljevi samog poduzeća. Kako bi se mogla provijeriti kontrola sustava te i kako bi se rizici u poduzeću mogli umanjiti koristi se holistička analiza. (Vukšić i dr., 2008)

3.4. Rizici u poduzeću

Kada se govori o aktivnostima poduzeća, mora se uzeti u obzir kako sve aktivnosti koje poduzeće planira, ili je već poduzelo, donosi i rizik koji može naštetiti poslovanju. (Štulec, 2010).

Rizici se mogu podijeliti na:[38]

1. Prenosivi rizik – kod ovih rizika može se ustanoviti kada bi mogli nastati i koliku štetu bi mogli napraviti
2. Neprenosivi rizik ili poslovni rizik – kod ovih rizika se ne može utvrditi kada bi mogli nastati ni koliku štetu bu mogli napraviti

Dakle, kada govorimo o poslovnim rizicima ili neprenosivim rizicima u nekom poduzeću, tada govorimo o onim rizicima koji mogu znatno naštetiti poslovanju, razlog tome je da poduzeće ne može ostvariti željeni financijski rezultat (Deželjin i dr., 1999).

Za željeni uspjeh poslovanja poduzeća, ne smije se izostaviti niti jedan rizik koji bi bitno mogao utjecati na bilo kakve poslovne aktivnosti, zato treba analizirati poslovne aktivnosti te vidjeti moguće rizike koji bi se mogli pojaviti te upropastiti željeni rezultat. Ljudski faktor igra važnu

[37] Analiza rizika upravljanja poduzećem; Ana Udovičić, univ.spec.oec., Željka Kadlec, struč.spec.oec.; https://hrcak.srce.hr/file/175103 (pristupano 20.06.2020)
[38] https://www.enciklopedija.hr/natuknica.aspx?id=53028 (pristupano 06.06.2020)

ulogu u upravljanju rizicima u poduzeću, pošto su oni izvorište znanja, oni su ti koji se koriste informacijskom tehnologijom u informacijskom sustavu, nadziru poslovne procese, stvaraju sustave te sami donose odluke u poslovnom sustavu.[39]

Dakle, da bi poduzeće ostvarilo željeni uspjeh te postiglo dobar financijski rezultat u poslovanju, potrebno je imati sustav, sustav kojim bi se upravljalo rizicima. Pošto je svaka poslovna aktivnost podložna rizicima kao što su promjene kamatnih stopa, povećanje ili smanjenje cijena materijala potrebno je uvesti sustav za upravljanje tim rizicima, on je proces u organiziciji koji prati rizike i njihove aktivnosti te tako ostvaruje stalnu dobit za poduzeće. (Miloš Sprčić, 2008).

Karakteristike upravljanja rizicima u nekom poduzeću: (Jakaša i dr., 2008)

1. dijelovi organizacijske strukture
2. proces koji upravlja rizicima
3. znanja i vještine
4. metodologije, sustavi i instrumenti

Prije svega, prije samih identifikacija rizika, poduzeće mora definirati ciljeve. Tu proizlazi sustav u poduzeću koji se bavi upravljanjem rizicima koji jamči da se ciljevi u poduzeću definiraju te da podupiru i misiju, ujedno vodeći računa o mogućim rizicima. Kada se govori o identifikaciji događaja, podrazumijevaju se bilo kakvi događaji koji bi mogli utjecati na ostvarivanje ciljeva poduzeća, a identifikaciju postižemo razlikom rizika sa mogućnosti. Na temelju svega navedenoga mogu se uočiti prilike za poduzeće u ostvarivanju njegovih ciljeva.[40]

Dakle, kada se govori o procjeni rizika, govori se procesu gdje glavni menadžment mora donijeti odluke o tome kako će, te na koji način upravljati rizicima nakon što su ustanovili o kojem se riziku radi, što znači da su proveli temeljnu analizu rizika. Kako bi se odgovorilo na rizike potrebno je uraditi razne procedure i provesti mnoge politike, odnosno kontrolne aktivnosti.[41]

[39] Analiza rizika upravljanja poduzećem; Ana Udovičić, univ.spec.oec., Željka Kadlec, struč.spec.oec.; https://hrcak.srce.hr/file/175103 (pristupano 20.06.2020)
[40] Analiza rizika upravljanja poduzećem; Ana Udovičić, univ. spec. oec., Željka Kadlec, struč. spec. oec.; https://hrcak.srce.hr/118470 (pristupano 27.10.2020)
[41]Analiza rizika upravljanja poduzećem; Ana Udovičić, univ. spec. oec., Željka Kadlec, struč. spec. oec.; https://hrcak.srce.hr/118470 (pristupano 27.10.2020)

Nadziranjem koje se postiže analizom koja je odvojena ili vođenjem računa o tijeku aktivnosti poduzeća kojom ono upravlja i nadograđivanjem sustava koji upravlja rizicima zovemo monitoring. Svaka varijabla u procesu može utjecati na neku drugu varijablu u sustavu upravljanja rizikom.[42]

Glavna razlika između klasičnog i modernog pristupa kod sustava koji upravlja rizicima je ta što kod klasičnog pristupa upravljanja rizikom, gleda na rizike kao prijetnju, dok s druge strane moderni pristup upravljanja rizikom ne gleda na rizike kao prijetnju, nego vidi i priliku u procesu upravljanja rizikom.[43]

Svaki kutak poslovanja se mora detaljno analizirati, detaljnom analizom poslovanja može se naći svaki mogući rizik koji bi mogao naštetiti poslovnim aktivnostima te tako pod temeljnom obavezom svih zaposlenika u poduzeću spada analiza poslovnih aktivnosti. Nakon analize poslovnih aktivnosti dolaze druge tehnike, ovaj korak mora biti na prvom mjestu kako bi mogli nastaviti dalje u procesu upravljanja rizikom, ne samo što je temelj za obavljanje drugih tehnika upravljanja rizikom nego i za cilj ima razumijeti samo poslovanje kao takvo te dati infromaciju na kojoj će se bazirati ostale metode.[44]

Prije nego što se krene dalje na neku drugu metodu upravljanja rizikom, mora se znati općenito o poduzeću i njegovu okružju, prepoznati opasnosti i prijetnje koje bi mogle naštetiti ciljevima poduzeća, nakon što se sve to zna, kreće definiranje rizika, gdje se svaki mogući rizik mora dokumentirati te identificirati. Pomoću adekvatnih tehnika i metoda identificiranja rizika ostvarujemo prvi korak identifikacije rizika.[45]

Analiza rizika čini poseban proces u kojemu se ostvaruje analiza svih identificiranih rizika. Kod analize rizika, dakle, potrebno je odrediti koliku prijetnju rizik može uzrokovati te na temelju

[42]Analiza rizika upravljanja poduzećem; Ana Udovičić, univ. spec. oec., Željka Kadlec, struč. spec. oec.; https://hrcak.srce.hr/118470 (pristupano 27.10.2020)
[43] Analiza rizika upravljanja poduzećem; Ana Udovičić, univ. spec. oec., Željka Kadlec, struč. spec. oec.; https://hrcak.srce.hr/118470 (pristupano 27.10.2020)
[44] Analiza rizika upravljanja poduzećem; Ana Udovičić, univ. spec. oec., Željka Kadlec, struč. spec. oec.; https://hrcak.srce.hr/118470 (pristupano 27.10.2020)
[45] Analiza rizika upravljanja poduzećem; Ana Udovičić, univ. spec. oec., Željka Kadlec, struč. spec. oec.; https://hrcak.srce.hr/118470 (pristupano 27.10.2020)

saznanja, izabrati najekonomičniju zaštitu, možemo ga izmjeriti kvantitativno i kvalitativno. Nakon svega navedenoga, treba odabrati i strategiju kojom bi mogli upravljati rizikom[46]

Proces izvještavanja o riziku:[47]

1. izvještavanje,
2. komunikacija i
3. dokumentiranje.

[46] Analiza rizika upravljanja poduzećem; Ana Udovičić, univ. spec. oec., Željka Kadlec, struč. spec. oec.; https://hrcak.srce.hr/118470 (pristupano 27.10.2020)
[47] Analiza rizika upravljanja poduzećem; Ana Udovičić, univ. spec. oec., Željka Kadlec, struč. spec. oec.; https://hrcak.srce.hr/118470 (pristupano 27.10.2020)

4. INFORMACIJSKI RIZICI

Informacijski rizici predstavljaju vjerojatnost nekog nepoželjnog događaja kao što su prijetnje koje u datim okolnostima uzrokuju štetu, umanjenje inteziteta rada informacijskog sustava, zastoj ili štetu na informacijama koje su u njemu spremljene. Postoje informatički rizici koji se odnose na intezivnu primjenu digitalnih tehnologija u organizaciji poslovanja, to su vrste informatičkih rizika (Spremić M. 2017).

Postoji više različitih informatičkih rizika: (Spremić M. 2017)

1. strateški informatički rizici; usklađenost poslovanja ti rizici ugrožavaju poslovni interes
2. provedba projekata i programa; rizik ulaganja u informacijsku tehnologiju neće se ispravno voditi ili neće kreirati nove vrijednosti
3. provedba poslovnih procesa; rizik promjene informacijske tehnologije
4. infrastrukturni informatički rizici; rizici rada, infrastrukture i opreme

Informatički rizici imaju dvojnu narav i uvijek su prisutni: (Spremić M. 2017)

1. nove poslovne prilike, dobro vođene informacijske incijative stvaraju novu vrijednost i konkurenciju
2. lošije organizirane informatičke strategije uništavaju poslovanje, ne postoje nove vrijednosti, a trošak je golem te kreiraju deficite

Kada informacijski sustav bude napadnut, obično se radi o krađi identiteta korisnika (socijalni inženjering, phishing) te napadi razrađeni s zadatkom krađe podataka, izmjeni sadržaja (upadi u računalne mreže, zlonamjerni računalni kod) (Spremić, M. 2017).

Socijalni inženjering uključuje razne načine pribavljanja lozinki za neovlašten pristup sustav a poznatiji su:

1. žrtva nesvjesno otkriva zaporku neposrednim fizičkim uvidom, naziva se „surfanje preko ramena“
2. pretraga otpada odnosno traženje po tuđem džepu s ciljem naci lozinku za pristup sustavu i sl.

