Provedba revizije informacijskih sustava primjenom različitih metodologija

Višnjić, Marija

Sveučilište u Zagrebu

Ekonomski fakultet

Integrirani preddiplomski i diplomski sveučilišni studij

Poslovna ekonomija – smjer Menadžerska informatika

PROVEDBA REVIZIJE INFORMACIJSKIH SUSTAVA PRIMJENOM RAZLIČITIH METODOLOGIJA

Diplomski rad

Marija Višnjić

Zagreb, lipanj 2021.

Sveučilište u Zagrebu

Ekonomski fakultet

Integrirani preddiplomski i diplomski sveučilišni studij

Poslovna ekonomija – smjer Menadžerska informatika

PROVEDBA REVIZIJE INFORMACIJSKIH SUSTAVA PRIMJENOM RAZLIČITIH METODOLOGIJA

IMPLEMENTATION OF INFORMATION SYSTEMS AUDIT USING DIFFERENT METHODOLOGIES

Diplomski rad

Student: Marija Višnjić

JMBAG studenta: 0066234846

Mentor: prof. dr. sc. Mario Spremić

Zagreb, lipanj 2021.

_____

Ime i prezime studenta

IZJAVA O AKADEMSKOJ ČESTITOSTI

Izjavljujem i svojim potpisom potvrđujem da je završni / diplomski / poslijediplomski specijalistički rad, odnosno doktorski rad isključivo rezultat mog vlastitog rada koji se temelji na mojim istraživanjima i oslanja se na objavljenu literaturu, a što pokazuju korištene bilješke i bibliografija.

Izjavljujem da nijedan dio rada nije napisan na nedozvoljen način, odnosno da je prepisan iz necitiranog rada, te da nijedan dio rada ne krši bilo čija autorska prava.

Izjavljujem, također, da nijedan dio rada nije iskorišten za bilo koji drugi rad u bilo kojoj drugoj visokoškolskoj, znanstvenoj ili obrazovnoj ustanovi.

_____

(mjesto i datum)

_____

(vlastoručni potpis)

SAŽETAK

Današnje poslovanje velike većine organizacija obilježava korištenje informacijskih tehnologija. Budući da je porastao značaj informacijskih sustava u postizanju glavnih ciljeva organizacija porasla je i potreba za kontrolom i revizijom kako bi se pravovremeno detektirale nepravilnosti u radu i nadzoru informacijskih sustava i rizici koje proizlaze iz uočenih nepravilnosti.

Kako revizija informacijskih sustava više nije tako nova grana revizije, sasvim je razumljivo kako je i porastao broj okvira i metodologija koje definiraju i reguliraju navedeno područje. Upravo zbog svega navedenog u diplomskom radu su prikazane metodologije i okviri revizije informacijskih sustava.

Naglasak je stavljen na CobIT metodologiju kao krovnu metodologiju, međutim, obrađuju se i druge metodologije poput ISO27001, PCI DSS, NIST, SANS i ITIL metodologije. Također, prikazan je i pregled trendova korištenja pojedinih metodologija u odabranim vrstama poduzeća u Republici Hrvatskoj.

Kako se diplomski rad ne bi svodio samo na teoretski dio, proveden je anketni upitnik nad stručnjacima iz područja revizije informacijskih sustava kao i nad stručnjacima upravljanja informacijskim sustavom kojim se dobio uvid koju metodologiju (ili kombinaciju metodologija) stručnjaci preferiraju u praksi.

KLJUČNE RIJEČI: informacijski sustav, revizija informacijskih sustava, metodologija, kontrola, CobIT

SUMMARY

Today's business of the vast majority of organizations is marked by the use of information technology. As the importance of information systems in achieving the main goals of organizations has increased, so has increased the need for control and audit to detect irregularities in the operation and supervision of information systems and the risks arising from observed irregularities in a timely manner.

Since the audit of information systems is no longer such a new branch of audit, it is quite understandable that the number of frameworks and methodologies that define and regulate this area has increased. Precisely because of all of the above, the diploma thesis presents methodologies and frameworks for auditing information systems.

Emphasis is placed on the CobIT methodology as an umbrella methodology, however, other methodologies such as ISO27001, PCI DSS, NIST, SANS and ITIL methodologies are also addressed. Moreover, an overview of trends in the use of certain methodologies in selected types of companies in the Republic of Croatia is presented.

In order to reduce the thesis not only to the theoretical part, a questionnaire was conducted on experts in the field of information systems audit as well as on information system management experts which gave insight into which methodology (or combination of methodologies) experts prefer in practice.

KEY WORDS: information system, audit of information system, methodology, control, CobIT

SADRŽAJ

UVOD

Uvodno poglavlje ovoga rada opisuje predmet i cilj rada, izvore iz kojih su podaci preuzeti te metode istraživanja. Dodatno, uz navedeno prikazan je sadržaj i struktura rada gdje su ukratko opisani dijelovi rada.

