Revizija informacijskih sustava

Kardašić, Marija

Sveučilište Jurja Dobrile u Puli
Fakultet ekonomije i turizma
«Dr. Mijo Mirković»

MARIJA KARDAŠIĆ

REVIZIJA INFORMACIJSKIH SUSTAVA

Završni rad

Pula, 2020.

Sveučilište Jurja Dobrile u Puli
Fakultet ekonomije i turizma
«Dr. Mijo Mirković»

MARIJA KARDAŠIĆ

REVIZIJA INFORMACIJSKIH SUSTAVA

Završni rad

JMBAG: 0303067815, redovita studentica
Studijski smjer: Informatički menadžment

Predmet: Elektroničko poslovanje
Znanstveno područje: Društvene znanosti
Znanstveno polje: Ekonomije
Znanstvena grana: Poslovna informatika
Mentorica: prof. dr. sc. Vanja Bevanda

Pula, srpanj 2020.

IZJAVA O AKADEMSKOJ ČESTITOSTI

Ja, dolje potpisani ***Marija Kardašić***, kandidat za prvostupnika ekonomije/poslovne ekonomije, smjera ***Informatički menadžment*** ovime izjavljujem da je ovaj Završni rad rezultat isključivo mojega vlastitog rada, da se temelji na mojim istraživanjima te da se oslanja na objavljenu literaturu kao što to pokazuju korištene bilješke i bibliografija. Izjavljujem da niti jedan dio Završnog rada nije napisan na nedozvoljen način, odnosno da je prepisan iz kojega necitiranog rada, te da ikoji dio rada krši bilo čija autorska prava. Izjavljujem, također, da nijedan dio rada nije iskorišten za koji drugi rad pri bilo kojoj drugoj visokoškolskoj, znanstvenoj ili radnoj ustanovi.

Student

_____

U Puli, srpanj, 2020. godine

IZJAVA

o korištenju autorskog djela

Ja, ***Marija Kardašić*** dajem odobrenje Sveučilištu Jurja Dobrile u Puli, kao nositelju prava iskorištavanja, da moj završni rad pod nazivom ***Revizija informacijskih sustava*** koristi na način da gore navedeno autorsko djelo, kao cjeloviti tekst trajno objavi u javnoj internetskoj bazi Sveučilišne knjižnice Sveučilišta Jurja Dobrile u Puli te kopira u javnu internetsku bazu završnih radova Nacionalne i sveučilišne knjižnice (stavljanje na raspolaganje javnosti), sve u skladu s Zakonom o autorskom pravu i drugim srodnim pravima i dobrom akademskom praksom, a radi promicanja otvorenoga, slobodnoga pristupa znanstvenim informacijama.

Za korištenje autorskog djela na gore navedeni način ne potražujem naknadu.

U Puli, srpanj, 2020. godine

Potpis

_____

Sadržaj

1. UVOD

Tema ovog završnog rada je *Revizija informacijskog sustava*. Informatika stalno napreduje i sve je više susrećemo u našim životima i poslovanju. Cilj rada jest upoznati se s revizijom informacijskih sustava kako bi se izbjegli složeni, neučinkoviti i nefleksibilan model funkcioniranja IT-a. Treba li provoditi reviziju informacijskih sustava?

U prvom poglavlju, objasnit će se pojam samog informacijskog sustava i mjerenje kvalitete unutar njega. Vezan je uz raznovrsno plaćanje koje obavljamo putem naših pametnih mobitela, no tako je potrebna i revizija svakog informacijskog sustava da bi se naši podaci zaštitili, a i samim time smanjili razne greške ako ih taj informacijski sustav sadrži.

Drugo poglavlje se odnosi na temu ovog završnog rada, reviziju informacijskih sustava. Objasnit će se krovni i izvedeni standardi, CobIT i ITIL, koji nam pomažu pri pružanju kvalitete usluga i unaprjeđenju upravljanja pojedinoga područja informacijskog sustava i ostalih zadataka na što se revizor mora fokusirati kako bi omogućio što bolji IS, a samim i time kako revizori informacijskih sustava primjenom raznih izvedenih standarda mogu smanjiti greške i olakšati menadžmentu pri obavljaju njihovog posla.

Treće poglavlje, provedba revizije informacijskih sustava. Objasnit će se koji su koraci i faze koje moraju prvo proći. Također, imamo primjer provedbe financijskog sektora u RH (HNB). Poslije, revizor mora prezentirati izvještaj, te je objašnjeno kako postići što bolju prezentaciju i koje se aktivnosti poslije revizije ispunjavaju.

U četvrtom poglavlju se susrećemo s planovima revizije, što bi se trebalo testirati, koji su rizici u poslovanju, koje bi se dokumentacije trebale pregledati i kontrolna područja na koje treba posvetiti pažnju.

Zadnje, primjeri revizije informacijskih sustava u stvarnom svijetu, točnije CEZIH i Oracle RSUBP-a i na što oni posvećuju pažnju prilkom njihove revizije.

2. Što je to informacijski sustav?

Informacijski sustav, organizirani skup postupaka kojima se prikupljaju, obrađuju, spremaju, pretražuju i prikazuju podatci i informacije značajni za neku organizaciju, ustanovu, društvo ili državu. Sastavni je dio informacijskoga sustava i osoblje obrazovano za rad u sustavu te odgovarajuća oprema. Današnji se informacijski sustavi pretežito ostvaruju uz pomoć suvremene informacijske i komunikacijske tehnologije.[1]

U situacijama i poslovnim sredinama gdje informacijski sustavi povezuju poslovne procese i predstavljaju temelj poslovnog modela, stvorili su se nužni infrastrukturni i organizacijski preduvjeti strateške primjene informatike u poslovanju. Suvremene digitalne i informacijske tehnologije (kao podskup informacijskih sustava) sve više se ugrađuju u postojeće proizvode, stvaraju nove potrebe i usluge, nepovratno mijenjaju poslovne procese i djelatnosti, a uporaba i učinkovito upravljanje informacijskim sustavnima čije su sastavni dio, postaju ključnim pitanjima funkcioniranja i razvitka. [2]

Prisjetimo se da danas više nije nikakvo „čudo“ niti novost plaćati parkiranje ili pak pregledavati popis najbližih slobodnih parkirališnih mjesta putem mobilnog telefona. Dapače nije niti neočekivano pozvati mobilnu aplikaciju kojom se, uz određene prostorne, tehnološke i infrastrukturne pretpostavke, moguće ostaviti svoj automobil da sam pronađe parkirno mjesto u posebno opremljenoj garaži i „javi se“ gdje je parkiran kada nam opet zatreba. Šef smjene u velikom supermarketu može šetati među policama i, zahvaljujući RFID tehnologiji, na zaslonu dlanovnika (engl. *Handheld Terminal*) bežičnim putem pregledavati obilježja proizvoda koji se na njima nalaze (koliko je stanje zalihe, kada će isteći rok trajanja pojedinom proizvodu, itd.)
Sva ta i brojna ostala obilježja suvremenih poslovnih procesa ne bi bila moguća bez učinkovite i mehanički točne primjene informacijskih sustava u poslovanju. To su sve obilježja primjene informacijskih sustava kao strateškog partnera poslovanju odnosno poslovne funkcije čija učinkovita i intenzivna primjena može doprinijeti digitalnoj transformaciji i poboljšati rezultate poslovanja (niži troškovi, diferencijacija, rast, povezivanje tvrtke s okruženjem, bolja konkurentska pozicija, inovacija modela

[1] Izvor: *Enciklopedija*, Dostupno na: http://www.enciklopedija.hr/natuknica.aspx?id=27410, [Pristupljeno: 19. kolovoza 2019.]
[2] M. Spremić, *Digitalna transformacija poslovanja,* Zagreb, Ekonomski fakultet, 2017., 204 str.

poslovanja, strateška promjena poslovnih procesa, stvaranje digitalnih poslovnih platformi, nepovratna promjena strukture u pojedinim industrijama itd.) [3]

2.1. Mjerenje učinka i kvaliteta infomacijskih sustava

Kvaliteta informacijskih sustava predstavlja relativnu kategoriju kojom se mjeri odstupanje njegove realne funkcije za idealnom (Panian, 2001.). Što je odstupanje (zaostajanje) realne funkcije sustava za idealnom manje, sustav je kvalitetniji, i obratno. Informacijski sustavi se sastoje od niza komplementarnih dijelova (hardware, software, dataware, lifeware, netware, orgware), koji koordinirano djeluju u skladu s poslovnim zahtjevima. Stoga je mjerenje kvalitete informacijskih sustava vrlo složen i zahtjevan postupak u sklopu kojega treba utvrditi idealnu funkciju sustava i pregledavati i provjeriti (revidirati) njegovu trenutnu razinu uspješnosti. Da bi se provjerila uspješnost informacijskog sustava, nužno je dobro poznavati i provjeravati uspješnost sastavnih dijelova i njihovih međudjelovanja. **Osnovni čimbenici kvalitete informacijskog sustava su:**