Socijalni inženjering koristi metode sakupljanja informacija te metode napada mnogih grana zaštite, samu bit socijalnog inženjeringa sadrži odnos pouzdanja te izgrađivanje odnosa. Prioritet svakog napadača je da privuče povjerenje žrtve te naknadno iskorištavanje istog. Prije nego što napadač sakupi otvoreno prezentirane podatke (novine, web, vijesti) neistinito se predstavi te uporabom prikupljenih podataka napravi priču ubjedljivom (Dragičević, D. 2004.).

Tehnika socijalnog inženjeringa je Phishing koja se odnosi na aktivnosti kojima se računalni kriminalci i prevaranti koriste na način što šalju lažne elektroničke poruke, a koje izgledaju kao izvorno poslane od institucije s ciljem kako bi dobili pristup povjerljivim korisničkim podacima. Phishing jest metoda podvale te općenito metoda napada na sigurnost računala. One se mijenjaju sukladno socijalnim normama i ljudskim navikama, a danas ih već dijelimo u kategorije: (Spremić, M. 2017)

1. uvjerljivost
2. napad kroz web stranicu
3. napad zlonamjernim softverom
4. ostali napadi kao lažno predstavljanje IT kompanije

Keyloggers su hardverski ili softverski uređaji koji bilježe svaki udarac u tipkovnici , uređaji su za samog korisnika nevidljivi ali bilježe i prate sve što korisnici upisuju, zatim prikupljene podatke algoritmima šalju kriminalcima (Spremić, M. 2017).

Pri prisluškivanju, linije telefonskih uređaja ili mobilnih uređaja se prisluškuju radi prenošenja informacija kod prikupljanja zaporki. Može se tako i postaviti prislušni aparat na linije telefonskih ili mobilnih uređaja u sklopu samog računalnog centra (Dragičević, D. 2004.).

Program kojeg se ubacuje u sustav sa željom narušavanja tajnosti podataka je zlonamjerni softver ili kod koji namjerno ugrožava žrtvu. Zlonamjerni softver čini veliku opasnost računalima i mrežama. Ima ih više različitih vrsta i svi rade slično: (Datt, S. 2016)

1. krađa i prikupljanje važnih informacija poput identiteta
2. omogućavanje pristupa na daljinu s ciljem preuzimanja kontrole nad zaraženim računalom i njegovim resursima
3. izvođenje napada odbijanjem usluga, usporavanjem mreže

4. zahtjevanje otkupnine za dešifriranje i šifriranje diska
5. što je duže moguće skrivanje
6. opiranje da se ukloni od računala

Teško je popraviti štetu koju zlonamjerni softver učini. Veliki napori su potrebni kako bi se osposobilo zaraženo računalo ili da se mreža vrati u normalu.

Neki zlonamjerni softveri su: (Datt, S. 2016)

1. trojanci (trojanski konj)
2. crvi
3. špijunski program
4. virusi
5. Ransomeware i dr.

Zadatak zlonamjernog softvera, špijunskog programa, jest tajno pribavljanje bitnih, tajnih informacija, crvi se zakopavaju u sistem računala i onda ga razaraju (Datt, S. 2016).

Kombinacija socijalnog inženjeringa i zlonamjerog softvera su dobar primjer trojanca. Napadač nudi zlonamjerni softver npr. trojanac se karakterizira kao legalan softver i pokušava da tako i djeluje, te u pozadini radi zlonamjerni kod. Ucjenjivački softver (eng. Ransomware) jedan je od najopasnijih zlonamjernih softvera , to je maliciozni softver dizajniran da šifrira podatke a zatim traži otkupninu. Šifriranje je vrlo jako i tako spriječava dešifriranje u razumnom vremenu. (Datt, S. 2016).

Žrtva na kraju ima samo dvije opcije:

1. zaboraviti na podatke ako neuspješno dešifrira
2. ili da plati otkupninu

Osim napada na krađu podataka, napadi su vrlo česti na onemogućavanje rada informacijskog sustava. Spriječavanje ovlaštene primjene računalnog sustava, mreže ili programa korištenjem njihovih sredstava je napad uskraćivanjem usluga (Spremić, M. 2017).

Potrebno se vrlo dobro zaštititi od spomenutih tehnika cyber napada jer predstavljaju veliku opasnost informacijskom sustavu.

4.1. Informacijska sigurnost

Informacijska sigurnost svodi se na sigurnost informacijskog sustava i samih informacija zasebno. Svaka organizacija ili poduzeće koje se služi digitalnom tehnologijom ima probleme sa sigurnošću samih informacija kao i cijelog informacijskog sustava, te je tako izložena rizicima kao sto su informacijski rizici. Ako sustav nije dovoljno zaštićen velike štete mogu nastati i dovesti do samog zastoja poslovanja. Primjenom informacijske tehnologije u industrijskim granama čini pozitivan učinak na poslovanje. Skup metoda i zaštitnih mjera obuhvaća sigurnost cijelog informacijskog sustava i sigurnost informacija. To je kontrola kojom se štite informacije i informacijki sustav od neovlaštenog otkrivanja , upotrebe, pristupa ili promjena i uništenja. (Spremić, M. 2017).

Globalizacijom i razvojem društva informacije i informacijski sustav postali su vrijedan potencijal državnog sektora i ostalih. Stoga treba promatrati u cjelini cijelokupno društvo i informacijski prostor, usklađivanjem potreba i razlika informacijske sigurnosti u različitim društvenim područjima. Zahtjevi informacijske sigurnosti proistječu iz klasičnih zahtjeva zaštite podataka arhiviranih u državnom sektoru. (Andrijanić I., i drugi 2016)

Tri osnovna zahtjeva sigurnosti su: (Spremić, M. 2017)

1. Raspoloživost; usredotočuje se na pristupačnost informacija i podataka nadležnim osobama
2. Sigurnost; uključuje sigurnost informacija i podataka te izgrađuje uvjete za nesmetano djelovanje
3. Tajnost; usredotočuje se na privatne podatke koji su dostupni samo nadležnim korisnicima.

Sigurnosni propusti ili pogreške, narušavanje sigurnosnih zahtjeva mogu biti vrlo negativne posljedice za organizaciju.

4.2. UPRAVLJANJE RIZICIMA INFORMACIJSKOG SUSTAVA

Svođenje opasnosti koje ugrožavaju informacijski sustav na najmanju mjeru, neophodno ih je detektirati, ocijeniti i pokrenuti mjere sigurnosti. Rizik informacijskog sustava označava opasnost neke prijetnje u pojedinim uvijetima iskoristi slabost sustava. (Spremić, M. 2017)

Postupak upravljanja rizicima označava bitnu sastavnicu za uspješno djelovanje informacijskog sustava te da upravljanje rizikom bude učinkovito te kako bi procijenjeni rizik odgovarao realnom stanju sustava potrebno ga je implementirati u životni period informacijskog sustava.[48]

Životni period informacijskog sustava:[49]

1. korak uvođenja sustava
2. korak izgradnja sustava
3. korak implementiranja sustava
4. korak održavanja sustava
5. korak dispozicije sustava

U informacijskom sustavu upravljanje rizicima ima dva važna koraka: postupak umanjenja rizika i ukupni postupak analize rizika. Glavni cilj je doznati i detektirati slabosti u sustavu, procijeniti nivo opasnosti kojom su izložena sredstva i ponuditi razuman, ostvariv i troškovno efikasan način umanjivanja njihova opsega. (Spremić, M. 2017)

4.2.1. Analiza rizika

Analiza rizika informacijskog sustava:[50]

1. prepoznavanje prijetnji
2. svojstvo informacijskog sustava
3. analiza kontrola
4. prepoznavanje ranjivosti
5. analiza utjecaja

[48] Hrvatska agencija za nadzor financijskih usluga (2014.) Smjernice za primjereno upravljanje rizicima informacijskih sustava subjekata nadzora [online]. Dostupno na: https://www.hanfa.hr/objave-sasjednica/24102014_-66-sjednica-upravnog-vijeca-hanfe/, str. 23. (pristupano 26.07.2020)
[49] Information security; Stoneburner, G., Goguen, A., Feringa, A. (2002.) Risk Management Guide for Information Technology Systems. Recommendations of the National Institute of Standards and Technology. U.S. Department of Commerce: NIST [online]. NIST SP 800-30. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf (pristupano 26.07.2020)
[50] Information security; Stoneburner, G., Goguen, A., Feringa, A. (2002.) Risk Management Guide for Information Technology Systems. Recommendations of the National Institute of Standards and Technology. U.S. Department of Commerce: NIST [online]. NIST SP 800-30. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf (pristupano 26.07.2020)

6. utvrđivanje vjerojatnosti
7. utvrđivanje rizika
8. dokumentacija
9. ispitivanje i analiza

Neophodno je napraviti analizu prijetnji u informacijskom sustavu, tako di se zaustavilo pojavljivanje novog nepoželjnog događaja.

4.2.1.1. Svojstvo informacijskog sustava

Za uspješno definiranje rizika treba shvatiti sustav te okružje u kojem se nalazi. Definiranje svojstva informacijskog sustava utvrđuje obim postupaka analize rizika. Prije utvrđivanja svojstva informacijskog sustava neophodno je utvrditi informacije i sredstva u samom sustavu:[51]

1. Software
2. Hardware
3. informacije i podaci
4. sistemska sučelja
5. svrha sustava
6. IT stručnjaci i korisnici
7. neophodnost i osjetljivost podataka i sustava

Sve ostale informacije koje bi se mogle koristiti za utvrđivanje svojstva informacijskog sustava usklađene su operativnim okruženjem informacijskog sustava.

Nužne informacije mogu se pribaviti na razne načine: ankentnim upitnikom, razgovorom (eye to eye) ili pregledom dokumenata. Pomoću prikupljenih podataka i utvrđivanja svojstva informacijskog sustava kreće prepoznavanje potencijalnih prijetnji koje slijede.