1.1. Predmet i cilj rada

Današnje vrijeme obilježava korištenje informacijskih tehnologija kako bi se postigli glavni ciljevi poslovanja organizacija. Iako korištenje informacijskih sustava donosi velike koristi te unaprjeđuje poslovanje postoje brojni novi rizici s kojima se organizacije suočavaju prilikom korištenja istih.

Svima su nam poznati hakerski napadi te isti bivaju sve učestaliji u moderno doba, a pogotovo u sadašnjem vremenu kada postoji način udaljenog rada. Zbog toga se javlja potreba ulaganja u načine zaštite i prevencije navedenih napada.

Jednu od vodećih uloga u tome je zauzela revizija informacijskih sustava koja se danas sve češće koristi kao metoda otkrivanja nedostataka u upravljanju informacijskim sustavom. Revizija informacijskih sustava više nije tu samo za potrebe regulatornog izvještavanja nego preuzima savjetodavnu funkciju koja olakšava menadžmentu upravljanje informacijskim sustavima organizacije.

1.2. Metode istraživanja i izvori podataka

U svrhu izrade diplomskog rada korišteni su primarni i sekundarni izvori podataka. Kao primarni izvor korišten je anketni upitnik proveden nad stručnjacima iz područja revizije informacijskih sustava kao i nad stručnjacima upravljanja informacijskim sustavom kojim se dobio uvid koju metodologiju (ili kombinaciju metodologija) stručnjaci preferiraju u praksi.

Kao sekundarni izvor podataka koristile su se znanstvene i stručne knjige, časopisi, internet članci i stranice te znanstvene publikacije i radovi kako bi se obradio teorijski dio diplomskog

rada. Kroz rad su se koristile različite metode: metoda deskripcije, metoda indukcije, dedukcije te metode ankete i analize.

1.3. Sadržaj i struktura rada

Rad je podijeljen u pet poglavlja s pripadajućim potpoglavljima. Prvo poglavlje se sastoji od uvoda u kojem se definiraju predmet i cilj rada, metode istraživanja i sadržaj i struktura rada. U drugom poglavlju se definiraju osnovni pojmovi informacijskog sustava, revizije informacijskog sustava te se daje pregled metodologija i okvira za reviziju informacijskih sustava. Treće poglavlje daje pregled trendova korištenja pojedinih metodologija revizije informacijskih sustava u odabranim vrstama poduzeća (industrijama) u Republici Hrvatskoj gdje su izdvojene telekomunikacijska i osiguravajuća društva te kreditne institucije budući da iste imaju obvezu regulatorne revizije i izvještavanja prema nadzornim regulatornim tijelima. Četvrto poglavlje sadrži empirijsko istraživanje na populaciji od 60 ispitanika. Upitnik je istraživao koju metodologiju (ili kombinaciju metodologija) revizije informacijskih sustava stručnjaci preferiraju u praksi te mišljenje o važnosti tehnoloških i poslovnih vještina za reviziju i upravljanje informacijskim sustavima. U posljednjem, petom poglavlju, naveden je zaključak cjelokupnog diplomskog rada.

2. DEFINICIJA OSNOVNIH POJMOVA

2.1. Objašnjenje pojma informacijski sustav

Današnje vrijeme obilježavaju brze promjene koje nastaju unutar okruženja poslovnog sustava te koje donose potrebu za stvaranjem efikasnih informacijskih sustava koji bi omogućili olakšano donošenje poslovnih odluka kako bi se poslovni sustav što brže, bolje i lakše prilagodio promjenama u vlastitoj okolini.

Okosnica svakog poslovanja su podaci koji predstavljaju skup znakova zapisanih na nekom mediju, a nakon što navedeni skup znakova pročitamo i interpretiramo dobivamo informaciju. Informacija je potrebna prilikom donošenja važnih odluka vezanih uz poslovanje budući da se iste oslanjaju na obavijesti, tj. značenju koje informacija ima. Samim time je vrlo bitno da informacija bude kvalitetna.[1]