- infrastrukturna podrška i pripadajući softver (uređaji koji podržavaju rad informacijskog sustava, računalna oprema i komunikacijska infrastruktura zajedno sa sistemskim, aplikativnim i komunikacijskim softverom koji omogućuje njihov rad),
- podaci (transakcijski i ostali podaci, dostupnost, cjelovitost i sigurnost podataka, metode i načini pohrane i arhiviranje svih vrsta podataka),
- korištenje i utjecaj na poslovanje (funkcionalnost informacijskog sustava, učinkovitost podrške poslovnim transakcijama, djelotvornost, podrška poslovanju),
- zadovoljstvo korisnika (jednostavnost korištenja i zadovoljstvo korisnika zrelošću informatičkog sustava i podrškom provedbi poslovnih transakcija.[4]

Čimbenici kvalitete informacijskog sustava djeluju koordinirano u skladu za zahtjevima poslovanja, a sukladni su komponentama informacijskog sustava. Zakon minimuma kvalitete informacijskih sustava kaže da je kvaliteta

[3] loc. cit.
[4] ibidem str. 207

informacijskog sustava jednaka umnošku razine kvalitete svake pojedine komponetne odnosno svodi se na kvalitetu njegove najslabije komponetne. [5]

3. Objašnjenje pojma revizije informacijskih sustava

Revizija informacijskih sustava (engl. Information System Audit) je sustavni postupak kojime se ocjenjuje djeluje li informatika u skladu s poslovnim ciljevima, u kojoj mjeri djelotvorno i učinkovito podupire ciljeve poslovanja i kakva je praksa (zrelost) upravljanja i kontrole informacijskih sustava na raznim hijerhijskim razinama.[6]

Revizija informacijskih sustava je proces provjere uspješnosti informacijskih sustava obzirom na to što poslovanje od njih očekuje odnosno obzirom na mogućnosti koje njihova primjena u poslovanju pruža. Revizijama informacijskih sustava provjerava postoji li neka informatička kontrola i u kojoj je mjeri učinkovita, prikupljaju se argumenti i dokazi pomoću kojih je moguće procijeniti rizike za poslovanje i dati preporuke za njihovo smanjenje, što na kraju omogućuje bolje upravljanje informacijskih sustava kroz postupke analize njihova učinka na poslovanje i provjere njihove točnosti, učinkovitosti, djelotvornosti i pouzdanosti.[7]

Radi se o skupu složenih menadžerskih, revizorskih i tehnoloških aktivnosti kojima se pregledavaju (provjeravaju) učinci, ali i rizici uporabe informacijskih sustava i u konačnici ocjenjuje njihov utjecaj na poslovanje. To je složen proces prikupljanja i procjene dokaza temeljem kojih se može procijeniti učinkovitost i zrelost informatičkih kontrola odnosno sustavan i metodološki utemeljen postupak kojime se ocjenjuje:

- djeluje li informatika u skladu s poslovnim ciljevima,
- u kojoj mjeri djelotvorno i učinkovito podupire ciljeve poslovanja i
- kakva je praksa (zrelost) upravljanja i kontrole informacijskih sustava na raznim hijerarhijskim razinama.[8]

Na mnogim tržištima vrlo mlada struka, pa i često krivo tumačena ili pogrešno shvaćena, nastala isprva kao potopa reviziji financijskih izvještaja, revizija informacijskih sustava osim egzaktne, analitičke, danas predstavlja i suvremenu

[5] loc. cit.
[6] M. Spremić, *Digitalna transformacija poslovanja,* Zagreb, Ekonomski fakultet, 2017., 209 str.
[7] Panian, Ž., Spremić, M. *Korporativno upravljanje i revizije informacijskih sustava*, Zagreb, Zgombić i partneri, 2007.
[8] M. Spremić, *Digitalna transformacija poslovanja,* Zagreb, Ekonomski fakultet, 2017., 210 str.

savjetodavnu funkciju, desnu ruku koja menadžmentu pomaže pri (korporativnom) upravljanju informatikom.

Primjenom krovnih (CobIT) izvedenih standarda (ISO27000, ITIL, PCI DSS), revizijom informacijskih sustava moguće je metadološki utemeljeno procijeniti razinu njihove kvalitete, čime revizija postaje „analitička“ komponenta strateškog upravljanja informatikom i, kao takva, neozaobilazna pomoć menadžmentu pri vođenju informatike.[9]

Objekt revizije informacijskih sustava jest sustavno, temeljito i pažljivo pregledati kontrole unutar svih dijelova informacijskog sustava, a osnovni zadatak procijeniti njegovo trenutno stanje (zrelost, razinu uspješnosti), otkriti rizična područja, procijeniti razinu rizika i dati preporuke menadžmentu za poboljšanje prakse njegova upravljanja.[10]

Konačan rezultat tih postupaka jest **izvještaj revizora informacijskog sustava** koji se, prema područjima analize (temeljene na svjetski priznatim normama ili okvirima poput CobIT-a) sastoji od sljedećih koraka:

- analiza stanja (zrelosti) primjene informacijskih sustava u poslovanju prema propisanim područjima,
- procjena poslovnih rizika koji proizlazi iz zatečenog stanja,
- preporuka menadžmentu za poboljšanjem toga stanja uz očitavanje Uprave o provedbi.[11]

Najčešći „povod“ primjeni *integrirane revizije* informacijskih sustava jesu *regulatorni zahtjevi* (primjerice, Sarbanes-Oxley zakon, Basel II norme, smjernice Hrvatske narodne banke o upravljanju operativnim rizicima, pojedine odredbe Zakona o bankama i obveze provedbe revizije financijskih izvještaja). Pored toga, porastom važnosti primjene informacijskih sustava u poslovanju savjetodavna funkcija revizije informacijskih sustava postaje sve prisutnijom. Koristi se kako bi neovisno tijelo „snimilo“ stanje, uočilo kritične točke, procijenio rizike primjene informatike u poslovanju i dalo preporuke kako tim rizicima učinkovito upravljati. Time se, pored regulatorne koja je u mnogim zemljama obvezna, revizija informacijskih sustava sve

[9] ibidem, str. 210
[10] Spremić M., *Measuring IT Governance Performance: A Research Study on CobIT – Based Regulation Framework Usage, International Journal of Mathematics and Computers in Simulation, Volume 1,* Issue 6, pp. 17-25.
[11] loc. cit. str. 210

češće koristi i kao analitička i savjetodovana aktivnost kojom se žele poboljšati postojeća poslovna praksa.[12]

3.1. Standardi i smjernice revizije informacijskih sustava

Već dugi niz godina i desetljeća informatička struka „traži“ odgovarajuće, svjetski priznate, specifične a istodobno i dovoljno općenite profesionalne standarde koji će se opisati i propisati najbolja praksa u korištenju informacijske tehnologije. Razvoj standarda korištenja informatike može dovesti u uzročno-posljedičnu vezu s njezinim ulogama u poslovanju. Raniji informatički standardi mahom su se odnosili na korištenje informatike kao tehnološke infrastrukture. U tome su razdobljima nastali brojni tehnološki standardi i svjetske priznate norme (primjerice, OSI referentni model), kojima se uređivalo ili prepisivalo kako koristiti tehnološku infrastrukturu. Ti su standardi bili gotovo isključivo usmjereni tehnologiji i vrlo su detaljno propisivali kako se neka tehnologija treba koristiti, no vrlo su se rijetko odnosili na poslovnu stranu problema njihova korištenja. Često je njihova primjena bila upitne isplativosti jer su standardi bili slabo dostupni, skupi, a čak i njihova dosljedna primjena nije mogla jamčiti uspješne rezultate.[13]

Novim načinom standardizacije informacijski sustavi i pripadne tehnologije dostižu svoju zrelost uporabe i postaju kohezivnim elementom u strukturi organizacije, pa daljnji razvoj informatike u smjeru procesnog (uslužnog) partnera i strateškog partnera poslovanju vodi i prema razvoju potpuno novih, sveobuhvatnih i u svjetskim razmjerima vrlo aktualnih standarda i normi. Današnji, u svjetskim razmjerima i na raznim razinama organizacije najčešće korišteni standardi i norme u informatici (CobiT, ITIL, ISO 27000 norme, PCI DSS, NIST, SANS, CMMI itd.) redom su usmjereni prema koristima koje informacijski sustavi mogu donijeti u poslovanju i prema dostizanju odgovarajućih mjerljivih ciljeva usklađivanja informatike i poslovanja. Većina navedenih standarda je međusobno komplementarna, svaki ima svoje prednosti u točno određenim područjima, pa se često koristi i tzv. integrirani pristup, kada se, ovisno o revizorskom zadatku, kombiniraju područja u kojima su pojedini okviri najbolji.[14]