[51]Information security; Stoneburner, G., Goguen, A., Feringa, A. (2002.) Risk Management Guide for Information Technology Systems. Recommendations of the National Institute of Standards and Technology. U.S. Department of Commerce: NIST [online]. NIST SP 800-30. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf (pristupano 26.07.2020)

4.2.1.2. Prepoznavanje prijetnji

Dakle, kada želimo prepoznati prijetnju, bitno je prisjetiti se ranije nepoželjnih događaja. Kada govorimo o prijetnjama, to znači da govorimo o nepoželjnim čimbenicima koji negativno djeluju na povjerljivost, integritet i dostupnost sredstava. Možemo ih podijeliti na dvije bitne skupine a to su namjerne i nenamjerne:

1. Namjerni: dakle, to su one prijetnje koje ciljano napadaju slabo razvijene sustave radi stjecanja neovlaštenog pristupa. Kao što smo prije naveli razne informacijske rizike tu spadaju navedeni trojanci i crvi.
2. Nenamjerni: tu spadaju prijetnje koje se slučajno zadese poput neke elementarne nepogode poput potresa, požara ili poplave i slično.

Veoma je važno prepoznati prijetnju te za svaku od njih odrediti podudarnost sa sredstvima u poduzeću, te kako bi one mogle utjecati na poslovni postupak.[52]

4.2.1.3. Prepoznavanje ranjivosti

Dakle, ranjivost podrazumijeva sve slabosti u sigurnosnom sustavu koje mogu doprinijeti neovlaštenu aktivnost. Može biti posljedica grešaka u postupku sustava ili propust provođenja sigurnosnih pravila. Vrlo je bitno da se kombinirano analiziraju ranjivosti i prijetnje pošto su međusobno povezani. Kada govorimo o prepoznavanju i analizi ranjivosti mora se naći način koji je najbolje provesti za njihovu potpunu analizu. Kao što su:

1. Analiza rezultata koji su od prije već analizirani rizici
2. Analiza unutrašnjih izvještaja te dokumentacija
3. Pregledavanje javnih baza ranjivosti
4. Provedba specijalnih sigurnosnih ispitivanja
5. Razgovori sa djelatnicima i programerima

[52] CARNet CERT u suradnji s LS&S; Upravljanje sigurnosnim rizicima; CCERT-PUBDOC-2003-10-44 https://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2003-10-44.pdf; str.7. i 8. (pristupano 25.10.2020)

Ova faza mora biti detaljno razrađena, te njen ishod mora sadržavati sve ranjivosti u sustavu te njihova povezivost sa prepoznavanjem prijetnji.[53]

4.2.1.4. Analiza kontrola

Ovdje je svrha analizirati kontrole koje već postoje ili će se tek početi koristiti radi sigurnosti informacijskih sredstava[54]. Koristi se radi otkrivanja pomoću detektivne kontrole, ispravljati pomoću korektivne kontrole i spriječiti pomoću preventivne kontrole neželjene događaje. To je sustav kojim se otkrivaju, ispravljaju i spriječavaju neželjenih događaja i neželjeni procesi u informacijskom sustavu. Sama bitna osnovna ideja kontrole je umanjenje očekivanih gubitaka koji bi nastali nakon neželjenih događaja ili ostvarivanja neželjenih procesa u sustavu. (Panian, Ž. 2001)

4.2.1.5. Utvrđivanje vjerojatnosti

Dakle, ovaj korak u postupku analize rizika jest utvrđivanje mogućnosti neke ranjivosti od njihovih pripadajućih zaštitnih prijetnji. Bitni faktori:[55]

1. Motiviranost i sposobnost izvora prijetnji
2. Nazočnost te efikasnost postojećih zaštitnih kontrola
3. Svojstvo ranjivosti

Kada se mogućnost ranjivosti od pojedinog izvora prijetnji treba iskazati, to bi najbolje bilo učiniti linearno:

1. Niska mogućnost izvora prijetnji je nedostatak motivacije iskorištavanje ranjivosti
2. Srednja mogućnost izvora prijetnji jest jednim dijelom motivirano za iskorištavanje
3. Visoka mogućnost izvora prijetnji je značajno motivirana za iskorištavanje ranjivosti

[53] CARNet CERT u suradnji s LS&S; Upravljanje sigurnosnim rizicima; CCERT-PUBDOC-2003-10-44 https://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2003-10-44.pdf; str.7. i 8. (pristupano 25.10.2020)
[54] CARNet CERT u suradnji s LS&S; Upravljanje sigurnosnim rizicima; CCERT-PUBDOC-2003-10-44 https://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2003-10-44.pdf; str. 9 (pristupano 25.10.2020)
[55] CARNet CERT u suradnji s LS&S; Upravljanje sigurnosnim rizicima; CCERT-PUBDOC-2003-10-44 https://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2003-10-44.pdf; str. 9 (pristupano 25.10.2020)

4.2.1.6. Analiza utjecaja

Veoma značajan korak u projektu analize rizika, ovdje vidimo gubitke ako se iskoristi neka ranjivost. Treba voditi računa o:

1. Svrsi i zadaći sredstava u poslovnom sustavu
2. Senzibilnost podataka i sredstava
3. Kritičnost sredstava

U ovom projektu se definiraju i analiziraju nepoželjne poslijedice za poduzeće ako se zadesi neki nepredvidivi događaj te i kao određivanje tehnika koje omogućavaju prezentiranje i mjerenje. Kada određujemo moguće gubitke treba uzeti u obzir nedostatke a tako i prednosti kvalitative i kvantitativne (brojevi) analize, isti im je cilj te jedina je u prikazivanju rezultata.[56]

4.2.1.7. Određivanje rizika

Najbitniji korak u cijelom projektu analize rizika do sada. Faktori koje bi trebali posmatrati:

1. Mogućnost iskorištavanja neke ranjivosti od njene prijetnje.
2. Kvaliteta te ekonomičnost zaštitnih kontrola
3. Moguće posljedice realizacije

Najlakše određivanje rizika može se utvrditi iz prethodnih koraka a to su:

1. Utvrđivanje vjerojatnosti
2. Analizom utjecaja

4.2.1.8. Ispitivanje i analiza

Kada smo ustanovili rizik za pojedina sredstva, treba analizirati te dati savjet kako umanjiti ustanovljeni rizik. Prije nego što se daje savjet za umanjenje rizika, treba razmotriti:[57]

[56] CARNet CERT u suradnji s LS&S; Upravljanje sigurnosnim rizicima; CCERT-PUBDOC-2003-10-44 https://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2003-10-44.pdf; str. 9 (pristupano 25.10.2020)
[57] CARNet CERT u suradnji s LS&S; Upravljanje sigurnosnim rizicima; CCERT-PUBDOC-2003-10-44 https://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2003-10-44.pdf; str. 9 (pristupano 25.10.2020)

1. Efikasnost kontrola
2. Troškovi održavanja
3. Pravni aspekt
4. Okruženje na poslovanje
5. Sigurnosna politika poduzeća
6. Reakcije korisnika ...

4.2.1.9. Dokumentacija

Na temelju izvršenja svih prethodnih koraka, izrađuje je dokumentacija koja sadrži rezultat. Ta dokumentacija se isporučuje glavnom menadžmentu u poslovanju, te na njima ovisi tada kako će umanjiti pojedini rizik u poduzeću, te na koji se neće ni obazirati. Dokumentacija mora biti pregledna i jednostavna za razumijevanje.[58]

4.2.2. Ublažavanje rizika

Scenariji upravljanja su:[59]

1. Prihvaćanje rizika – ovakav definirani rizik se prihvaća ukoliko se dokaže da je utrošak ulaganja u zaštitu sredstava veći nego gubitak tih istih sredstava.
2. Umanjenje rizika – za ovakav definirani rizik se primjenjuje adekvatna zaštitna kontrola
3. Izbjegavanje rizika – .ovaka se definirirani rizik ignorira
4. Podjela rizika – u slučaju provedbe ovako definiranog rizika, on sam te i troškovi se prebacuje nekom drugom poduzeću

Ublažavanje rizika se umanjuje tek toliko da zadovolji ciljeve te i potrebe poduzeća. Potpuno umanjenje rizika je veoma neisplativo. Menadžment će odlučiti kako će se umanjiti rizik nakon što ga detaljno procijene.

[58] CARNet CERT u suradnji s LS&S; Upravljanje sigurnosnim rizicima; CCERT-PUBDOC-2003-10-44 https://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2003-10-44.pdf; str. 9 (pristupano 25.10.2020)
[59] CARNet CERT u suradnji s LS&S; Upravljanje sigurnosnim rizicima; CCERT-PUBDOC-2003-10-44 https://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2003-10-44.pdf; str. 9 (pristupano 25.10.2020)

4.2.3. Kontrole informacijskog sustava

Glavni cilj kontrole informacijskog sustava jest umanjenje mogućih gubitaka zbog nekog nepoželjnog događaja ili procesa u samom sustavu.[60]

Vrste informatičkih kontrola:[61]

1. Upravljačke: ove kontrole djeluju na najvećoj razini menađmenta te su glavni dio unutarnjih kontrola poslovanja (provođenje strategije informacijskog sustava, projekta financijskog izvještavanja, provođenja zaštitne politike informacijskih sustava)
2. Aplikacijske: ove kontrole kontroliraju rad aplikacija u poslovanju, provođenje informatičkih ativnosti i servisa
3. Korektivne: ove kontrole imaju svrhu umanjiti prijetnje na minimum, saznati kako je nastao problem te automatski obavljaju instrukcije za ispravak grešaka.
4. Detektivne: ove kontrole pokazuju greške ili propuste nekog dijela informacijskog sustava
5. Preventivne: ove kontrole imaju svrhu saznati u čemu je problem, procijeniti nepoželjne događaje prije nego što nastupe.

Razvrstavaju se prema normama ili okvirima pri procjeni učinkovitosti.