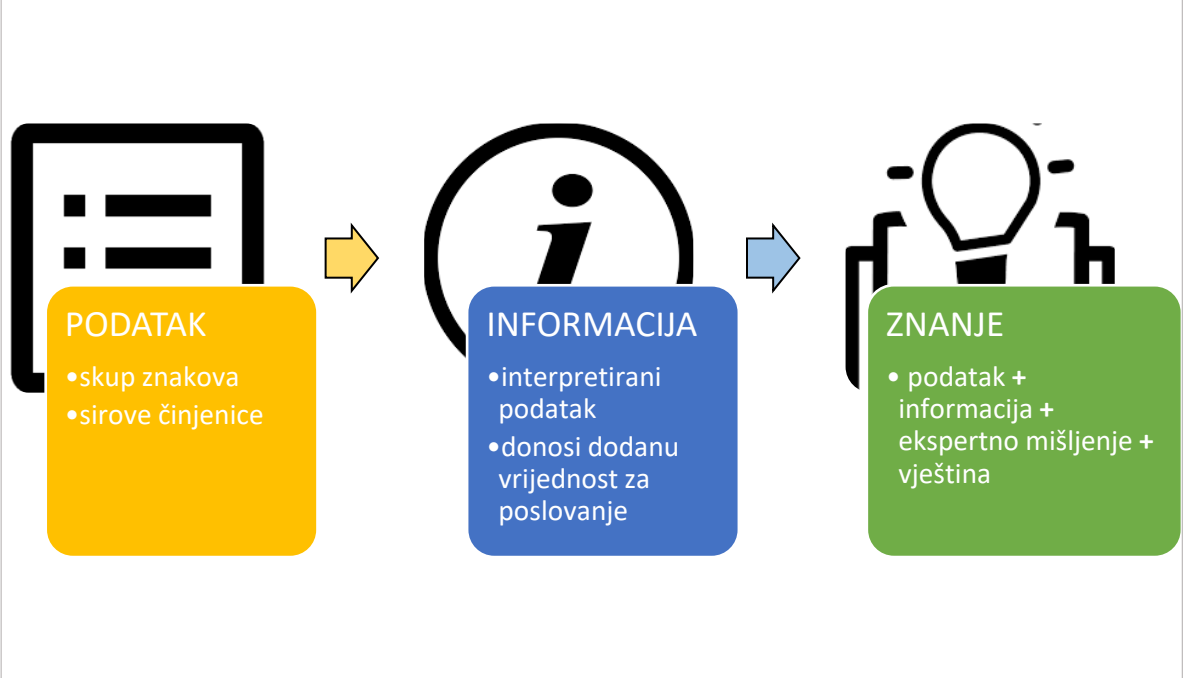
Glavne karakteristike kvalitetne informacije su da je ista:

- točna – što znači da informacija korektno opisuje stanje stvari,
- potpuna – što znači da informacija u cijelosti i objektivno opisuje stanje stvari,
- primjerena odnosno relevantna – što znači da informacija odgovara problemu koji iziskuje odlučivanje i osobi koja odlučuje,
- pravovremena – što znači da je informacija dobivena na vrijeme.[2]

Kombinacijom podataka i informacija dolazimo do znanja kojem je još dodano i ekspertno mišljenje, vještina i iskustvo. [3] Znanje zapravo „zna“ kako i na koji način iskoristiti kvalitetnu informaciju kako bi dalo odgovor na poslovni problem ili stvorilo konkurentsku prednost u poslovanju. Navedena grupacija od podataka do znanja je prikazana na slici 1.

[1] Varga, M. et al. (2016.) Informacijski sustavi u poslovanju, Zagreb, Ekonomski fakultet, str. 3
[2] Ibid., str. 4
[3] Ibid., str. 5

Slika 1: Prikaz podatka, informacije i znanja



Izvor: samostalna izrada autorice prema Varga, M. et al. (2016.) Informacijski sustavi u poslovanju, Zagreb, Ekonomski fakultet

Budući da podaci i informacije koje proizlaze iz interpretacije podataka imaju veliku vrijednost za poslovanje organizacije te se trebaju sistematizirati svaka organizacija će uspostaviti sustav postupanja s istima koji bi trebao biti organiziran, formalan i efikasan. Navedeni sustav se zove informacijski sustav.