[12] M. Spremić, *Digitalna transformacija poslovanja,* Zagreb, Ekonomski fakultet, 2017., 211 str.
[13] ibidem, str. 212
[14] ibidem, str. 213

3.1.1. Krovni i izvedeni standardi revizije informacijskih sustava

Krovni standardi korporativnog upravljanja informatikom i revizije informacijskih sustava kako njihove analitičke funkcije na cjelovit način povezuju poslovanje i informacijske sustave, prije svega iz razloga što „pokrivaju“ brojna područja u kojima se ta usklađenost ostvaruje. Krovni standard upravljanja revizije informacijskih sustava je CobIT (engl. Control Objective for Information and Related Technology). Izvedeni standardi upravljanja informacijskim sustava i njihove revizije predstavljaju zahtjeve, norme i okvire koji su specijalizirani za upravljanje pojedinim područjem poslovnih informacijskih sustava, ali i ne i dovoljni za upravljanje cjelinom. To znači da učinkovito upravljanje pojedinim područjem informacijskih sustava ne znači i optimalno upravljanje cjelinom. Osnovna značajka izvedenih standarda upravljanja i revizije informacijskim sustavima jest da su specijalizirani za unaprjeđenje upravljanja pojedinoga područja informacijskog sustava ili njihovih dijelova, odnosno da „pokrivaju“ uže ili specifično područje upravljanja informatikom. Za razliku od CobiT-a koji je krovni standard jer na cjelovit način obuhvaća vezu između poslovanja i informatike, primjenom izvedenih standarda moguće je poboljšati praksu upravljanja informacijskim sustavima u pojedinome području.[15]

Prema područjima provjere razlikujemo sljedeće izvedene standarde korporativnog upravljanja i revizije informacijskih sustava:

- upravljanje razvojem poslovnih informacijskih sustava,
- upravljanje informatičkim uslugama,
- upravljanje ulaganjem u informatiku,
- upravljanje informatičkim rizicima,
- upravljanje sigurnošću poslovnih informacijskih sustava,
- upravljanje projektima,
- upravljanje kontinuitetom poslovanja.[16]

3.1.2. CobiT – Analitička komponenta revizije informacijskih sustava

Control Objectives for Information and Related Techologies je krovni standard korporativnog upravljanja informatikom unutar kojega se propisuju područja, procesi i pojedinačne kontrole za korporativno i operativno upravljanje

[15] ibidem, str. 214
[16] loc. cit.

informatikom. Izvorno (CobiT v1 iz 1996.) je nastao kao alat za podršku provedbe revizije financijskih izvještaja, CobiT se vrlo brzo razvijao i pratio razvoj uloge informatike u poslovanju (CobiT v2 iz 2009. već je u svjetskim razmjerima postao najkorišteniji okvir kontrole informacijskih sustava, verzija 3 iz 2004. godine je predstavljala integralni okvir upravljanja informatikom, a trenutno važeća verzija – CobiT 5 predstavlja najvažniji okvir provedbe koncepta korporativnog upravljanja informatikom), koja uključuje i neke ranije izvedene standarde.[17]

Procesno je usmjeren i obuhvaća sve komponente (područja) korporativnog upravljanja informatikom, a osnovna mu je funkcija ponuditi preporuke za usklađenje ciljeva poslovanja s ciljevima rada informatike. Promotrimo najvažnije značajke CobiT-a:

- CobiT je u svjetskim razmjerima najvažnija, krovna metodologija korporativnog upravljanja informatikom,
- CobiT je najčešće korišteni alat provedbe kontrole i revizije informacijskih sustava,
- CobiT predstavlja smjernice za analizu, mjerenje i kontrolu primjene informacijskih sustava i pripravne tehnologije u poslovanju.[18]

3.1.3. ITIL

ITIL pruža tzv. *top-down,* odnosno poslovno usmjeren pristup menadžmentu informatike koji stavlja poseban naglasak na stratešku poslovnu vrijednost informatike i potrebe da se isporuči njezina visokokvalitetna usluga (informatička usluga, IT usluga). Osim toga, ITIL pruža smjernice i preporuke koje su usmjerene radu ljudi, funkcioniranju procesa i korištenju tehnologije pri korištenju informatike i pružanju kvalitetne usluge.[19]

ITIL se sastoji od uputa temeljenih na najboljoj praksi upravljanja informatičkim uslugama u javnim i privatnim organizacijama širom svijeta. Formalno se sastoji od skupa knjiga kojima su propisane upute za pružanje kvalitetnih informatičkih usluga i procedurama, opremi i aktivnostima koje omogućuju kvalitetnu informatičku podršku.

[17] ibidem, str. 215
[18] ibidem, str. 216
[19] Spremić M., *Sigurnost i revizija informacijskih sustava u okruženju digitalne ekonomije,* Zagreb, Ekonomski fakultet, 2017. str. 210

Osim toga pruža vrlo precizne upute i smjernice kako procijeniti kvalitetu usluge, kako kontrolirati isporuku usluge i, u konačnici, kako upravljati cjelokupnom informatičkom uslugom. Vrlo je korisna mogućnost što se za svaki proces odnosno uslugu može procijeniti usklađenost s ITIL preporukama, čime se ocjenama od 0 do 5 (kao u CobiT-u) procjenjuje zrelost načina njezina korištenja, što omogućuje procjenu kvalitete cjelokupne informatičke usluge, podrške i upravljanja. ITIL je osobito korišten u Europi, najčešće u javnom sektoru (za čije potrebe i nastao) jedini trenutno važeći „standard" za upravljanje informatičkim uslugama jest ISO 20000, koji je gotovo u potpunosti preuzeo svu ITIL terminologiju i djelokrug.[20]

Jedan od poznatijih i priznatijih certifikata za revizore informacijskih sustava jest CISA.

Slika 1. Certified Information System Auditor

Izvor: *Revizija IT sustava,* Mreže (11/2012), Dostupno na: http://alterinfo.hr/fullpage.aspx?PartID=155, [Pristupljeno: 11. kolovoza 2019.]

[20] loc. cit.

4. Provedba revizije informacijskih sustava

Revizija informacijskih sustava je složen postupak sastavljen od niza koraka i faza kojima se u konačnici testiranjem učinkovitosti informatičkih kontrola prikupljaju dokazi i argumenti za procjenu poslovnog rizika (rizika kojim je poslovanje izloženo temeljem činjenice da se u provedbi poslovnih procesa koristi informacijski sustav i tehnološka podrška) i stručnu procjenu zrelosti kontrolnog okruženja. Dodana vrijednost revizije informacijskih sustava proizlazi iz preporuka za unaprjeđenjem kontrolnog okruženja kojima se nastoji poboljšati poslovna praksa, osobito izvođenje važnih poslovnih procesa i ostvarenje ciljeva poslovanja. Pri isticanju preporuka revizor informacijskih sustava treba voditi računa o:

- njihovoj provedivosti (ima li kompanija tehnoloških i ostalih znanja i sposobnosti provesti ih u djelo) i
- financijskoj isplativosti (koliko resursa mjernih mahom u vremenu i novcu treba utrošiti u provedbu i je li provedba uopće opravdana odnosno nadmašuje li trošak provedbe preporuka financijsku vrijednost rizika kojega „branimo“) i
- utvrditi odgovornu osobu i rok provedbe.[21]

Najvažniji koraci i faze provedbe revizije informacijskih sustava su:

1. Uvodni pregled – „snimka stanja“ informatike i područja revizije.
2. Određivanje područja (objekta) revizije (ŠTO revidirati? – koja područja, funkcije, procese i podatke treba provjeravati).
3. Određivanje ciljeva kontrole za svako područje.
4. Provedba testova kontrola (KAKO revidirati? – koje organizacijske, tehnološke kontrole, fizičke kontrole, korporativne, aplikativne, opće i sve ostale kontrole provjeravati).
5. Provedba detaljnih analitičkih testova.
6. Prikupljanje dokaza i procjena poslovnih rizika (preporuke).
7. Priprema i prezentiranje izvještaja revizora informacijskih sustava upravi.[22]

Razlog provedbe informacijskih sustava je potreban kako bi se smanjili niz ljudskih propusta namjernih ili nenamjernih koji se događaju. Tablica prikazuje stvarne primjere gubljenja povjerljivih podataka nekih informacijskih sustava

[21] M. Spremić, op.cit., str. 225
[22] ibidem, str. 225

Tablica 1. Gubitak povjerljivosti podataka

NEKI OD POZNATIH SIGURNOSNIH INCIDENATA		
Godina	**Organizacija**	**Opis incidenta**
2007.	TJX Companies	Zbog nezaštićene bežične mreže ukradeni podaci 94 milijuna kreditnih i debitnih kartica.
2007.	HM Revenue & Customs	Izgubljena dva diska s osobnim podacima 25 milijuna obitelji u Velikoj Britaniji.
2007.	HSBC bank	Kazna od 3,2 milijuna funti zbog gubitka podataka životnog osiguranja od 180.000 klijenata. Uzrok je izgubljeni disk u pošti na kojem podaci nisu bili kriptirani.
2008.	Bank of New York Mellon	Ukradene trake s pričuvnom pohranom podataka iz sistemske sobe. Disk je sadržavao osobne podatke 12,5 milijuna klijenata.
2009.	Heartland Payment Systems	Izgubljeno oko 130 milijuna podataka o transakcijama zbog infekcije informacijskog sustava zloćudnim kodom.
2011.	Sony Playstation Network	Ukradeno cca. 24 milijuna osobnih podataka, transakcija, zaporki i sl. korisnika Sony Playstation mreže. Gubitak se procjenjuje na 171 milijun dolara.
2001.	Dio hrvatskih telekoma	Poznati DDoS napad 21. travnja 2001. Napadnuti su hrvatski internetski poslužitelji, što je imalo za posljedicu nemogućnost pristupa Internetu na neko vrijeme.
2002.	Riječka banka	Nestalo je oko 75 milijuna eura putem transakcija koje je godinama vodio diler Riječke banke. Zakazao je kompletan sustav unutarnjih kontrola.