4.3. Standardi i okviri informacijske sigurnosti

Prema uredu vijeća za nacionalnu sigurnost mjere informacijske sigurnosti su opća pravila zaštite podataka koja se realiziraju na fizičkoj, tehničkoj ili organizacijskoj razini. Standardi informacijske sigurnosti su organizacijske i tehničke procedure i rješenja namijenjena sustavnoj i ujednačenoj provedbi propisanih mjera informacijske sigurnosti.[62]

Dakle, sama sigurnost informacijskoga sustava čini sve one prakse koje se koriste u osiguranju radi najbolje moguće zaštite podataka te upravljanja rizicima u IT sektoru. Uključuje korištenje

[60] Računovodstveni informacijski sustavi 1.-8. Izv.prof.dr.sc. Jerko Glavaš
Bruno Mandić, mag.oec., asistent; http://www.efos.unios.hr/poslovni-informacijski-sustavi/wp-content/uploads/sites/281/2019/11/RIS-2019_2020_1-8-predavanja.pdf (pristupano 25.10.2020)
[61]Metode provedbe revizije informacijskih sustava; Methods of auditing information systems; Prof. dr. sc. Mario Spremić; zef2007_17.pdf (pristupano 25.10.2020)
[62] https://www.uvns.hr/hr/sto-su-to-mjere-i-standardi-informacijske-sigurnosti (pristupano 30.10.2020)

mjera informacijske sigurnosti u planiranju i uvođenju informacijskih sustava, upravljanje dnevnim zapisima, neprekidnost poslovanja te analizu mogućih prijetnji. Sigurnošću informacijskog sustava upravlja se tijekom cijelog životnog razdoblja istog. Sve fizičke, administrativne te tehničke mjere moraju se koristiti u skladu s propisima standarda informacijske sigurnosti. Sigurnost informacijskog sustava ne obuhvaća samo zaštitu podataka napisanih u digitalnom obliku, već i zaštićuje podatke napisane na bilo koje mediju, čak i na papiru.[63]

Prema članku 2. u narodnim novinama informacijska sigurnost je: „Informacijska sigurnost je stanje povjerljivosti, cjelovitosti i raspoloživosti podatka, koje se postiže primjenom propisanih mjera i standarda informacijske sigurnosti te organizacijskom podrškom za poslove planiranja, provedbe, provjere i dorade mjera i standarda“[64]

Prema članku 5 u NN,mjere i standardi informacijske sigurnosti obuhvaćaju:[65]

1. nadzor pristupa i postupanja s klasificiranim podacima,
2. postupanje prilikom neovlaštenog otkrivanja i gubitka klasificiranih podataka,
3. planiranje mjera prilikom izvanrednih situacija,
4. ustrojavanje posebnih fondova podataka za podatke klasificirane u Republici Hrvatskoj te za klasificirane podatke koje je predala druga država, međunarodna organizacija ili institucija s kojom Republika Hrvatska surađuje.

Prema članku 16. u pravilniku o informacijskoj sigurnosti ministartva obrane i oružanih snaga RH; NN 168/03: “Svi komunikacijsko-informacijski sustavi koji obrađuju klasificirane informacije trebaju biti štićeni primjenom sigurnosnih mjera radi postizanja povjerljivosti, integriteta i dostupnosti informacija i pratećih servisa i resursa.

Sigurnosne mjere trebaju uključiti sljedeće:[66]

1. mehanizme za pouzdanu provjeru identiteta i autentičnosti osoba koje imaju autoriziran pristup,

[63] https://www.zsis.hr/default.aspx?id=346 (pristupano 30.10.2020)
[64] https://narodne-novine.nn.hr/clanci/sluzbeni/2007_07_79_2484.html (pristupano 30.10.2020)
[65] https://narodne-novine.nn.hr/clanci/sluzbeni/2007_07_79_2484.html (pristupano 30.10.2020)
[66] http://www.propisi.hr/print.php?id=3973 (pristupano 30.10.2020)

2. mehanizme koji će osigurati dovoljno informacija za provođenje istrage o otkrivanju ili slučajnoj kompromitaciji povjerljivosti, integriteta i dostupnosti klasificiranih informacija i pratećih servisa i resursa,
3. informacije i mehanizmi kojima se kontrolira pristup sustavu trebaju biti nadzirani i štićeni pod uvjetima pod kojima se nadziru i štite informacije najvećeg stupnja tajnosti do kojih je moguć pristup putem sustava,
4. organizaciju pristupa do podataka u komunikacijsko-informacijskom sustavu temeljenu na mogućnosti pristupa isključivo samo do onih podataka koji su neophodno potrebni autoriziranim osobama za njihov rad,
5. mehanizme za verifikaciju integriteta i originalnosti informacija i pratećih servisa i resursa,
6. mehanizme za održavanje integriteta klasificiranih informacija i pratećih servisa i resursa,
7. mehanizme za održavanje dostupnosti klasificiranih informacija i pratećih servisa i resursa,
8. mehanizme za kontrolu povezivanja sustava koji obrađuju klasificirane informacije,
9. mehanizme za kontrolu pouzdanosti poduzetih mjera,
10. mehanizme za procjenu i verifikaciju pravilnog funkcioniranja zaštitnih mehanizama tijekom životnog ciklusa sustava,
11. mehanizme za istraživanje i nadzor korisničkih i sustavnih aktivnosti.“

Vrste informatičkih sigurnosti su sigurnost podataka informacijskog sustava, poslovne suradnje, fizička te sigurnosna provjera

Jedni od najpoznatijih su: ISO, COBIT i ITIL.

4.3.1. IS

ISO je nastao 1946. godine u Londonu, 65 delegata iz 25 zemalja sastalo se da bi razgovarali o budućnosti međunarodne standardizacije. 1947. godine ISO službeno postoji sa 67 tehničkih odbora, skupine stručnjaka usredotočenih na određenu temu. 1951. godine objavljen je prvi ISO standard nazvan ISO/R1:1951 standard referentna temperatura za industrijska mjerenja duljina. 2005. zajednički tehnički odbor ISO-a i IEC-a JTC1 lansira ISO/IEC 27001, standard sustava

upravljanja informacijskom sigurnošću. Kako se poduzeća sve više oslanjaju na informacijsku tehnologiju, osiguravanje sustava i minimiziranje rizika je postalo od velike važnosti. ISO 27001:2005 postao je jedan od najpopularnijih ISO standarda.[67]

ISO/IEC 27001:2013 poznatiji i kao ISO27001[68] je međunarodna norma koja utvrđuje specifikaciju za sustav upravljanja informacijskom sigurnošću (ISMS). On pomaže organizacijama u upravljanju njihovom informacijskom sigurnošću obračajući se ljudima kao resursima informacijskog sustava, procesima i tehnologiji. Njegovim certifikatom pokazuje da je organizacijski ISMS usklađen sa najboljom praksom informacijske sigurnosti. ISO 27001 kao dio serije ISO 27000 standarda informacijske sigurnosti, predstavlja okvir koji pomaže ogranizacijama da uspostave, ugrade, djeluju, ndadgledaju, pregledavaju, održavaju i kontinuirano poboljšavaju ISMS. Najnovija verzija ISO 27001 objavljena je u rujnu 2013. godine zamjenjujući verziju iz 2005. godine.[69]

ISMS je holistički pristup osiguranju povjerljivosti, integriteta i dostupnosti korporativne informacijske imovine. Sastoji se od politika, postupaka i drugih kontrola koje uključuju ljude, procese i tehnologiju. Informiran redovitim procjenama zaštite od rizika radi informacijske sigurnosti, ISMS je učinkovit pristup zasnovan na riziku i tehnološki neutralan za zaštitu organizacijske informacijske imovine.[70]

Osim ISO 27001 imamo i druge norme iz ISO 27000 serije kao što su:[71]

1. ISO27002 - daje smjernice zaorganizacijske standarde informacijske sigurnosti i prakse upravljanja informacijskom sigurnošću, uključujući odabir provedbu i upravljanje kontrolama uzimajući u obzir organizacijsko okruženje za informacijsku sigurnost
2. ISO 27003 - pruža i objašnjava smjernice o ISO 27001
3. ISO 27004 – pruža smjernice namijenjene pomaganju organizacijama u ocijenjivanju performansi informacijske sigurnosti i učinkovitosti sustava upravljanja informacijskom sigurnošću u svrhu ispunjavanja zahtjeva ISO 27001.

[67] https://www.iso.org/about-us.html#16 (pristupano 30.10.2020)
[68] https://youtu.be/io6w3Yw4q9w (pristupano 30.10.2020)
[69] https://www.itgovernance.co.uk/iso27001 (pristupano 30.10.2020)
[70] https://www.itgovernance.co.uk/iso27001 (pristupano 30.10.2020)
[71] https://www.iso.org/standard/54533.html (pristupano 30.10.2020)

4. ISO 27005 –upravljanje rizikom informacijske sigurnosti

4.3.2. COBIT

COBIT (eng. Control Objectives for Information and related Technology)[72] označava kontrolne ciljeve za informatiku i srodnu tehnologiju. Okvir koji je za upravljanje i upravljanje informacijskom tehnologijom stvorio ISACA (eng.Information System Audit and Control Association, ISACA). Dizajniran je kao potporni alat menadžerima. COBIT je temeljito prizanata smjernica koja se može primjeniti u bilo kakvoj organizaciji u bilo kojoj industriji. Osigurava kvalitetu, kontrolu i pouzdanost informacijskih sustava u organizaciji, što je ujedno i najvažniji aspekt svakog poslovanja. Koristi se svuda u svijetu u svrhu upravljanja rizicima povezanih sa informacijskom tehnologijom i njihovim procesima, on jamči cjelovitost informacijskog sustava.[73]

ISACA (eng.Information System Audit and Control Association) je započela 1967. godine od male skupine pojedinaca sa sličnim poslovima koji su vršili kontrolu u računalnim sustavima koji su postajali sve kritičniji za rad u njihovim organizacijama. Skupina je uvidjela potrebu za centraliziranim izvorom informacija i smjernica na terenu i formalizirana je 1969. godine, uključivši se kao Udruženje revizora EDP-a. 1976. godine, udruga je osnovala obrazovnu zakladu za poduzimanje opsežnih istraživačkih napora kako bi proširila znanje i vrijednost područja upravljanja i kontrole informacijske tehnologije.[74]

Poslovna orijentacija COBIT uključuje povezivanje poslovnih ciljeva sa svojom IT infrastrukturom pružanjem različitih modela koji mjere postignuće istodobno identificirajući povezane poslovne odgovornosti procesa informacijske tehnologije. Glavni fokus COBITA 4.1 ilustriran je procesno zasnovanim modelom podijeljenim u četiri specifične skupine uključujući:[75]

1. Planiranje i organizacija
2. Preuzimanje i provođenje
3. Dostavljanje i podršku

[72] https://youtu.be/Ei3-1KgjARA (pristupano 30.10.2020)
[73] https://www.simplilearn.com/what-is-cobit-significance-and-framework-rar309-article (pristupano 30.10.2020)
[74] https://www.isaca.org/why-isaca/about-us/history (pristupano 30.10.2020)
[75] https://www.simplilearn.com/what-is-cobit-significance-and-framework-rar309-article (pristupano 30.10.2020)

4. Praćenje i ocjenjivanje

COBIT 5 temelji se na pet principa koji su bitni za učinkovito upravljanje i upravljanje informacijskim sustavom u poduzeću:[76]

1. Udovoljavanje potrebama dioničara
2. Pokrivanje poduzeća od početka do kraja
3. Primjena jedinstvenog integriranog okvira
4. Omogućavanje holističkog pristupa
5. Odvajanje politika or upravljanja

Načela omogućuju organizaciji da izgradi holistički okvir za upravljanje informacijskom tehnologijom koje se temelje na sedam mogućnosti:[77]

1. Ljudi, politike i okviri
2. Procesi
3. Organizacijska struktura
4. Kultura, etika i ponašanje
5. Informacija
6. Usluge, infrastruktura i aplikacije
7. Ljudi i vještine

Principi i mogućnosti zajedno, omogućuju organizaciji da uskladi svoja ulaganja u informacijsku tehnologiju sa svojim ciljevima kako bi shvatila vrijednost svojih ulaganja.