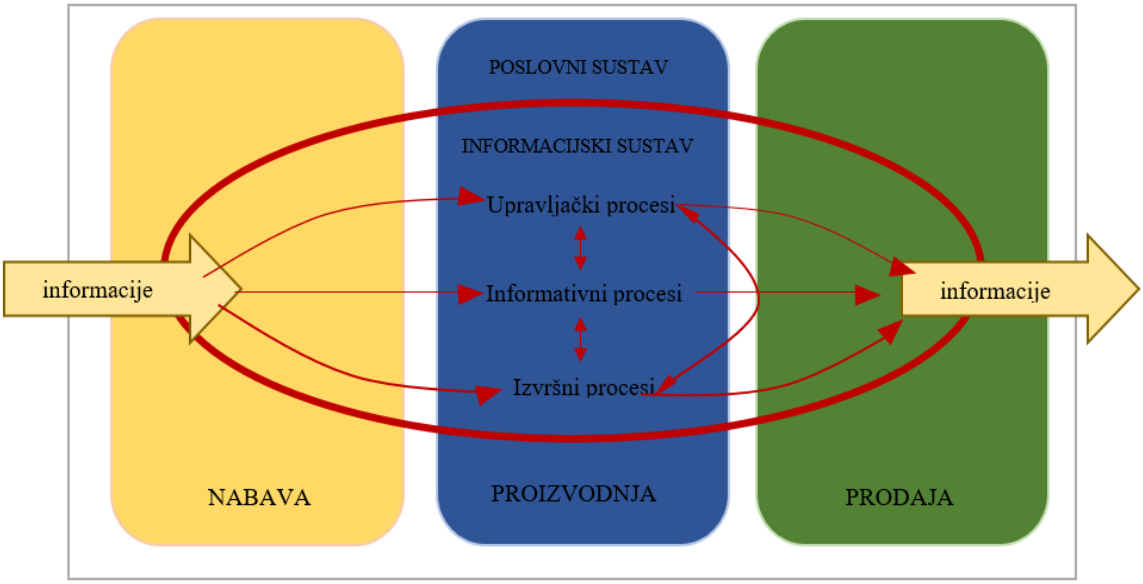
Informacijski sustav se definira kao „sustav koji prikuplja, pohranjuje, čuva, obrađuje i isporučuje informacije važne za organizaciju i društvo, tako da budu dostupne i upotrebljive za svakog tko ih želi koristiti, uključujući poslovodstvo, klijente, osoblje i ostale. Informacijski sustav je aktivni društveni sustav koji se može, ali i ne mora, koristiti suvremenom informacijskom tehnologijom.“[4] Informacijski sustav koji ne mora koristiti suvremenu informacijsku tehnologiju nazivamo manualnim informacijskim sustavom te se danas vrlo rijetko koristi budući da sadašnji poslovni uvjeti zahtijevaju korištenje informacijsko-komunikacijskih tehnologija u većini aktivnosti pa je danas zastupljeniji kompjuterizirani informacijski sustav. [5]

[4] Varga, M. (1994.) Baze podataka: konceptualno, logičko i fizičko modeliranje podataka, Zagreb, Društvo za razvoj informacijske pismenosti (DRIP), str. 2
[5] Bosilj Vukšić, V. et al. (2020.) Osnove poslovne informatike, Zagreb, Ekonomski fakultet, str. 175

Informacijski sustav je zapravo dio poslovnog sustava neke organizacije te istome omogućuje komunikaciju unutar sebe i s okolinom. Budući da su temeljne aktivnosti poslovnog sustava izvršavanje poslovnih procesa te upravljanje poslovnim sustavom možemo reći kako je zadatak informacijskog sustava opskrba poslovnog sustava potrebnim, tj. relevantnim informacijama koje su potrebne za obavljanje navedenih temeljnih aktivnosti.

Slikom 2. je vizualno prikazano kako informacijski sustav funkcionira unutar samog poslovnog sustava. Crvenim linijama je označeno na koji način informacije teku unutar samog informacijskog sustava dok je žutim strelicama prikazan ulaz i izlaz informacija, tj. materijalnih tokova unutar samog poslovnog sustava.

Slika 2: Informacijski sustav kao dio poslovnog sustava



Izvor: preuzeto i prilagođeno iz knjige Varga, M. et al. (2012.) Upravljanje podacima, Zagreb, Element

Kako bi poslovni sustav mogao funkcionirati na najbolji mogući način potrebno je istome osigurati efikasan informacijski sustav koji može dati odgovore na pitanja što je cilj samog informacijskog sustava, koje su njegove funkcije i od čega se isti sastoji.[6]

Osnovni cilj svakog informacijskog sustava je dostaviti pravu (relevantnu) informaciju na pravo mjesto, u pravo vrijeme i uz minimalne troškove. Međutim, često se nailazi na problem prepoznavanja prave informacije jer čak i najiskusniji stručnjaci unutar organizacije često ne znaju reći koji su to podaci i informacije koji su potrebni za rješavanje nekog problema. Kako bismo došli do odgovora i odredili koje su informacije potrebne i relevantne u informacijskom

[6] Ibid., str. 174

sustavu potrebno je zapravo definirati problem koji se želi riješiti informacijskim sustavom te koje informacije su poželjne kako bi se isti riješio na uspješan način.[7]

Informacijski sustav zapravo ima četiri osnovne funkcije:

- prikupljanje podataka – prikuplja podatke s izvora te ih priprema za unos i obradu, a kako bi se navedeno odradilo u skladu s očekivanjima organizacije potrebno je odrediti koje izvore podataka ćemo koristiti te definirati koje metode prikupljanja, pripreme i unosa istih ćemo koristiti.
- obrada podataka – informacijski sustav obrađuje podatke u skladu s unaprijed definiranim zahtjevima i potrebama korisnika informacijskog sustava te se nad istima vrše operacije sažimanja, pretvorbe i/ili raščlanjivanja.
- pohranjivanje (spremanje) podataka i informacija – prikupljeni podaci (obrađeni, ali i izvorni) se mogu spremati unutar informacijskog sustava kako bi se mogli dalje koristiti ili kako bi se pripremili za druge obrade.
- distribucija podataka i informacija korisnicima – kako bi korisnici mogli napraviti potrebne analize i donositi odluke važne za poslovanje organizacije informacije se dostavljaju istima u razumljivom obliku (npr. izvještaji, tablice, grafikoni i sl.).[8]