Izvor: *Revizija IT sustava,* Mreže (11/2012), Dostupno na: http://alterinfo.hr/fullpage.aspx?PartID=155, [Pristupljeno: 03. kolovoza 2019.]

4.1. Revizija IS u RH

Revizija informacijskih sustava polako se probija u posebnu granu ICT industrije kojoj samo fali završna potvrda u vidu formalnog državnog certifikata koji bi uveo još malo više reda u relativno dobro funkcionirajuće tržište. Naime, obrazovni je sustav obogaćen predmetima vezanim uz reviziju informacijskih sustava na većini fakulteta tehničkih znanosti, a neki od njih (npr. FOI) imaju i poseban studij posvećen upravo tome. U Hrvatskoj također djeluje Udruga za reviziju i kontrolu informacijskih sustava u sklopu koje djeluje i hrvatski ISACA ogranak, a certifikat CISA postao je *de facto* standard za revizore informacijskog sustava.[23]

[23] Izvor: *Revizija IT sustava,* Mreže (11/2012), Dostupno na: http://alterinfo.hr/fullpage.aspx?PartID=155, [Pristupljeno: 03. kolovoza 2019.]

Reviziji informacijskih sustava trenutno se najviše pažnje pruža u financijskom sektoru. Mora se priznati da Hrvatska narodna banka daje jak ritam razvoju metodologije revizije, pogotovo glede izvođenja vanjske revizije informacijskog sustava kreditnih institucija. Tako HNB redovno organizira sastanke s vanjskim revizorima informacijskih sustava na kojima se prezentiraju analize prethodnih revizija te daju očekivanja za sljedeće. Očekivanja od revizora sistematizirana su u dokumentu prema kojem je revizorsko društvo dužno sastaviti revizorsko izvješće o obavljenoj reviziji za potrebe HNB-a koje, među ostalim, mora sadržavati i informacije o provedenoj reviziji informacijskog sustava, kao i ocjenu stanja tog sustava i adekvatnosti upravljanja tim sustavom te bi trebalo kreditnoj instituciji i HNB-u pružiti kvalitetne i iscrpne informacije o rizicima kojima je taj informacijski sustav izložen.

Pritom treba naglasiti da se ovaj dokument ne može smatrati formalnom metodologijom za obavljanje revizije informacijskih sustava kreditnih institucija. Naposljetku, valja naglasiti da HNB-ova očekivanja vezana uz obavljanje revizije informacijskih sustava imaju za cilj bolje razumijevanje uloga i odgovornosti kreditnih institucija i revizorskih društava u tom procesu. Temeljni su akti, odnosno relevantna područja za reviziju informacijskog sustava kreditnih institucija:

- Odluka o primjerenom upravljanju informacijskim sustavom (ožujak 2010.),
- Zakon o kreditnim institucijama (listopad 2008. + dodaci 74/09,153/09),
- Zakon o zaštiti osobnih podataka (lipanj 2003. + dodaci 118/06,41/08,130/11),
- Odluka o eksternalizaciji (zadnje siječanj 2010.),
- Odluka o upravljanju rizicima (zadnje ožujak 2010.),
- Odluka o sadržaju revizije u kreditnim institucijama (zadnje siječanj 2009.),
- Odluka o sustavu unutarnjih kontrola (zadnje ožujak 2010.).[24]

Osim gore navedene regulative, revizija se obavlja prema najboljim svjetskim praksama za upravljanje informacijskim sustavima i informacijskom sigurnošću kao što su:

- Smjernice za upravljanje informacijskim sustavom u cilju smanjenja operativnog rizika (HNB, ožujak 2006.),
- CobiT (“Control Objectives for Information and related Technology”),

[24] Izvor: Revizija IT sustava, Mreže (11/2012), Dostupno na: http://alterinfo.hr/fullpage.aspx?PartID=155, [Pristupljeno: 11. kolovoza 2019.]

- ISO/IEC 27002:2005,
- ITIL/ISO 20000 (“Information Technology Infrastructure Library”).[25]

4.2. Priprema i planiranje revizije informacijskih sustava

Prije pokretanja samog postupka revizije informacijskih sustava, valja konkretizirati ciljeve te revizije, uzimajući u obzir razloge zbog kojih se pristupa reviziji, specifičnosti tvrtke i njenog informacijskog sustava, vrijeme i okolnosti u kojima će se revizija provoditi. Valja precizno utvrditi koja će dokumentacija biti iskorištena tijekom revizije te s kojim će ljudima u poduzeću revizori obaviti razgovore odnosno intervjue. Revizore zanimaju prvenstveno relevante činjenice. Međutim, takvih činjenica može biti izuzetno velik broj pa će u fazi pripreme biti dobro utvrditi primarni fokus revizijskog procesa. Obično će to biti snage i slabosti sustava, tj. one točke ili segmenti u kojima je sustav najjači i najslabiji. Revizori moraju dobiti u uvid u to što sustav jako radi dobro, ali isto tako i u ono što u njemu ne valja. Na temelju toga oni će izgraditi svoja očekivanja glede rezultata revizije. To nikako ne znači bilo kakvo prejudiciranje rezultata revizije, već naprosto služi za usmjeravanje gdjekad i vrlo opsežnog revizijskog procesa, čime se povećavaju izgledu da taj posao bude izvršen na najracionalniji mogući način.[26]

Reviziju informacijskih sustava treba planirati dugoročno i kratkoročno. Dugoročni planovi predstavljat će okvir za kratkoročno planiranje, tako da kratkoročni planovi ne samo da moraju biti kompatibilni s dugoročnima, već predstavljati njihovu detaljnu razradu. Za dugoročne planove treba razvijati kao prve, nakon čega će uslijediti izrada kratkoročnih planova. Ciljevi dugoročnog planiranja revizije informacijskih sustava su dvojaki:

1. Izrada općih smjernica za provedbu revizije.
2. Osiguranje odgovarajućih resursa da bi se aktivnosti u sklopu revizije mogle izvršavati djelotovorno i učinkovito.[27]

Dakle, dugoročno će planiranje biti od pomoći pri utvrđivanju fokusa (područja od posebnog interesa) revizijskih aktivnosti. Kratkoročno planiranje odnosi se na sasvim konkretan revizijski posao odnosno revizijsku kampanju. Revizijska kampanja

[25] Izvor: Revizija IT sustava, Mreže (11/2012), Dostupno na: http://alterinfo.hr/fullpage.aspx?PartID=155, [Pristupljeno: 11. kolovoza 2019.]
[26] Panian Ž., *Korporativno upravljanje i revizija informacijskih sustava,* Zagreb, Zgombić i partneri, 2007., str. 163
[27] ibidem, str. 165

je projekt koji, kao i svaki drugi projekt, mora imati točno definiran početak tijek i trajanje te završetak a cilj mu je za konkretni slučaj (primjerice, podsustav informacijskih sustava ili određenu aplikaciju) utvrditi u kojoj se mjeri uspijeva očuvati imovina, održati integritet podataka, te kakva je pritom djelotvornost i učinkovitost jedinice promatranja (podsustava, aplikacije, itd.). Pri razvijanju kratkoročnih planova revizije valja se osloniti na načela upravljanja rizicima jer će primjena tih načela diktirati opseg i realizaciju revizijskog projekta (kampanje). Valja slijediti korake procesa upravljanja rizicima koji su sljedeći:

1. *Identifikacija jedinice istraživanja.* Ranije su se tradicionalno kao jedinice istraživanja uzimale funkcionalne organizacijske jedinice (primjernice, nabava, prodaja, računovodstvo, itd.). Danas se, međutim, program upravljanja rizicima obično usmjeravaju na temeljne poslovne procese primjeri kojih su nabava materijala, likvidacija ulaznih faktura, proizvodni procesi, fakturiranje isporučene robe ili usluge kupcima, itd.
2. *Identifikacija skupa generičkih rizika svojstvenih jedinici istraživanja*. Razni izvori sugeriraju različite taksonomije (klasifikacije) rizika. Tako, primjerice, J. Erickson preporučuje podjelu na financijske i sistemske rizike,[28], dok konzultantska kuća Arthur Andersen razlikuje rizike okruženja, rizike procesa i informatičke rizike.[29] Menadžment tvrtke, u dogovoru s revizorima, odabrat će taksonomiju koja, prema njihovu mišljenju, najbolje udovoljava njihovim potrebama. Jedinstvene preporuke za taj odabir, nažalost, nema.[30]
3. *Utvrđivanje težine rizika za svaku jedinicu istraživanja*. U konteksu analize svake jedinice istraživanja treba utvrditi važnost svakog generičkog rizika iz odabrane taksonomije, koja se potom izražava njegovom težinom, odnosno ponderom.
4. *Utvrđivanje revizijskih prioriteta na temelju težine rizika.* Kada su svim rizicima pridijeljeni odgovarajući težinski faktori (ponderi), treba utvrditi prioritete za svaku jedinicu istraživanja. Takva lista prioriteta predstavljat će osnovu za planiranje i terminiranje revizijskih akcija.

[28] Erickson, John: "Integrated Risk Assessment – Part Two: Coverage, Scenarios, Yearly Review Plan and Linkage". *IS Audit & Control Journal,* br. I/1996., str. 44-48
[29] Dahliberg, Patricia: "Q&A on New Model for Information Technology Risk Management". *IS Audit & Control Journal,* br. III/1996., str. 22-26
[30] Panian Ž., *Korporativno upravljanje i revizija informacijskih sustava,* Zagreb, Zgombić i partneri, 2007., str. 165

5. *Utvrđivanje sredstava (resursa) potrebnih za izvršavanje programa revizijskih aktivnosti.* Valja utvrditi potrebe u kadrovima i financijskim sredstvima nužnima za realizaciju utvrđenog plana revizijskih aktivnosti te procijeniti trajanje revizijskog posla (kampanje). [31]

4.3. Predstavljanje (prezentacija) izvješća

U nekim ranijim vremenima vjerovalo se da je jednom napisano revizijsko izvješće potrebno još samo distributirati u pisanom obliku (tradicionalom ili elektroničkom) osobama odnosno instancama kojima je izvješće namijenjeno. No, takav je pristup danas uglavnom napušten i to iz više razloga:

1. Čitanje i analiza cjelokupnog izvješća iziskuju obično puno vremena, kojega danas nitko više nema napretek.
2. Veliko je pitanje hoće li izvješće osobe kojima je namijenjeno odista i pročitati i proanalizirati dovoljno temeljito.
3. Pitanje je također, hoće li komentari, preporuke i poruke revizora biti uvijek ispravno shvaćene.
4. Čitatelji nemaju mogućnost izravnog postavljanja pitanja revizoru i traženja eventualno potrebnih dodatnih objašnjenja.
5. Povratne informacije o reakcijima relevantnih osoba i instanci na sadržaj izvješća stižu sa zakašnjenjem, ponekad čak tako kasno da više nisu relevantne.
6. Revizor nema mogućnosti samoinicijativnog, ad hoc, nadopunjavanja ili dodatnog obrazlaganja pojedinih elemenata izvješća.
7. Revizor nema intrinzičnog zadovoljstva izravnog svjedočenja reakcijama (posebno pozitivnih) onih kojima je izvještaj namijenjen.[32]

Da bi predstavljanje izvješća bilo uspješno, revizor bi se prigodom same prezentacije trebao držati nekih pravila, među kojima su neka od važnijih sljedeća:

- Prezentaciju bi revizor trebao započeti uvodom koji će relaksirati ozračje i slušatelje.
- Treba govoriti jednostavnijim jezikom, izbjegavati izraze koje slušatelj možda neće razumijeti.

[31] ibidem, str. 166
[32] ibidem, str. 190

- Valja iznositi samo bitne činjenice, konstatacije i tvrdnje odnosno ocjene iz izvješća.
- Revizor informacijskih sustava u funkciji predstavljača svojega izvještaja mora biti samouvjeren i odrješit, dokazujući time da vlada materijom koju izlaže. No, pritom ne smije ostaviti dojam arogancije ili prepotencije, jer to kod većine slušatelja neće biti dobro prihvaćeno.
- Pri kraju prezentacije treba izložiti ono što je izloženo i pri kraju revizijskog izvješća – konačne zaključke i detaljne preporuke za akciju, po mogućnosti s naznakom prioriteta...[33]

4.4. Aktivnosti nakon rezivije informacijskih sustava

Nakon obavljenje revizije informacijskog sustava i prezentacije revizijskog izvješća, posao revizora ipak nije okončan. Naime, menadžment tvrtke trebao bi ostaviti nešto vremena svim osobama i instancama (organizacijskim jedinicama) za pomno isčitavanje i analizu revizijskog izvješća, a nakon isteka tog roka organizirati sastanak ili niz sastanaka na kojima će biti utvrđen, dogovoren i usklađen plan svih aktivnosti koje proizlaze iz nalaza i preporuke revizora.[34]

Na sastanak bi trebali bi biti pozvani – i prisustovati mu – voditelji svih organizacijskih jedinica poduzeća koje su bile obuhvaćene revizijom i svi izvršitelji poslova za koje je revizijom utvrđeno da bi trebali doživjeti određene promjene, poboljšanja, modifikacije ili unaprjeđenja. Tako će, primjernice, voditelj službe računovodstva biti pozvan onda kada su revizijom informacijskih sustava otkriveni nedostaci u zaštiti privatnosti zaposlenika prilikom obračuna plaća, a uz njega i osoba izravno angažirana na obračunu plaća. Slično tome, voditelj korisničke podrške bit će pozvan na sastanak ako je revizijom utvrđeno da stupanj zaštite integriteta podataka o reklamacijima klijenata nije zadovoljavajući, a s njim i djelatnici koji bi trebali izravno provoditi mjere kojima će se integritet podataka dovesti na potrebnu razinu.[35]

[33] ibidem, str. 191
[34] ibidem, str. 191
[35] ibidem, str. 192

5. Planovi i programi provedbe revizije učinkovitosti kontrola sigurnosti informacijskog sustava

5.1. Plan revizije strateške primjene informatike u poslovanju

Umjesto repetitivnih i rutinskih revizija temeljenih na „check-lista“ revizori bi trebali biti konzultanti poslovanju i zagovaratelji inovativne primjene informacijske tehnologije u poslovanju. Interni revizori bi trebali biti ne interni „policajci“, nego, pored CIO-a i ostalih menadžera, interni konzultanti u digitalizaciji poslovanja i nužan „korektiv“ upravi koja možda nema dovoljno znanja i kompetencije iz ovoga područja. Naravno da bi važan dio svakodnevnih aktivnosti trebale ostati redovite revizije dijelova informacijskih sustava (prema planu rada interne revizije sva ključna područja informacijskih sustava bi trebalo periodički dobro provjeriti), no one ne bi trebale biti samo usmjerene na rutinu „check-lista“ odnosno unaprijed pripremljenog skupa pitanja i kontrolnih područja koja treba „proći“ s korisnicima. Redovite revizije bi se trebale provoditi s ciljem stvaranja preduvjeta za uspješnu digitalnu transformaciju odnosno stratešku primjenu informatike u poslovanju. To znači da se revizori informacijskih sustava, osobito rukovodeće osoblje, trebaju posvetiti i strateškim revizijama odnosno provjerama poslovne prakse koja izravno utječu na ostvarenje strateških poslovnih ciljeva, ili, pak, intervenirati ako primijete da su strateški poslovni ciljevi pogrešno postavljeni jer ne uvažavaju utjecaj informatike.[36]

Najvažnije organizacijske kontrole i dokumenti kojima su propisana ključna načela koncepta korporativnoga upravljanja informatikom, a koje revizor treba detaljno proučiti su:

- Strategija informacijskog sustava,
- Strateški plan informatike,
- Strategija (metadologija, politika) ulaganja u informatiku,
- Metadologija (politika) procjene izvedivosti i isplativnosti ulaganja u informatiku,
- Metadologija (politika) upravljanja informatičkim projektima,
- Metadologija (politika) upravljanja informatičkim i cyber rizicima,
- Politika sigurnosti informacija i informacijskog sustava,

[36] Spremić M., *Sigurnost i revizija informacijskih sustava u okruženju digitalne ekonomije,* Zagreb, Ekonomski fakultet, 2017., str. 219

- Strategija kontinuiteta poslovanja i slične korporativne organizacijske kontrole.[37]

Strateška revizija odnosno revizija koncepta korporativnoga upravljanja informatikom trebala bi riješiti ili znatno utjecati na rješavanje sljedećih poslovnih problema:

- razočarenja poslovne strane neuspjelim informatičkim inicijativima, visokim IT troškovima i slabom percepcijom vrijednosti koju IT pruža poslovanju,
- složeni, neučinkovit i nefleksibilan model funkcioniranja IT-a,
- nemogućnost donošenja brzih odluka vezanih za IT,
- isključivo tehnološka preokupacija IT zaposlenika, nedostatak poslovnih znanja i kompetencija.[38]

Plan revizije logičkog pristupa informacijskome sustavu i provjere ovlasti rada (ŠTO revidirati: rizici, kontrolna područja):

Kojim rizicima će poslovanje biti izloženo u slučaju da su kontrole neučinkovite?