COBIT 5 može pomoći svim organizacijama:[78]

1. Poboljšati i odražavati visokokvalitetne informacije za potporu u poslovnim odlukama
2. Učinkovito korištenje informacijske tehnologije za postizanje poslovnih ciljeva
3. Korisštenje tehnologije za promicanje operativne izvrnosti
4. Osiguranje da organizacije shvate vrijednosti ulaganja u informacijsku tehnologiju
5. Postizanje usklađivanja zakona, propisa i ugovornih sporazuma

[76] https://www.itgovernance.co.uk/cobit (pristupano 30.10.2020)
[77] https://www.itgovernance.co.uk/cobit (pristupano 30.10.2020)
[78] https://www.itgovernance.co.uk/cobit (pristupano 30.10.2020)

6. Osiguranje efektivnog upravljanja rizicima informacijske tehnologije

4.3.3. ITIL

ITIL je nastao 1980-ih kada je britanska vlada shvatila da kvaliteta njihovih IT usluga jednostavno nije bila na glasu. Središnja agencija za računala i komunikacije (CCTA) kasnije preimenovana u Ured državne trgovine (OGC), imala je zadatak stvoriti skup standardnih praksi koje bi mogle povezanije ujediniti IT sustave javnog i privatnog sektora. Cilj je bio razviti učinkovitiji okvir i financijski održiviji način korištenja IT sredstva.[79]

Najranija kreacija ITIL-a objavljena je krajem 80-ih. GITIM, vladino upravljanje informacijskom tehnologijom, se vrlo razlikuje od današnjeg ITIL-a, oboje dijele cilj pružanja poboljšane podrške i isporuke. Rašireno prihvaćanje okvira od državnih agencija i organizacija iz privathinh sektora Europe, a početkom ranih 90-ih ITIL je počeo mjenjati lice informacijske tehnologije, ne samo u Velikoj Britaniji i Europi, već i širom svijeta. ITIL je ubrzo prerastao u snažni katalog od 30 kniga koji je preporučivao i pružao najbolje IT prakse koje su se usredotočile i udovoljavale potrebama klijenata i poslovanja.[80]

Na prijelazu u novo tisućljeće CCTA se promijenio u OGC. 2000. godine Microsoft je također usvojio ITIL kao temelj za razvoj svog microsoftovog okvira (MOF), zajedno s prvo velikom promjenom ITIL-a, što je rezultiralo ITILv2. nova verzija bila je usredotočena na to da ITIL učini dostupniji masama, a okvir od 30 knjiga rasporedio je u devet kategorija. Tijekom sljedećih nekoliko godina, ITIL je postao standard za najbolju IT praksu i najčešće korišten alat za upravljanje IT uslugama na svijetu.[81]

2006. godine objavljen je pojmovnik ITIL-a, koji je još jednom naklonjen ITIL-ovoj predanosti da bude prijateljski naklonjen korisnicima. Sljedeće godine objavljena je treća verzija ITIL-a, ona s većim naglaskom na integraciju IT poslovanja i koja je bila usredotočena na koncept strukture

[79] https://www.itiltraining.com/blog/2018/11/06/itil-history/ (pristupano 31.10.2020)
[80] https://www.itiltraining.com/blog/2018/11/06/itil-history/ (pristupano 31.10.2020)
[81] https://www.itiltraining.com/blog/2018/11/06/itil-history/ (pristupano 31.10.2020)

životnog stila usluga. ITIL v3 sažeo je 26 procesa i funkcija u samo 5 knjiga i nakon poktretanja stekao naziv ITIL Refresh Project.[82]

U 2011-oj godini AXELOS je objavio reviziju ITIL-a koja je riješila pogreške i nedosljednosti s V3. u ovoj ažuriranoj verziji izdanja iz 2007. godine, 5 knjiga ćini katalog ITIL usluga:[83]

1. ITIL Service Strategy
2. ITIL Service Design
3. ITIL Service Transition
4. ITIL Service Operation
5. ITIL Continual Service Improvement

Ovih 5 knjiha čine osnovu za sve najbolje prakse ITIL-a širom svijeta. Od 2013. godine ITIL je u vlasništvu AXELOS Ltd – zajedničkog ulaganja Capita Plc i ureda britanske vlade.

Trenutna verzija ITIL-a pokrenuta 2019. godine V4 ima više praktičnih smjernica o tome kako koristiti ITIL, posebno u suradničkim okruženjima. To organizacijama olakšava usklađivanje ITIL-a s metodama rada DevOps, Agile i Lean. S V4, ITIL je usvojio više cijelovitije filozofije prema upravljanju uslugama čineći ga širim i uključivim za suvremeno IT okruženje. ITIL i dan danas ostaje zlatni standard za IT na globalnoj razini, zahvaljujući svojoj sposobnosti pružanja stvarnih psolovnih pogodnosti prilagođavanjem poslovnim potrebama. Kao dio ILX Grupe, vodećeg međunarodnog rješenja za profesionalno učenje i savjetovanje, ITIL Training donosi brojne prednosti ITIL-a poduzećima po svuda.[84]

[82] https://www.itiltraining.com/blog/2018/11/06/itil-history/ (pristupano 31.10.2020)
[83] https://www.itiltraining.com/blog/2018/11/06/itil-history/ (pristupano 31.10.2020)
[84] https://www.itiltraining.com/blog/2018/11/06/itil-history/ (pristupano 31.10.2020)

5. FINANCIJSKI ASPEKT UPRAVLJANJEM RIZIKA

Uobičajena formula koja se koristi za opisivanje rizika je:

RIZIK = PRIJETNJA * RANJIVOST * POSLJEDICA

Ne treba formulu shvatiti doslovno matematički, nego treba shvatiti kocenpt. Za cijelovitu matematičku formulu trebale bi postojati neke uobičajne, neutralne mjerne jedinice za definiranje prijetnje, ranjivosti ili posljedice, ali na žalost to ne postoji. Postoje neke uobičajene jedinice poput CVSS[85] za opisivanje ranjivosti, za dijelove formule, ali one ovise o okolini ili su subjektivne onima koji koriste formulu. S druge strane ako se uspije ukloniti jedan dio formule, poput dijelova prijetnje ili ranjivosti, te ga zamjeniti sa nulom, rezultat vrijednosti rizika također se smanjuje na gotovo ništa.[86]

Prvi dio formule za rizik (prijetnja x ranjivost), može se gledati kao vjerojatnost. Ta je vjerojatnost gruba mjera koja opisuje šanse da će određenu ranjivost otkriti i koristiti akter prijetnje. Iako se može ograničiti neke čimbenike, akter prijetnje je u većini slučajeva, izvan naše kontrole. Ocijena aktera prijetnje ovisi o brojnim vrijednostima, uključujući:[87]

1. Razina vještine napadača
2. Motiv
3. Prilika
4. Sposobnost

Upravljanje rizicima je sustav koji ciljano identificira i upravlja svim učincima rizika, sa svrhom da sagleda sve pojedinačne i ukupne rizike, i ovisi o raznim činiteljima kao sto su politička i ekonomska pitanja, poslovne linije i prirode poduzeca i jos mnogi drugi a dijele se i na vanjske i unutarnje čimbenike. Vanjski čimbenici su ekonomske promjene i razvoj financijskog tržišta te opasnosti koje izviru iz pravnog, politickog, tehnološkog, demografskog okruzenja i financijske

[85] CVSS (eng. The Common Vulnerability Scoring System) – pruža način za bilježenje glavnih karakteristika ranjivosti i izradu numeričke ocjene koja odražava njezinu ozbiljnost.
[86] Simplifying risk management; Koen Van Impe; 28.03.2017; https://securityintelligence.com/simplifying-risk-management/; (pristupano 10.08.2020)
[87] Simplifying risk management; Koen Van Impe; 28.03.2017; https://securityintelligence.com/simplifying-risk-management/; (pristupano 10.08.2020)

krize.Unutarnji činitelji su razne prijevare i pronevjere unutar sustava, problemi u proizvodnji , ljudski resursi.(Olson, Wudash, 2008.).

Svrha sustava za upravljanje rizikom i njegov razvoj omogućavaju sigurnost poduzeću na način da se rizik kroz razvoj prepozna i razumije te da se odredi prioritet značajnosti samog rizika. Potrebno je promatrati sve rizike kojemu je poduzeće podložno da bi menadžment poduzeća mogao odgovoriti na vrijeme te umanjio moguće rizike.[88]

Kada govorimo o upravljanju rizikom, treba obuhvaćati: (AIRMIC, Alarm, IRM, 2010.):

1. procjenu rizika;
2. identificiranje te prepoznavanje rizika;
3. ocjenu rizika;
4. te odgovoriti na rizike;
   - tolerancijom,
   - tretiranjem,
   - transferom,
   - uklanjanjem,
5. kontrola izvora rizika;
6. planiranje;
7. izvještavanjem i nadzorom rizika;
8. revidiranje okvira upravljanja rizikom.