Prema Ćurko, K. i Pivar, J. osnovne komponente informacijskog sustava su sljedeće:

- hardver *(eng. hardware)* – materijalna komponenta informacijskog sustva (primjerice, radne stanice, serveri, hostovi, pisači, modemi i sl.)
- softver *(eng. software)* – nematerijalna komponenta u obliku programskih rješenja, rutina ili metoda na kojima se temelji rad hardvera (operativni sustav, poslovne aplikacije i sl.)
- korisnici *(eng. lifeware)* - ljudi koji rade s informacijskim sustavom
- organizacija *(eng. orgware)* - organizacijski postupci, metode i načini povezivanja ljudi, strojne i programske potpore u skladnu cjelinu
- mreža *(eng. netware)* – koncepcija i realizacija povezivanja svih podsustava
- podaci *(eng. dataware)* – koncepcija i organizacija baze podataka i svih raspoloživih informacijskih resursa.[9]

Slika 3: Osnovne komponente informacijskog sustava

[7] Ibid.
[8] Ibid.
[9] Ibid., str. 175

Izvor: samostalna izrada autorice prema Bosilj Vukšić, V. et al. (2020.) Osnove poslovne informatike, Zagreb, Ekonomski fakultet

Navedeni elementi bi trebali biti usklađeni i biti na istoj razini kvalitete kako bi se omogućilo uspješno funkcioniranje informacijskog sustava namijenjenog poslovanju. Međutim, u praksi je teško postići da svi elementi informacijskog sustava budu u potpunosti usklađeni te se zbog toga najveća pažnja posvećuje kvaliteti i mjerenju kvalitete samog informacijskog sustava koja se postiže prikupljanjem kvalitetnih informacija o kojima je već bilo riječi u radu.

Dakle, kvalitetna informacija mora omogućiti korisniku informacijskog sustava donošenje odgovarajućih odluka za organizaciju koje će organizaciji donijeti korist, tj. dodanu vrijednost. Zbog svega navedenog možemo reći da je informacijski sustav kvalitetan onoliko koliko je kvalitetna najslabija karika, tj. komponenta unutar samog sustava.

Budući da tehnologija napreduje iz dana u dan rijetki su trenutci kada sama tehnologija biva najslabija karika informacijskog sustava. Uglavnom najveću prijetnju za zadovoljavajuću kvalitetu informacijskog sustava čini ljudski faktor koji svojim nedovoljnim znanjem i vještinama može onemogućiti optimalno korištenje informacijskog sustava (hardverske, softverske, komunikacijske, podatkovne i organizacijske komponente) u praksi što dovodi do

neusklađenosti između velikih ulaganja u komponente informacijskog sustava i skromnih koristi koje proizlaze iz neoptimalnog korištenja istog.

Sukladno navedenome, vrlo je važno uspostaviti proces upravljanja informacijskim sustavom *(eng. IT governance)* unutar organizacije.

Prema Spremić, M. korporativno upravljanje informatikom (ili informacijskim sustavom) se svodi na dvije razine:

- stratešku (korporativnu) razinu *(eng. IT governance*) koja se usmjerava na eksterno okruženje i strateško razmišljanje i viziju kako bi ostvarila cilj, a to je ostvarenje interesa svih dionika organizacije i,
- operativnu (uglavnom tehnološku) razinu *(eng. IT management)* koja je usmjerena na interno okruženje, upravljanje i administraciju poslovnih procesa te pronalaženje najboljih tehnoloških i administrativnih rješenja kako bi se inovativni poslovni model sproveo u djelo.[10]

Pojam upravljanja informacijskim sustavom možemo definirati kao dio korporativnog upravljanja *(eng. corporate governance)* koji se brine o kvalitetnom iskorištavanju informacijske tehnologije koja se koristi unutar informacijskog sustava kako bi se postigli ciljevi organizacije. Konkretno, definira kako se donose odluke, tko ih donosi, tko je odgovoran i kako se mjere i vrednuju rezultati donesenih odluka.[11]

Prema Spremić, M. najvažniji ciljevi korporativnog upravljanja informatikom su:

- ulaganje u digitalne i informacijske tehnologije kako bi se stvorila viša vrijednost i korist za poslovanje,
- primjena digitalne i informacijske tehnologije kako bi se bolje shvatili rizici i kako bi se bolje upravljalo njima,
- bolje upravljanje svim informatičkim resursima (infrastruktura, podaci, a posebno ljudi) kako bi se strateški planovi digitalizacije i primjene informacijskih tehnologija uspješno sproveli u djelo,
- pružanje podrške digitalizaciji poslovanja.[12]

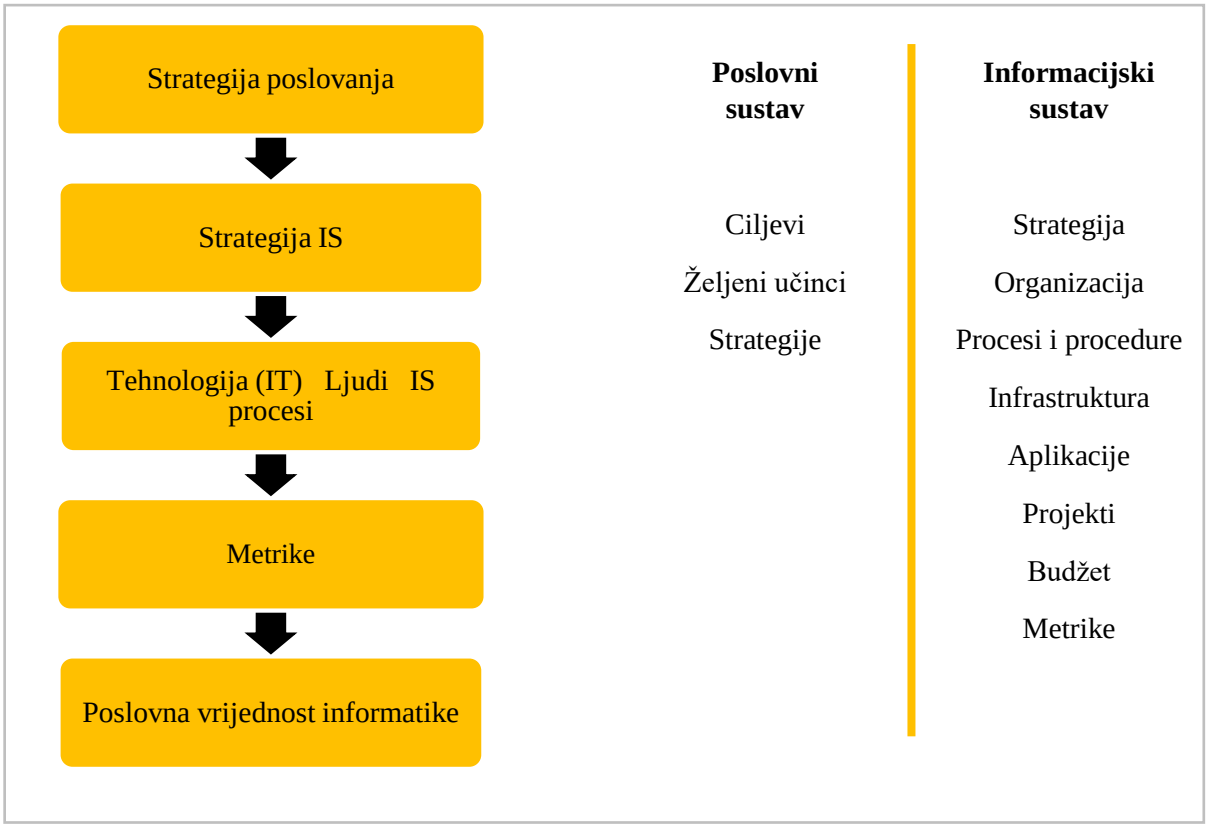
[10] Spremić, M. (2017.) Digitalna transformacija poslovanja, Zagreb, Ekonomski fakultet, str. 205
[11] prilagođena definicija sukladno Symons, C., (2005.): IT Governance Framework: Structures, Processes and Framework, Forrester Research, Inc., str. 2
[12] Spremić, M. (2017.) op.cit., str. 206

Na višoj razini možemo reći da upravljanje informacijskim sustavom zapravo osigurava provođenje strategije informacijskog sustava koja proizlazi iz poslovne strategije organizacije, tj. iz poslovnih ciljeva organizacije se određuje strategija informacijskog sustava.