- neovlaštena osoba će imati pravo pristupa sustava,
- pojedinac će dobiti prekomjerna prava pristupa sustavu (podaci, aplikacijama, izvještajima, aktivnostima, ...)[39]

Dokumentaciju koju treba detaljno pregledati:

- Politika sigurnosti informacija i sigurnosti infomacijskih sustava,
- Registar informacijske imovine,
- Procedura dodjele ovlasti rada nad resursima informacijskog sustava,
- Procedura dodjele, opoziva i upravljanja privilegiranim korisničkim računima.[40]

Kontrolna područja:

- Provjeriti procedure dodjele prava pristupa (zahtjev, odobravanje, provedba, dodjela, održavanje, izmjenu i ukidanje korisničkih računa,
- Provjeriti učinkovitosti procedura stalnog nadzora korisničkog pristupa,
- Postavke lozinki, procedure upravljanja lozinkama,
- Moguće zlouporabe identiteta korisnika,

[37] loc. cit.
[38] ibidem, str. 223
[39] ibidem, str. 225
[40] ibidem, str. 225

- Jesu li promijenjene inicijalno postavljene lozinke?[41] ...

Analitički testovi učinkovitosti kontrola u području logičkoga pristupa informacijskome sustavu (KAKO revidirati):

- Provjera tehnologije logičke identifikacije (ID, PIN, korisničko ime, lozinka, pogađanje lozinki, „dictionary attacks“),
- Kontrola i zaštita – upravljanje lozinkama, složenost i duljina lozinke, ponavljajuće lozinke, neuspješne prijave...[42]

5.2. Plan revizije kontinuiteta poslovanja

Rizici za poslovanje:

- Prekid rada IS-a će uzrokovati prekid odvijanja poslovnih procesa,
- Izravna financijska i materijalna šteta + reputacijski rizik.

Dokumentaciju koju treba detaljno pregledati:

- Politika sigurnosti informacija i sigurnosti informacijskih sustava,
- Procedure arhiviranja podataka (back-up) (i svi „podređeni“ interni akti),
- Radne upute za arhiviranje podataka, radne upute za pohranu podataka itd.[43]

Primjeri analitičkih testova u području revizije kontinuiteta poslovanja:

- *Papirnati testovi* (engl. *Desk-based evaluation/paper test)* – najjedostavnija za provođenje, najjeftinija, ne provodi se stvarni oporavak procesa niti resursa informacijskog sustava,
- *Test kroz kontrolne liste* (eng. *Check list*) – provodi se prije svih ostalih testiranja. Putem testa kroz kontrolne liste pregledava se plan kontinuiteta poslovanja, provjera raspoloživost i adekvatnost informacija i resursa,
- *Test za stolom* (eng. *Tabletop testing)* – Provodi se prije testa kroz simulaciju. Pregled dokumentacije dodijeljenjih procedura i odgovornosti, upoznavanje s ciljevima i scenarijem testiranja,
- *Potpuni test* (engl. *Full operational test*). Svi postupci koje bi trebalo provesti u slučaju stvarnoga narušavanja poslovnih procesa.[44]

[41] loc. cit. str 226
[42] ibidem, str. 226
[43] ibidem, str. 231
[44] ibidem, str. 232

5.3. Plan revizije sigurnosti fizičkoga pristupa

- Smjestiti značajnu informatičku opremu u posebne prostorije,
- Osigurati kontrolu pristupa medijima za pohranu podataka koji su bez nadzora,
- Ograničiti izloženost značajne informatičke opreme prirodnim pojavama,
- Osigurati primjerenu zaštitu od požara poslovnih prostora i prostorija sa značajnom informatičkom opremom,
- Osigurati temperaturu prostorije u kojoj je smještena značajna informatička oprema primjerenu za funkcioniranje te opreme.[45]

5.4. Plan revizije promjene softvera

Rizici za poslovanje:

- nedovoljno testiran softver će se koristiti u produkciji.

Organizacijske i tehničke kontrole koje treba testirati:

- Procedura promjene softvera (zahtjev – odobrenje – testiranje – autorizacija promjene – „spuštanje“ u produkciju),
- Testni podaci, autorizacija promjena,
- Testna – razvojna – produkcijska okolina (pristup, nadzor),
- Dokumentiranje promjena (verzija softvera),
- Izvještavanje.[46]

Plan revizije u području razvoja i održavanja informacijske tehnologije i aplikacija informacijskog sustava:

- Osigurati primjereno održavanje hardvera, softvera i podržavajuće infrastrukture,
- Ograničiti ovlaštenje za izmjene na hardveru, softveru i podržavajućoj infrastrukturi,
- Primjereno nadzirati ključne pokazatelje funkcionalnosti informacijske tehnologije,
- Uključiti krajnje korisnike u proces izrade specifikacija aplikacije...[47]

[45] ibidem, str. 234
[46] ibidem, str. 234
[47] ibidem, str. 235

5.5. Plan revizije provedbe transakcija

Ciljevi revizije provedbe poslovnih transakcija se mogu svesti na pitanja poput:

- Jesu li podaci korektno obrađeni i korišteni (prijenos salda-konti – glavna knjiga)?
- Ima li praznina između evidencijama podataka?
- Postoji li mogućnost da netko neovlašten prati/mijenja/unosi podatke i programe?[48]

Plan revizije u području provedbe transakcija:

- Otkrivanje **višestrukih pojava** – npr. isti račun plaćen dva puta, isti redni broj transakcije,
- Pronalaženja **duplikata** – duplih faktura, duplih matičnih podataka dobavljača,
- Pregled **događanja po vremenskom kriteriju** – knjiženja nakon određenih datuma, knjiženje na datum 31.12., evidencija događaja nakon radnog vremena,
- **Spajanje datoteka** – Prodavač koji nije ispostavio niti jedan račun, ali ima realizaciju,
- **Pronalaženje prijevara** – zaobilaženje poslovnih pravila. (Benfordov zakon)[49]

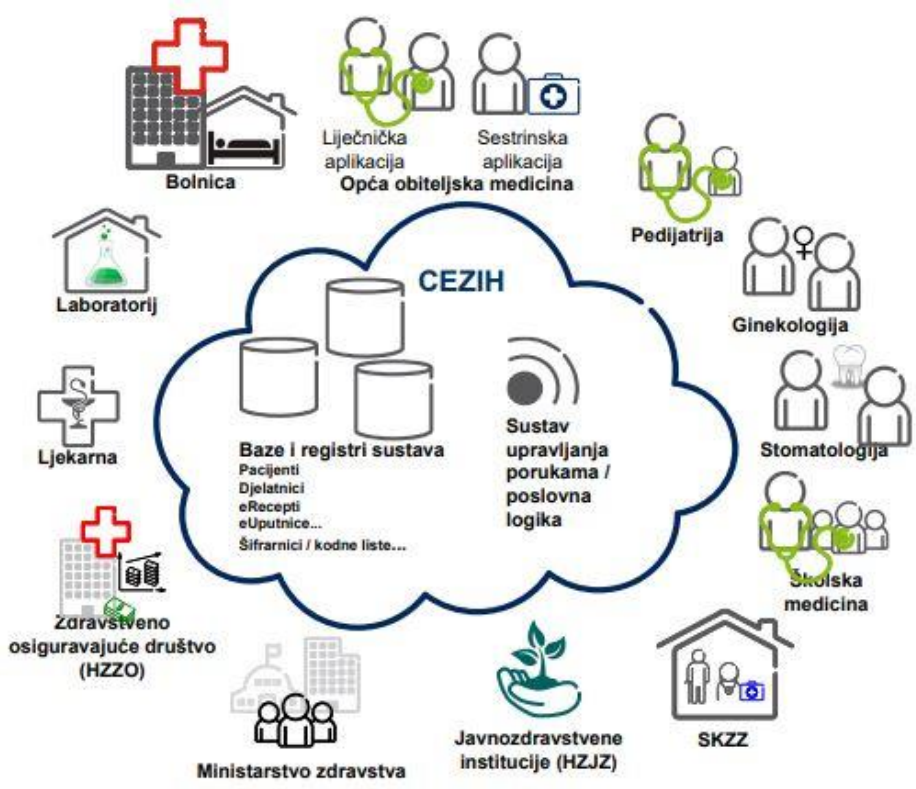
[48] ibidem, str. 236
[49] ibidem, str. 236

6. Primjeri revizije informacijskog sustava

6.1. Centralni zdravstveni informacijski sustav Republike Hrvatske (CEZIH)

CEZIH je Centralni zdravstveni informacijski sustav Republike Hrvatske koji povezuje niz aplikacija i sustava zdravstva u Republici Hrvatskoj. Ministarstvo zdravlja Republike Hrvatske je vlasnik, a Hrvatski zavod za zdravstveno osiguranje je operator središnjeg dijela integralnog informacijskog sustava CEZIH.[50]

Slika 2. Pregled CEZIH sustav



Izvor: Ministarstvo zdravlja, CEZIH, Dostupno na:
http://www.cezih.hr/pzz/dokumentacija/01_00_CEZIH_koncept_sustava.pdf
[Pristupljeno: 22. srpnja 2019.]