Dakle, kada se procijeni da neki rizik postoji treba započeti proces definiranja istog te razvrstati moguće rizike po njihovim vrstama i podvrstama. Rizici ne djeluju izlirano nego su u međusobnoj interakciji. Jako je bitno za upravljanjem rizikom znati koliko brzo rastem, koliko brzo se na isti može odgovoriti i protok vremena za odgovor na pojavu i učinak rizika. Osim brze reakcije, također je bitno mjeriti rizik pomoću skala koje određuju vjerojatnost nastanka, učinak i druge dimenzije. Da bi mogli odgovoriti na rizik, mora se provoditi mjerenje kvantitativnom i kvalitativnom metodom da bi se mogla izabrati najekonomičnija strategija upravljanja rizikom, te tako efikasno upravljamo poslovanjem poduzeća.[89]

[88] https://hrcak.srce.hr/file/300901 (pristupano 13.09.2020)
[89] https://hrcak.srce.hr/file/300901 (pristupano 13.09.2020)

Dijelovi sustava upravljanja rizikom:[90]

1. unutarnja kontrola,
2. postavljanje ciljeva,
3. identifikacija događaja,
4. procjena rizika,
5. odgovori na rizike,
6. aktivnosti kontrole,
7. informacije i komunikaciju,
8. nadzor.

Rani signali predstavljaju pokazatelje rizika koji upozoravaju na rast rizika, količinu izloženosti rizika pomoću kojih menadžment donosi konkretne mjere i odluke za korištenje pojedinih prilika. Govoreći o bitnim signalima, to su oni signali koji nam govore o prilikama i aktivnostima koje bi poduzeće trebalo iskoristiti ili poduzeti radi umanjenja pojedinog rizika. Ključni signali moraju uključivati sljedeće elemente (Beasly, M., Branson, B., Hancook, B., 2010.):

1. Temelj na praksi iz prošlosti,
2. Dosljedan razvoj u organizaciji ,
3. Osiguranje novog pogleda na rizike,
4. Osiguranje mjerenja kroz vremenski period i poslovnih jedinica,
5. Omogućavanje pristupa performansama preuzimatelja rizika u određenom vremenu,
6. Efikasno korištenje resursa.

Poduzeća u svojem poslovanju susreću se sa različitim vrstama rizika, zato je bitno kontinuirano raditi na razvoju upravljanja rizicima.[91]

[90] https://hrcak.srce.hr/file/300901 (pristupano 13.09.2020)
[91] https://hrcak.srce.hr/file/300901 (pristupano 13.09.2020)

5.1. Analiza i procjena rizika

Analiza rizika je proces prepoznavanja ranjivosti i prijetnji, moguće štete i protumijera,[92] te je jedna od najbitnijih i najsloženijih faza u izgradnji sustava sigurnosti informacijskih sustava. Složenost analize ovisi o riziku informacijskog sustava koji proizlazi iz inforcmacijske tehnologije odnosno korištenja informacijskih resursa i informacijskog sustava. Promjena resursa informacijskog sustava znatno utječe na rano otkrivanje rizika i svih promjena koje su nastale u sustavu ili okruženju, te ubrzava rano poduzimanje potrebnih mjera za smanjenje rizika. „Po istraživanju ISSA[93] postoji više od 70 vrsta metoda za procjenu rizika“. Dvije su osnovne metodologije pristupa procjeni rizika:[94]

1. kvantitativni, i
2. kvalitativni

Razlika je ta što kvantitativne koriste apsolutne brojčane vrijednosti dok kvalitativne koriste relativne vrijednosti parametara. Najčešće se koristi kombinacija metodologija koja ovisi o konkretnom informacijskom sustavu, no rizik se može izraziti i matematički po metodologiji NIST[95], u funkciji koja ovisi o: ranjivostima, vrjednostima resursa informacijskog sustava i prijetnjama:[96]

Rizik = f (P, R, V) (1)

gdje oznake varijabli predstavljaju:

P – prijetnje koje mogu nanijeti štetu,

R – ranjivost resursa na moguće prijetnje,

V – vrijednost resursa informacijskog sustava.

[92] https://beasthackerz.ru/hr (pristupano 15.10.2020)
[93] https://ww1.issa.int/the-issa (pristupano 15.10.2020)
[94] https://bib.irb.hr/datoteka/969022.Rad_-_Radoevi_Ivan_-_2014_DKU.pdf (pristupano 13.09.2020)
[95] https://www.nist.gov/ (pristupano 15.10.2020)
[96] https://bib.irb.hr/datoteka/969022.Rad_-_Radoevi_Ivan_-_2014_DKU.pdf (pristupano 13.09.2020)

da bi se procijenio rizik treba identificirati informacijske resurse koji suu okviru sustava upravljanja informacijskom sigurnošću (ISMS)[97]. Resursi se djele na glavne i opće.

Glavni resursi u informacijskoj imovini:[98]

1. ljudski resursi
2. podaci i dokumenti
3. programska oprema
4. sklopovska oprema
5. komunikacije

Opći resursi :prostori, klima uređaji, vanjski partneri i sl.

Nakon identifikacije resursa vrši se vrednovanje istih, na 3 sigurnosna zahtjeva : integritet, raspoloživost i povjerljivost. Za vrednovanje resursa koristi se skala koja sadrži 4 vrijednosne razine: vrlo visoka, visoka, srednja, niska. Zatim je potrebno identificirati prijetnje, ranjivost resursa i izračun rizika. Za kvalitativnu procjenu rizika najčešće se koriste matematički izrazi:[99]

Rizik = Prijetnja * Ranjivost * Posljedica (2)

ili

Rizik = Vjerojatnost * Posljedica (3)

„Vjerojatnost predstavlja mjeru pojave incidenta koja u sebi implicitno sadrži prijetnju i ranjivost. Procjena rizika prema navedenim izrazima (2) i (3), postiže se defi niranjem skala kojima se opisno defi niraju razine pojedinih varijabli, skala ocjene prijetnje, skala ocjene ranjivosti, skala ocjene posljedica i za izraz (3) skala ocjene vjerojatnosti. Vrijednosti u pojedinim skalama se mogu kretati od 0 ili 1 do određenog cijelog broja (3 ili 5 ili 8 itd). Koji raspon brojeva u skalama će se primijeniti i koja računska operacija kao što je množenje (što je u izrazima navedeno) ili neka

[97] https://www.poslovni-software.com/software/isms-information-security-management-system/530/ (pristupano 15.10.2020)
[98] https://bib.irb.hr/datoteka/969022.Rad_-_Radoevi_Ivan_-_2014_DKU.pdf (pristupano 13.09.2020)
[99] https://bib.irb.hr/datoteka/969022.Rad_-_Radoevi_Ivan_-_2014_DKU.pdf (pristupano 13.09.2020)

druga (npr. zbrajanje), zavisi od opredjeljenja same poslovne organizacije (ili profesionalne firme iz toga područja) u konkretnoj procjeni rizika.“ [100]

5.2. ZAŠTITA INFORMACIJSKIH SUSTAVA

Kompletna zaštita informacijskog sustava ne postoji, “Jedini informacijski sustav koji je zaista siguran, je onaj koji je ugašen, isključen iz napajanja, zaključan u sefu od titana, zakopan u betonski bunker, te okružen nervnim plinom i dobro plaćenima naoružanim čuvarima. Čak ni tad, ne bih se baš kladio na njega“ (dr. sc. Eugene Howard Spafford). Nakon izračuna rizika treba provesti isplativu analizu koja će biti tehnološki i financijski dostupnija kako bi se mogle donjeti važne odluke o upravljanju rizicima i mogučnosti o upravljanju rizicima:[101]

Prihvaćanje rizika – za koje ne treba poduzimati ništa jer je nizak utjecaj na funkcioniranje poslovanja pri postojećem informacijskom sustavu, ali trebaju biti redovito nadgledani ako se mjenjaju unutarnji i vanjski uvijeti rada i promjene suvremene tehnologije u radu jer se rizici u promjenjivim okolnostima mogu povećati i postati opasni.

Umanjenje rizika – provode se razne mjere i postupci koji imaju visoku i umjerenu vrjednosnu razinu procjene rizika. Za rizike umjerene i visoke razine opasnosti koje je potrebno smanjiti treba poduzeti ažurirane norme svjetskih znanja u okviru informacijske sigurnosti i odgovarajuće mjere za zaštitu informacijskog sustava. Jedni od najpoznatijih od njih su: ISO/IEC2 - 27001, ISO/IEC – 27002 i ISO/IEC – 27005.[102]

5.3. MJERE ZA SMANJENJE RIZIKA

Kada se umanjuje rizik u poduzeću, kod svih mjera umanjenja rizika sudjeluju sve razine upravljanja i odlučivanja stručnog kadra i po potrebi angažiraju se vanjski stručni suradnici. Pod zaštitne mjere spadaju postupci i procedure osiguranja zaštite informacijskih resursa od ranjivosti informacijskih sustava od prijetnji, incidenata i drugih neželjenih događaja. Između rizika i mjere

[100] https://bib.irb.hr/datoteka/969022.Rad_-_Radoevi_Ivan_-_2014_DKU.pdf (pristupano 13.09.2020)
[101] https://bib.irb.hr/datoteka/969022.Rad_-_Radoevi_Ivan_-_2014_DKU.pdf (pristupano 13.09.2020)
[102] https://bib.irb.hr/datoteka/969022.Rad_-_Radoevi_Ivan_-_2014_DKU.pdf (pristupano 13.09.2020)

zaštite postoje određene entitetske veze, koje predstavljaju tipove entiteta sa svojim jednoznačnim pojavnostima i atributima.[103]

Te veze mogu biti:[104]

1 :1 – za jedan rizik primjenjuje se jedna mjera zaštite,

1 : n – za jedan rizik primjenjuje se više mjera zaštite,

n : 1 – za više rizika primjenjuje se jedna mjera zaštite,

n : m – za više rizika primjenjuje se više mjera zaštite.