Prema Spremić, M. strateško planiranje informacijskog sustava predstavlja skup aktivnosti kojima je cilj uskladiti ciljeve informacijskog sustava s ciljevima poslovnog sustava te se u sklopu istih planira infrastruktura (informacijska) koja bi navedeno i omogućila.[13]

Kao što je i prikazano na slici 4. organizacija prvo donosi strategiju poslovanja iz koje proizlazi strategija informacijskih sustava, a tek nakon toga strategije sastavnih komponenti istoga. [14]

Slika 4: Izvođenje strategije informacijskog sustava iz strategije poslovanja



Izvor: Spremić, M. (2017.) Digitalna transformacija poslovanja, Zagreb, Ekonomski fakultet

U provođenje strategije poslovanja, pa tako i strategije informacijskog sustava treba biti uključen najviši menadžment organizacije, direktor odjela informatike koji je odgovoran Upravi organizacije *(eng. CIO – Chief Information Officer)* te menadžeri ostalih poslovnih funkcija važnih za poslovanje. Nije neuobičajeno i da se formiraju i zasebna organizacija tijela i odbori čija je zadaća nadzor nad provedbom strateškog plana informacijskog sustava.

[13] Spremić, M. (2017.) op.cit., str. 114
[14] Ibid.

Jedan od takvih odbora je i Odbor za upravljanje informacijskim sustavom koji je neovisan od odjela informatike unutar organizacije te je direktno odgovoran Upravi. Njegova zadaća je povezati poslovanje i informatiku, tj. uskladiti primjenu informatike i informacijske tehnologije s poslovnim ciljevima i prioritetima.[15]

2.2. Objašnjenje pojma revizija informacijskog sustava

Budući da danas gotovo i ne postoji organizacija koja se ne koristi nekim vidom informacijske tehnologije kojom se ostvaruju mnogobrojne poslovne koristi logičan je zaključak da se takve organizacije istodobno izlažu i novim prijetnjama, neželjenim posljedicama i brojnim novim rizicima (tzv. informatičkim (IT) rizicima, a posebice kibernetičkim *(eng. cyber)* rizicima).[16]

U nekim organizacijama takvi rizici se smatraju manje važnima i etiketiraju kao rizici koji nikako neće imati negativnih posljedica na poslovanje. Međutim, praksa je pokazala kako takve pogrešne procjene informatičkih rizika mogu dovesti do značajnih financijskih gubitaka i ostalim naknadnim štetama, a nerijetko dolazi i do gubitka reputacije uslijed značajnijih sigurnosnih incidenata izazvanih nepravovremenim poduzimanjem odgovarajućih mjera za smanjenje informatičkih rizika.

Postoje mnogobrojni primjeri, kako svjetski tako i domaći, u kojima je vidljivo kakve je posljedice imalo pogrešno etiketiranje informatičkih rizika i zanemarivanje ulaganja u načine zaštite od istih od strane menadžmenta. Iako bi možda mogli pomisliti kako su takvi incidenti stvar prošlosti (početak 2000-ih kada nije toliko zaživio pojam informacijske sigurnosti) te da su danas organizacije svjesnije opasnosti koje se nalaze u njihovom okruženju, praksa nam pokazuje drugačije.

2.2.1. Primjer iz prakse

Dovoljno je samo prisjetiti se kako je u veljači 2020. godine INA imala hakerski napad koji je trajao više od mjesec dana. Naime, koliko je poznato medijima, zlonamjerni softver, točnije *ransomware* je upao u sustav i zaključao kompletnu internu prepisku unutar kompanije (e-mail)

[15] Ibid., str. 114 - 115
[16] Ibid., str. 132.

i sve baze podataka o poslovanju. Napadom je bilo obuhvaćeno ukupno 180 servera INA-e i tvrtki članica INA Grupe. Naravno, za navedene zaključane podatke je tražena otkupnina. [17]

Najveći problem ovakvog napadao je ležao u sigurnosnoj kopiji podataka. Poznato je da je izrada periodičke sigurnosne kopije podataka *(eng. backup)* na zasebnim serverima preventivna kontrola u informacijskom sustavu kojom se žele izbjeći baš ovakvi scenariji, a ukoliko se takva sigurnosna kopija sprema na vanjski disk isti je potrebno odvojiti od računalnog sustava i spremiti na sigurnu lokaciju kako zlonamjerni softver ne bi mogao zaključati iste. Međutim, očito je da INA nije radila periodičku sigurnosnu kopiju podataka (dnevnu, tjednu ili mjesečnu) zbog čega je tada bila primorana uložiti ogromne napore i resurse (ljudske i novčane) kako bi povratila podatke o poslovanju.[18]

U slučaju INA-e se može postavljati puno pitanja: zašto sustav koji služi za detekciju i prevenciju napada (*eng. IPS – Intrusion Prevention System and IDS – Intrusion Detection System)* nije radio, tj. zašto odgovorna osoba nije pravovremeno reagirala na napad, zašto administratori sustava nisu redovito radili sigurnosne kopije podataka (ili ako jesu, zašto iste nisu odrađene u skladu s dobrim sigurnosnim praksama), postoje li nalazi i mišljenja interne i vanjske revizije koja su adresirala ovakav propust u upravljanju informacijskim sustavom te, ako postoje, zašto odgovorne osobe nisu napravile nešto kako bi otklonile preporuku i smanjile identificirani rizik?