6.1.1. Sigurnosni sustav CEZIH

Arhitektura CEZIH rješenja u skladu je s osnovama informacijske sigurnosti i to: povjerljivosti, integritetom i dostupnošću. S obzirom na osjetljivost podatka, CEZIH

[50] Dostupno na: http://www.cezih.hr/Cesto_postavljana_pitanja.html [Pristupljeno: 22. srpnja 2019.]

rješenje primjenjuje visoke standarde vezane uz implementaciju sigurnosti. Osnovni zahtjevi visoke standarde vezane uz implementaciju sigurnosti. Osnovni zahtjevi vezani uz CEZIH rješenje su:

- povjerljivost podataka,
- kontrola pristupa,
- visoka dostupnost,
- višeslojna implementacija rješenja.

Sigurnosne značajke CEZIH sustava možemo dva segmenta. Prvi segment obuhvaća zajedničke infrastrukturne i arhitekturalne značajke dok drugi segment obuhvaća aplikativne značajke u ovisnosti o realizaciji samih aplikacija.[51]

Revizija, (eng. *audit*) svi bitni detalji vezani uz korištenje CEZIH sustava se zapisuju. Prilikom prijave na sustav zapisuju se uspješni i neuspješni slučajevi na nivou servera za kontrolu pristupa. Zapisi o pristupu bilježe se u logove na nivou svih pristupnih servera. Greške se također zapisuju na nivou svih CEZIH servera. Navedeni zapisi vrijede za oba tipa sučelja: web servise i web aplikacije. Dodatno treba napomenuti da se sve ulazne poruke na servisnom sučelju bilježe u bazu. Na taj način mogu se analizirati poruke i utvrditi potpisnici pojedinih poruka te poslanih podatka.[52]

6.2. Revizija sigurnosti Oracle RSUBP-a

Za Oracle RSUBP-a prikazuje se pristup reviziji sigurnosti Oracle BP (baze podataka).

Informacijski (pod)sustav u današnjim je poduzećima vrlo važan dio cjelokupnog poslovnog sustava. U nekim privrednim područjima, npr. bankarstvu, informacijski je sustav možda i najvažniji podsustav. Stoga se u zadnjih petnaestak godina velika pažnja posvećuje sigurnosti informacijskog sustava. Sigurnost baza podataka, kao vrlo važan dio sigurnosti informacijskog sustava, jače se naglašava zadnjih sedam-osam godina. Kod uvođenja sustava upravljanja sigurnošću informacija

[51] Ministarstvo zdravlja, *Centralni zdravstveni informacijski sustav Republike Hrvatske (CEZIH) - Koncept sustava,* 2013. Dostupno na: http://www.cezih.hr/pzz/dokumentacija/01_00_CEZIH_koncept_sustava.pdf [Pristupljeno: 22. srpnja 2019.]

[52] Ministarstvo zdravlja, *Centralni zdravstveni informacijski sustav Republike Hrvatske (CEZIH) - Koncept sustava,* 2013. Dostupno na: http://www.cezih.hr/pzz/dokumentacija/01_00_CEZIH_koncept_sustava.pdf [Pristupljeno: 22. srpnja 2019.]

(eng. Information Security Management System - ISMS) uobičajeno se primjenjuje tzv. PDCA model upravljanja (Plan-Do-Check-Act).[53]

Oracle od baze 9i intenzivno pokušava pomoći svojim korisnicima da bazu podataka učine što sigurnijom. U bazama 10.1 i 10.2 u tome su uspješno nastavili. U sadašnjim verzijama baze 11.1 i 11.2 učinili su još veći pomak nabolje. Oracle u publikaciji [9][54] (koja se odnosi na bazu 11) preporuča sljedeće:

- *Provjeriti da li je instalirano samo ono što je potrebno Instalacija*. Oracle softver moguća je na dva načina – kao tipična instalacija i kao prilagođena (custom) instalacija. Za produkcijske baze preporučljivo je odabrati prilagođenu instalaciju, te instalirati samo ono što je potrebno za rad. Ako se kasnije pokaže da je još nešto potrebno, to se lako može instalirati naknadno. U toku revizije treba provjeriti da li su instalirane samo one opcije koje su potrebne.
- *Provjeriti da li su standardni (default) korisnički računi zaključani*. Kod instalacije, automatski se kreiraju neki standardni korisnički računi. Automatska instalacija automatski zaključava te korisničke račune. Kod prilagođene instalacije, administrator bi trebao ručno zaključati te korisničke račune. U toku revizije treba provjeriti da li su standardni korisnički računi zaključani.
- *Provjeriti da li su promijenjene standardne korisničke zaporke*. U toku revizije treba provjeriti da li su promijenjene standardne (default) korisničke zaporke postavljene kod instalacije, te da li su lozinke dovoljno kompleksne (najmanje 10 znakova, mješavina slova i brojki). Provjeriti da li su zaporke privilegiranih korisničkih računa različite. U toku revizije treba provjeriti da li su zaporke privilegiranih korisničkih računa (SYSTEM, SYSMAN, DBSNMP) međusobno različite, jer nije dobro da budu jednake.
- *Provjeriti da li je sprovedeno upravljanje zaporkama pomoću profila*. U toku revizije treba provjeriti da li su pomoću profila definirani barem sljedeći parametri za upravljanje zaporkama: prekid procesa prijave nakon određenog broja neuspješnih pokušaja, definirano trajanja zaporke, definirana (ne)mogućnost ponovne upotrebe iste zaporke, definirana pravila kompleksnosti zaporki.

---

[53] Sirotić Z., *REVIZIJA SIGURNOSTI ORACLE RSUBP-a,* Dostupno na: http://www.istratech.hr/wp-content/uploads/2010/12/case2010.pdf. [Pristupljeno: 12. kolovoza 2019.]

[54] Oracle Corporation (2008): Oracle Database Security Checklist, Oracle White Paper, http://www.oracle.com/technology/deploy/security/ database-security/pdf/twp_security_checklist_database.pdf (studeni 2009.)

- *Provjeriti da li je dobro upravljana dodjela rola SYSDBA i SYSOPER.* U toku revizije treba provjeriti da li su role SYSDBA i SYSOPER date samo onim korisnicima koji to trebaju dobiti. Također, treba provjeriti da li se radi auditiranje neuspješnih prijava kao SYSDBA i SYSOPER.
- *Provjeriti da li je uključena zaštita Oracle rječnika podataka*. Oracle rječnik podataka čine (meta)tablice baze podataka. One su privilegiranim korisnicima pristupačne kao i druge tablice - mogu se ne samo čitati, već i mijenjati. Privilegirani korisnici su u ovom slučaju oni koji imaju ANY sistemske privilegije. Takve pristupe treba zabraniti. U toku revizije treba provjeriti da li je parametar 07_DICTIONARY_ACCESSIBILITY postavljen na FALSE, čime se štiti rječnik od privilegiranih korisnika.
- *Provjeriti da li se postupa u skladu s principom davanja minimalnih potrebnih prava*. U toku revizije treba provjeriti da li su dana minimalna prava za obavljanje posla, ili je dato više od toga, što nije dobro za sigurnost. Naročito treba provjeriti da li su nepotrebno date DBA privilegije – njih trebaju imati samo oni korisnici koji zaista jesu DBA administratori.[55]

[55] Sirotić Z., *REVIZIJA SIGURNOSTI ORACLE RSUBP-a,* Dostupno na: http://www.istratech.hr/wp-content/uploads/2010/12/case2010.pdf. [Pristupljeno: 12. kolovoza 2019.]

7. ZAKLJUČAK

Informacijski sustavi stalno napreduju i zahtjevaju više vremena posvećenih na njih, tako da je i sve više potrebna i revizija informacijskih sustava. Revizijama IS-a provjeravamo kolika je kontrola i u kojoj je mjeri učinkovita te time i bolje upravljamo analizama u poslovanju. Također provjeravamo točnost, pouzdanost i djelotvornost.