„Složenost sustava prikazana je u obliku hijerarhijske dekompozicije (rastavljanje) na podsustave. Svaki od podsustava predstavlja sustav za sebe koji se isto tako u zavisnosti od složenosti može dekomponirati na podsustave niže razine. Brojčane oznake podsustava određuju mjesto u hijerarhijskoj dekompoziciji sustava odnosno podređenost i razinu na kojoj se dekomponiran podsustav nalazi. Na zadnjoj razini dekompozicije podsustava nalaze se elementi podsustava čije dalje rastavljanje (dekompozicija) nema funkcionalnog smisla. Svaka pojedinačna planirana i/ili implementirana mjera u zaštiti predstavlja krajnji element sustava zaštite IS. Od pouzdanosti odnosno rizika provedbe pojedinačnih mjera zaštite (krajnjih elemenata sustava) i vrste hijerarhijskih veza među podsustavima zavisi pouzdanost i rizik sustava mjera zaštite u cjelini“.[105]

„Najveći broj istraživanja i do sada prezentiranih i provjerenih metoda uglavnom se odnose na procjenu rizika sigurnosti informacijskog sustava. Na temelju te procjene definiraju se mjere zaštite IS-a. Mali je broj radova i metoda procjene rizika planiranja, implementacije i kontrole mjera zaštite informacijskih sustava odnosno sustava mjera zaštite. U ovom istraživanju se polazi od osnovnog objekta istraživanja a to je jedinična(konkretna i jedinstvena) mjera zaštite koja je krajnje dekomponirana i predstavlja elementarnu aktivnost. Pouzdanost provedbe može se zbog „atomske“ jednostavnosti pojedinačne mjere, iskazati u binarnom obliku 1 ili 0.“[106]

[103] https://bib.irb.hr/datoteka/969022.Rad_-_Radoevi_Ivan_-_2014_DKU.pdf (pristupano 13.09.2020)
[104] https://bib.irb.hr/datoteka/969022.Rad_-_Radoevi_Ivan_-_2014_DKU.pdf (pristupano 13.09.2020)
[105] https://bib.irb.hr/datoteka/969022.Rad_-_Radoevi_Ivan_-_2014_DKU.pdf (pristupano 13.09.2020)
[106] https://bib.irb.hr/datoteka/969022.Rad_-_Radoevi_Ivan_-_2014_DKU.pdf (pristupano 13.09.2020)

„Pouzdanost sustava kao skupa elementarnih mjera zaštite izravno je zavisna od provedbe svih predviđenih mjera zaštite. Svaka od mjera zaštite u svojoj implementaciji u određenom sustavu je neovisna od druge, što znači da implementacija jedne mjere ne ovisi od provedbe druge mjere. U tom slučaju pouzdanost i nepouzdanost a time i rizik sustava mjera zaštite sastavljenih pojedinačnih mjera zaštite, može se izračunati za svaki od podsustava zaštite: planiranje, implementacija i kontrola. Tako za podsustav planiranja mjera zaštite, primjenom teorije pouzdanosti se može izračunati:“[107]

Ppp = n (1) (4)

n

Npp = n (0) (5)

n

n(1) - broj mjera zaštite u podsustavu s vjerojatnošću provedbe planiranja = 1 (mjere su planirane)

n(0) - broj mjera zaštite u podsustavu s vjerojatnošću provedbe planiranja = 0 (mjere nisu planirane)

n - ukupan broj mjera u promatranom sustavu (podsustavu) mjera zaštite

Ppp - pouzdanost podsustava planiranja mjera zaštite

Npp - nepouzdanost podsustava planiranja mjera zaštite

Rizik mjera zaštite u podsustavu planiranja, može se izračunati:

Rpp = Npp (6)

ili

Rpp = 1 – Ppp (7)

[107] https://bib.irb.hr/datoteka/969022.Rad_-_Radoevi_Ivan_-_2014_DKU.pdf (pristupano 13.09.2020)

„Na ovaj način može se izračunati rizik mjera zaštite za svaki od preostalih podsustava: implementacija (Rpi) i kontrola (Rpk). Ovo je vrlo važan zaključak iz razloga što se na ovaj način osigurava nadležnost a time i odgovornost u sustavu mjera zaštite kao cjeline.“[108]

„Po izračunu pouzdanosti pojedinih podsustava može se izračunati i pouzdanost cijelog sustava mjera zaštite IS-a. Pri tome je važno provesti funkcionalnu zavisnost između pojedinih podsustava mjera zaštite. U složenom informacijskom sustavu po svim mjerilima složenosti (veličina poslovnog sustava, broj zaposlenih, mrežno orijentiran IS, veliki broj korisničkih računala, nekoliko server računala dr.), važno je osigurati da svaki od podsustava mjera zaštite ima svoju vrijednosnu procjenu rizika. Funkcionalna analiza međusobne povezanosti u provedbi mjera zaštite u složenim IS-a, pretpostavlja tzv. uvjetni (redni) oblik funkcionalne veze između podsustava: planiranja, implementacije i kontrole.Važno je konstatirati da svaka mjera zaštite u realizacijskom smislu pripada i zavisna je od sva tri podsustava“[109]

„Uvjetni oblik funkcionalne veze podsustava pretpostavlja da će sustav mjera zaštite ili samo jedinična mjera zaštite imati određenu vjerojatnost postojanosti samo ako njegovi svi podsustavi funkcioniraju s određenom vjerojatnošću koja je veća od nule. Odnosno ako i jedan od podsustava: plan ili implementacija ili kontrola imaju vjerojatnost realizacije 0 (nula), tada i vjerojatnost funkcioniranja sustava mjera zaštite odnosno jedinične mjere je nula. Rizik mjera zaštite u tom slučaju je najveći i iznosi 100% (1 – 0 = 1). Pod uvjetom neovisne provedbe jediničnih mjera zaštite ili podsustava, pouzdanost realizacije za uvjetni (redni) oblik njihove funkcionalne povezanosti može se izračunati prema izrazu iz teorije pouzdanosti:“[110]

P smz = Ppp * Ppi * Ppk (8)

Psmz – vjerojatnost pouzdanosti sustava mjera zaštite

Ppp – vjerojatnost pouzdanosti podsustava planiranja

Ppi – vjerojatnost pouzdanosti podsustava implementacije (provedbe)

Ppk – vjerojatnost pouzdanosti podsustava kontrole

[108] https://bib.irb.hr/datoteka/969022.Rad_-_Radoevi_Ivan_-_2014_DKU.pdf (pristupano 13.09.2020)
[109] https://bib.irb.hr/datoteka/969022.Rad_-_Radoevi_Ivan_-_2014_DKU.pdf (pristupano 13.09.2020)
[110] https://bib.irb.hr/datoteka/969022.Rad_-_Radoevi_Ivan_-_2014_DKU.pdf (pristupano 13.09.2020)

Rizik (nepouzdanost) sustava mjera zaštite, može se izračunati:

$$Rsmz = 1 - Psmz \quad (9)$$

6. ZAKLJUČAK

Informacijski sustav kao podsustav poslovnog sustava, komunicira s okolinom i od nje preuzima informacije koje tada obrađuje i tako prezentira u poslovnom sustavu što mu je i glavna svrha. U poslovni sustav ulaze i izlaze informacijski tokovi.

Informatički rizik predstavlja mogući budući nepoželjni događaj kao što je prijetnja koja u određenim okolnostima uzrokuje štetu. Sa sigurnosnog i financijskog aspekta informatičkog rizika te na temelju detaljnih istraživanja, informacijski rizici predstavljaju vjerojatnost nekog nepoželjnog događaja koji umanjuje intezitet rada, štetu na informacijama koje su u njemu spremljene i mnoge druge.

Na osnovu svega opisanog vidljivo je da nema stopostotnog sigurnosnog mehanizma za očuvanje i životni ciklus informacijskoga sustava te se može zaključiti kako se provođenjem određenih metodologija taj rizik itekako može prevenirati putem ulaganja u timove/odjele što u konačnici financijski može biti isplativije nego sanacija štete poslovanja i samog sustava.

Cilj svake tvrtke trebao bi biti pravovremeno reagiranje na opasnost te adekvatnim mjerama ublažiti rizik, a s njime i vrlo ozbiljne posljedice za samo poduzeće. Pisanjem ovoga rada upoznao sam se pobliže s metodologijama koje se u svrhu preveniranja informacijskih rizika koriste te važnost kontinuiranog ulaganja u razvoj svih potrebnih mjera za zaštitu poslovnog informacijskog sustava nekog poduzeća.

7. LITERATURA

Knjige:

1. Andrijanić, I.; Gregurek, M.; Merkaš, Z. (2016.) Upravljanje poslovnim rizicima. Zagreb: Libertas – Plejada
2. Datt, S. (2016.) Mrežna forenzika:zaštitite mrežu od unutarnjih i vanjskih ugroza, hakera i zlonamjernog softvera. Zagreb: Dobar plan
3. Dragičević, D. (2004.)Kompjutorski kriminalitet i informacijski sustavi. Zagreb: IBS
4. Horvat, Đ.; Kovačić, M.; Mlivić-Budeš, E.; Perkov, D.; Trojak, N. (2007): Temeljne funkcije upravljanja, Edukator, Zagreb
5. Karić, M. (2001):Ekonomika poduzeća, Grafika d.o.o., Osijek
6. Olson, D. L., Wu Dash, D., (2008.) Enterprises Risk Management,World Scientific Publishing Co. Pte. Ltd. Singapore
7. Panian, Ž. (2001.)Kontrola i revizija informacijskih sustava. Zagreb: Sinergija
8. Spremić, M. (2017.)Sigurnost i revizija informacijskih sustava u okruženju digitalne ekonomije. Zagreb: Ekonomski fakultet – Zagreb
9. Vukšić, VB.; Hernaus, T.; Kovačić, A. (2008): Upravljanje poslovnim procesima; organizacijski i informacijski pristup, Školska knjiga, Zagreb

Članci:

1. Štulec I., (2010): Ispitivanje utjecaja vremenskih prilika na poslovanje poduzeća u republici Hrvatskoj, Zbornik ekonomskog fakulteta u Zagrebu, godina 8., br. 2., Zagreb; Hrčak, https://hrcak.srce.hr/70781
2. Miloš Sprčić D., Tekavčić M., Šević Ž., (2008):Corporate risk management practices in Croatian companies, izvorni znanstveni rad; Hrčak; https://hrcak.srce.hr/25693
3. Jakaša T., Osmanagić Bedenik N., Iliopoulos F., (2008): Određivanje učinkovitosti sustava…, Energija, god. 57, br. 2.; Hrčak; https://hrcak.srce.hr/25939
4. Ana Udovičić, univ.spec.oec., Željka Kadlec, struč.spec.oec.;ANALIZA RIZIKA UPRAVLJANJA PODUZEĆEM; Pregledni rad; https://hrcak.srce.hr/file/175103 (pristupano 20.06.2020)

5. Prof.dr.sc. Igor Živko Ekonomski fakultet, Sveučilište u Mostaru, BiH prof.dr.sc. Zora Marijanović Ekonomski fakultet, Sveučilište u Mostaru, doc.dr.sc. Josipa Grbavac Ekonomski fakultet, Sveučilište u Mostaru, BiH; RIZICI U POSLOVANJU – UPRAVLJANJE PRISTUPOM FINANCIJA I RAČUNOVODSTVA; Pregledni rad; Hrčak; https://hrcak.srce.hr/file/300901 (pristupano 13.09.2020)
6. Prof. dr. sc. Mario Spremić; Metode provedbe revizije informacijskih sustava; Methods of auditing information systems; Prof. dr. sc. Mario Spremić; Hrčak; https://hrcak.srce.hr/file/41339 (pristupano 25.10.2020)

Internet izvori:

1. https://www.enciklopedija.hr/natuknica.aspx?id=27410 (pristupano 24.05.2020)
2. http://www.ss-strukovna-vvlatkovica-zd.skole.hr/images/pages/Nastavni_materijali/Spahic/Upotreba_IT/inf.doc (pristupano 24.05.2020)
3. http://tecajevi.freeservers.com/isuvod.htm (pristupano 24.05.2020)
4. https://www.enciklopedija.hr/natuknica.aspx?id=48887 (pristupano 26.10.2020)
5. https://www.enciklopedija.hr/natuknica.aspx?id=27405 (pristupano 26.10.2020)
6. http://www.efos.unios.hr/poslovni-informacijski-sustavi/wp-content/uploads/sites/216/2013/04/1.-POSLOVNI-INFORMACIJSKI-SUSTAVI.pdf (pristupano 26.10.2020)
7. https://www.enciklopedija.hr/natuknica.aspx?id=53028 (pristupano 06.06.2020)
8. https://www.hnb.hr/temeljne-funkcije/medunarodne-pricuve/rizici (pristupano 27.10.2020)
9. https://capital.com/hr/trzisni-rizik-definicija (pristupano 27.10.2020)
10. https://www.safu.hr/datastore/filestore/332/Upravljanje_rizicima_1.pdf (pristupano 06.06.2020)
11. https://repozitorij.unin.hr/islandora/object/unin%3A1969/datastream/PDF/view (pristupano 06.06.2020)
12. Analiza rizika upravljanja poduzećem; Ana Udovičić, univ.spec.oec., Željka Kadlec, struč.spec.oec.; https://hrcak.srce.hr/file/175103 (pristupano 20.06.2020)

13. Hrvatska agencija za nadzor financijskih usluga (2014.)Smjernice za primjereno upravljanje rizicima informacijskih sustava subjekata nadzora[online]. Dostupno na: https://www.hanfa.hr/objave-sasjednica/24102014_-66-sjednica-upravnog-vijeca-hanfe/, str. 23. (pristupano 26.07.2020)
14. Information security; Stoneburner, G., Goguen, A., Feringa, A. (2002.)Risk Management Guide for Information Technology Systems.Recommendations of the National Institute of Standards and Technology. U.S. Department of Commerce: NIST [online]. NIST SP 800-30. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf (pristupano 26.07.2020)
15. CARNet CERT u suradnji s LS&S; Upravljanje sigurnosnim rizicima; CCERT-PUBDOC-2003-10-44 https://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2003-10-44.pdf; str.7. i 8. (pristupano 25.10.2020)
16. Računovodstveni informacijski sustavi 1.-8. Izv.prof.dr.sc. Jerko Glavaš; Bruno Mandić, mag.oec., asistent; http://www.efos.unios.hr/poslovni-informacijski-sustavi/wp-content/uploads/sites/281/2019/11/RIS-2019_2020_1-8-predavanja.pdf (pristupano 25.10.2020)
17. https://www.uvns.hr/hr/sto-su-to-mjere-i-standardi-informacijske-sigurnosti (pristupano 30.10.2020)
18. https://www.zsis.hr/default.aspx?id=346 (pristupano 30.10.2020)
19. https://narodne-novine.nn.hr/clanci/sluzbeni/2007_07_79_2484.html (pristupano 30.10.2020)
20. http://www.propisi.hr/print.php?id=3973 (pristupano 30.10.2020)
21. https://www.iso.org/about-us.html#16 (pristupano 30.10.2020)
22. https://youtu.be/io6w3Yw4q9w (pristupano 30.10.2020)
23. https://www.itgovernance.co.uk/iso27001 (pristupano 30.10.2020)
24. https://www.iso.org/standard/54533.html (pristupano 30.10.2020)
25. https://youtu.be/Ei3-1KgjARA (pristupano 30.10.2020)
26. https://www.simplilearn.com/what-is-cobit-significance-and-framework-rar309-article (pristupano 30.10.2020)
27. https://www.isaca.org/why-isaca/about-us/history (pristupano 30.10.2020)
28. https://www.itgovernance.co.uk/cobit (pristupano 30.10.2020)

29. https://www.itiltraining.com/blog/2018/11/06/itil-history/ (pristupano 31.10.2020)
30. Simplifying risk management; Koen Van Impe; 28.03.2017; https://securityintelligence.com/simplifying-risk-management/; (pristupano 10.08.2020)
31. https://beasthackerz.ru/hr (pristupano 15.10.2020)
32. https://ww1.issa.int/the-issa (pristupano 15.10.2020)
33. https://www.nist.gov/ (pristupano 15.10.2020)
34. https://www.poslovni-software.com/software/isms-information-security-management-system/530/ (pristupano 15.10.2020)
35. Mr. sc. Ivan Radošević; PROCJENA RIZIKA PROVEDBE PLANIRANIH MJERA ZAŠTITE GLAVNIH RESURSA INFORMACIJSKIH SUSTAVA PRIMJENOM METODE ANKETE; Izvorni znanstveni rad / Originalscientific paper https://bib.irb.hr/datoteka/969022.Rad_-_Radoevi_Ivan_-_2014_DKU.pdf (pristupano 13.09.2020)
36. AIRMIC, Alarm, IRM, 2010.; https://www.academia.edu/12300755/A_structured_approach_to_Enterprise_Risk_Management_ERM_and_the_requirements_of_ISO_31000
37. Beasly, M., Branson, B., Hancook, B. (2010.): Developing Key Risk Indicators to Strengthen Enter prices Risk Management,Committee of Sponsoring Organizations of the Treadway Commission; https://www.coso.org/Documents/COSO-KRI-Paper-Full-FINAL-for-Web-Posting-Dec110-000.pdf
38. Perhot, D.(2011):Upravljanje rizicima metodom analitičko hijerarhijskog procesa, magistarski rad, Sveučilište u Zagrebu, Fakultet strojarstva i brodogradnje, Zagreb; https://www.fsb.unizg.hr/atlantis/upload/newsboard/10_10_2011__15630_Upravljanje_rizicima.pdf
39. Žugaj M., Šehanović J., Cingula M., (1999): Organizacija, udžbenik Sveučilišta u Zagrebu, Tiva tiskara, Varaždin; https://www.scribd.com/doc/58533997/Organizacija-poduzeca-knjiga
40. Deželjin J., (2007):Upravljanje rizikom i mjerenje izloženosti riziku, RRiF, br. 7, Zagreb; https://www.scribd.com/document/46860405/Upravljanje-Rizikom-i-Mjerenje-Izlozenosti-Riziku-10372C

europass Curriculum vitae

OSOBNE INFORMACIJE

Roso, Moris

Crnojezerska 18, 10090 Zagreb, Hrvatska.

- +385 91 1865 341

Moris_roso@hotmail.com

Spol Muško | Datum rođenja 04.03.1994 | Državljanstvo hrvatsko

ZVANJE

Stručni prvostupnik ekonomije (bacc. oec.)

RADNO ISKUSTVO

2015. – 2016.

Skladištar

DPD Croatia d.o.o.

Kovinska 4a, 10090 Zagreb, Hrvatska

Rad na traci, utovar i istovar paketa

Djelatnost ili sektor Skladište

01.08.2014. – 30.08.2014.

Stručna praksa

FINA – financijska agencija

Vrtni put 3, 10000, Zagreb

Rad u uredu, kopiranje, rad na računalu

Djelatnost ili sektor Pisarnica

2012. – 2014.

Anketar

GFK – Organizacija za istraživanje tržišta

Draškovićeva ul. 54, 10000, Zagreb

Rad u telekomunikacijskom centru, ispunjavanje anketa, rad na računalu

Djelatnost ili sektor Istraživanje tržišta

OBRAZOVANJE I OSPOSOBLJAVANJE

2016. – do sada

Financijski Menadžment

Veleučilište Baltazar Zaprešić, Ul. Vladimira Novaka 23, 10290 Zaprešić

Upravljačko računovodstvo, upravljanje obrtnim kapitalom, budžetiranje kapitala, poslovne financije poduzeća

Poslovna ekonomija i organizacija

2012. – 2016.

Veleučilište Baltazar Zaprešić, Ul, Vladimira Novaka 23, 10290 Zaprešić

Ekonomika transakcijskih troškova, marketing malog poduzeća, financijske intitucije i tržišta, osnove financija

Elektrotehničar za informatiku i računalstvo

2008. – 2012.

I. tehnička škola Tesla, Ul. Vjekoslava Klaića 7, 10000, Zagreb

OSOBNE VJEŠTINE

Materinski jezik: Hrvatski

Ostali jezici

	RAZUMIJEVANJE		GOVOR		PISANJE
	Slušanje	Čitanje	Govorna interakcija	Govorna produkcija	
Engleski	C1	B2	B2	B2	B2

Stupnjevi: A1/2: Početnik - B1/2: Samostalni korisnik - C1/2 Iskusni korisnik
Zajednički europski referentni okvir za jezike

Komunikacijske vještine
- Dobre komunikacijske vještine stečene tijekom rada u telekomunikacijskom centru

Organizacijske / rukovoditeljske vještine
- upravljanje (učio te vodio nove radnike u DPD skladištu)

Računalne vještine
- dobro vladanje alatima Microsoft Office™