Razne smjernice i standardi omogućuju revizorima da se fokusiraju na preporuke za usklađenje ciljeva poslovanja s ciljevima rada informatike (CobiT) i preporuke koje su usmjerene na ljude i pružanju kvalitetne usluge (ITIL).

Provedba revizije informacijskih sustava nije lak posao, revizori moraju proučiti i pripremiti se na različite aspekte, primjerice, financijsko stanje, rok provedbe i ostale elemente kako bi osigurali isplativost, a i samim time zaštitu IS određenog poduzeća. Par koraka koji revizori moraju proći prilikom provedbe su uvodni pregled, određivanja područja revizije, provedba testova kontrole, provedba detaljnih analitičkih testova, priprema i prezentiranje izvještaja revizora upravi.

Plan revizije strateške primjene informatike u poslovanju, plan revizije kontinuiteta poslovanja, plan revizije sigurnosti fizičkoga pristupa, plan revizije promjene softvera i plan revizije provedbe transakcija su spomenuti planovi u ovom završnom radu. U nekima od njih se postavljaju pitanja na moguće poteškoće IS, primjerice - jesu li podaci korektno obrađeni i korišteni (prijenos salda-konti – glavna knjiga)? Revizori se na taj način mogu fokusirati na specifične i česte probleme koji se znaju pojaviti u ovoj vrsti poslovanja. U ostalim planovima su također razne smjernice na koji način osigurati softver i kako smanjiti tehničke poteškoće.

Primjeri revizije CEZIH sustava sigurnosne značajke svrstavaju se u dva segmenta. Prvi segment obuhvaća zajedničke infrastrukturne i arhitekturalne značajke, dok drugi segment obuhvaća aplikativne značajke u ovisnosti o realizaciji samih aplikacija. Dok Oracle primjerice daje preporuke kako bi se zaštitili, primjerice jesu li promijenjene standardne korisničke zaporke, postupa li se u skladu s principom davanja minimalnih potrebnih prava.

Prilikom pisanja ovog rada, zaključujem kako treba provoditi reviziju informacijskih sustava, ne samo zbog stalnog napredovanja poslovanja nego i izbjegavanja mogućnosti da neovlaštene osobe dobiju pristup podacima od kojih bi se mogli okorisititi, ali i ostalih rizika koje prijete poslovanju.

8. LITERATURA

KNJIGE:

1. Spremić M., *Digitalna transformacija poslovanja,* Zagreb, Ekonomski fakultet, 2017.
2. Spremić M., *Sigurnost i revizija informacijskih sustava u okruženju digitalne ekonomije,* Zagreb, Ekonomski fakultet, 2017.
3. Panian, Ž., Spremić, M. *Korporativno upravljanje i revizije informacijskih sustava*, Zagreb, Zgombić i partneri, 2007.

ČLANCI:

1. Spremić M., *Measuring IT Governance Performance: A Research Study on CobIT – Based Regulation Framework Usage, International Journal of Mathematics and Computers in Simulation, Volume 1,* Issue 6, pp. 17-25.
2. Erickson, John: "Integrated Risk Assessment – Part Two: Coverage, Scenarios, Yearly Review Plan and Linkage". IS Audit & Control Journal, br. I/1996., str. 44-48
3. Dahliberg, Patricia: "Q&A on New Model for Information Technology Risk Management". IS Audit & Control Journal, br. III/1996., str. 22-26

INTERNET IZVORI:

1. Ministarstvo zdravlja, *Centralni zdravstveni informacijski sustav Republike Hrvatske (CEZIH) - Koncept sustava,* 2013. Dostupno na: http://www.cezih.hr/pzz/dokumentacija/01_00_CEZIH_koncept_sustava.pdf [Pristupljeno: 22. srpnja 2019.]
2. CEZIH, HZZO, *Često postavljana pitanja*, dostupno na: http://www.cezih.hr/Cesto_postavljana_pitanja.html [Pristupljeno: 22. srpnja 2019.]
3. Izvor: *Revizija IT sustava,* Mreže (11/2012), Dostupno na: http://alterinfo.hr/fullpage.aspx?PartID=155, [Pristupljeno: 03.08.2019.]
4. Sirotić Z., REVIZIJA SIGURNOSTI ORACLE RSUBP-a, Dostupno na: http://www.istratech.hr/wp-content/uploads/2010/12/case2010.pdf, [Pristupljeno: 12. kolovoza 2019.]
5. Oracle Corporation (2008): Oracle Database Security Checklist, Oracle White Paper, http://www.oracle.com/technology/deploy/security/ database-security/pdf/twp_security_checklist_database.pdf

POPIS SLIKA

POPIS TABLICA

SAŽETAK

Informacijski sustav, organizirani skup postupaka kojima se prikupljaju, obrađuju, spremaju, pretražuju i prikazuju podatci i informacije značajni za neku organizaciju, ustanovu, društvo ili državu.

Revizija informacijskih sustava je proces provjere uspješnosti informacijskih sustava obzirom na to što poslovanje od njih očekuje odnosno obzirom na mogućnosti koje njihova primjena u poslovanju pruža.

CobiT je krovni standard korporativnog upravljanja informatikom unutar kojega se propisuju područja, procesi i pojedinačne kontrole za korporativno i operativno upravljanje informatikom. ITIL pruža tzv. top-down, odnosno poslovno usmjeren pristup menadžmentu informatike koji stavlja poseban naglasak na stratešku poslovnu vrijednost informatike i potrebe da se isporuči njezina visokokvalitetna usluga (informatička usluga, IT usluga).

Reviziji informacijskih sustava trenutno se najviše pažnje pruža u financijskom sektoru. Mora se priznati da Hrvatska narodna banka daje jak ritam razvoju metodologije revizije, pogotovo glede izvođenja vanjske revizije informacijskog sustava kreditnih institucija.

Revizija informacijskih sustava je složen postupak sastavljen od niza koraka i faza kojima se u konačnici testiranjem učinkovitosti informatičkih kontrola prikupljaju dokazi i argumenti za procjenu poslovnog rizika (rizika kojim je poslovanje izloženo temeljem činjenice da se u provedbi poslovnih procesa koristi informacijski sustav i tehnološka podrška) i stručnu procjenu zrelosti kontrolnog okruženja.

CEZIH je Centralni zdravstveni informacijski sustav Republike Hrvatske koji povezuje niz aplikacija i sustava zdravstva u Republici Hrvatskoj. Ministarstvo zdravlja Republike Hrvatske je vlasnik, a Hrvatski zavod za zdravstveno osiguranje je operator središnjeg dijela integralnog informacijskog sustava CEZIH. Za Oracle RSUBP-a prikazuje se pristup reviziji sigurnosti Oracle BP (baze podataka).

Oracle od baze 9i intenzivno pokušava pomoći svojim korisnicima da bazu podataka učine što sigurnijom.U sadašnjim verzijama baze 11.1 i 11.2 učinili su još veći pomak nabolje.

ključne riječi: informacijski sustav, revizija informacijskih sustava, CobiT, ITIL, revizija informacijskih sustava Hrvatska, provedba revizije, primjeri revizije informacijskih sustava

SUMMARY

An information system, an organized set of procedures by which data, information and information relevant to an organization, institution, society or state are collected, processed, stored, searched and displayed.

Information systems audit is a process of checking the performance of information systems, considering what the business expects from them, or considering the opportunities that their application in business provides.

CobiT is an umbrella standard for corporate IT governance that defines areas, processes and individual controls for corporate and operational IT management. ITIL provides the so-called top-down, that is, a business-oriented approach to IT management that places particular emphasis on the strategic business value of IT and the need to deliver its high quality service (IT service, IT service).

Information systems auditing is currently receiving the most attention in the financial sector. It must be acknowledged that the Croatian National Bank gives a strong pace to the development of the audit methodology, especially regarding the external audit of the credit institutions' information system.

Information systems auditing is a complex process consisting of a series of steps and stages that ultimately test the effectiveness of IT controls to gather evidence and arguments for assessing business risk (the risk that a business is exposed to due to the fact that an information system and technological support is used in the implementation of business processes) and expert assessment of the maturity of the control environment.

CEZIH is the Central Health Information System of the Republic of Croatia, which connects a number of health care applications and systems in the Republic of Croatia. The Ministry of Health of the Republic of Croatia is the owner and the Croatian Institute for Health Insurance is the operator of the central part of the CEZIH integral information system. Access to Oracle BP (Database) Security Audit is displayed for Oracle RSUBP.

Oracle has been intensively trying to help its users make the database as secure as possible since Database 9i. In the current versions of Database 1.1 and 11.2, they have made an even greater improvement.

Keywords: information system, information systems audit, CobiT, ITIL, information systems audit Croatia, audit implementation, information systems audit examples