Bez obzira na odgovore, poprilično je jasno kako neadekvatno upravljanje informacijskim sustavom i propusti u identificiranju i tretiranju informatičkih rizika postoji i danas iako se sigurnost informacijskog sustava tretira kao jedna od važnijih tema u krugovima revizora i menadžmenta organizacija.

Kako bi se osigurala kvaliteta informacijskog sustava kroz koji organizacije ostvaruju svoje uspješno poslovanje te kako bi se identificirali svi oni potencijalni rizici i prijetnje koje organizacija nije odmah uočila, danas se sve veći naglasak stavlja na reviziju informacijskih sustava, kako od strane interne revizije tako i od strane vanjske, neovisne revizije.

Prema Spremić, M. revizija informacijskih sustava *(eng. Information System Audit)* je proces kojim se provjerava jesu li informacijskih sustavi uspješno ostvarili ciljeve s obzirom na ono što poslovanje od njih očekuje, tj. revizija informacijskih sustava provjerava usklađenost ciljeva

[17] „Hakerski napad na INU pokrenut je iz Mađarske i zaključao je podatke o poslovanju potrebne Lazardu“ (2020., online), dostupno na: https://www.nacional.hr/hakerski-napad-na-inu-pokrenut-je-iz-madarske-i-zakljucao-je-podatke-o-poslovanju-potrebne-lazardu/ [7. svibnja 2021.]
[18] Ibid.

poslovnih i informacijskih sustava.[19] Zapravo se može govoriti o skupu složenih menadžerskih, revizorskih i tehnoloških aktivnosti kojima se provjerava učinak i rizik korištenja informacijskog sustava unutar Društva te se ocjenjuje njihov utjecaj na poslovanje.[20]

Revizijom informacijskih sustava se zapravo želi ocijeniti:

- usklađenost informatike s poslovnim ciljevima,
- podupire li informatika, učinkovito i djelotvorno, ciljeve poslovanja i u kojoj mjeri te
- jesu li kontrole informacijskog sustava na raznim hijerarhijskim razinama dovoljno učinkovite (zrele).[21]

Dakle, kako je Spremić, M. naglasio objekt revizije informacijskih sustava je ispitati, temeljno, kontrole koje postoje unutar cjelokupnog informacijskog sustava dok je osnovni zadatak iste procjeniti zrelost, tj. razinu uspješnosti informacijskog sustava, otkriti područja koja predstavljaju rizik za poslovanje i procjeniti njihovu rizičnost te menadžmentu organizacije dati preporuke i savjete kako poboljšati upravljanje informacijskim sustavom.[22]

Budući da je objekt revizije informacijskih sustava procjena zrelosti kontrola trebalo bi reći da su informatičke kontrole su zapravo one kontrole koje čine sastavni dio informacijskog sustava i koje su međusobno povezane kako bi ostvarile ciljeve informacijskog sustava organizacije (ukoliko djeluju jedinstveno i usklađeno).[23]

Glavni razlog njihove primjene je sprječavanje (prevencija), otkrivanje (detekcija) ili ispravljanje (korekcija) neželjenih događa i / ili procesa.[24]

Sukladno navedenome, kontrole informacijskog sustava možemo razvrstati prema četiri kriterija koji će biti navedeni u nastavku.

Prema kriteriju **načina primjene** možemo razlikovati:

- **automatske kontrole** koje služe kao zaštitni mehanizmi poslovnih procesa te omogućavaju njihovo pravilno funkcioniranje. Primjerice, automatska kontrola je

[19] Spremić, M. (2017) Sigurnost i revizija informacijskih sustava u okruženju digitalne ekonomije, Zagreb, Ekonomski fakultet, str. 195
[20] Ibid.
[21] Ibid.
[22] Ibid., str. 196
[23] Ibid. str. 87
[24] Ibid.

nemogućnost ručnog knjiženja temeljnica unutar sustava poduzeća ukoliko korisnik ne posjeduje unaprijed dodijeljenu rolu za istu.

- **ručne kontrole** koje se koriste za ručno pregledavanje funkcionalnosti poslovnih procesa. Primjerice inventura, konfiguracija opreme i slično.[25]

S obzirom na **svrhu** zbog koje se poduzimaju možemo razlikovati:

- **preventivne kontrole** su one kontrole čiji je zadatak predvidjeti i otkriti probleme ili neželjene događaje prije nego se oni pojave te prevencijom pokušati spriječiti propuste koji bi doveli do tih neželjenih događaja. Navedeno bi podrazumijevalo konstantno praćenje aktivnosti i najvažnije operacije informacijskog sustava. Primjer ovakvih kontrola su logičke i fizičke kontrole pristupa, donošenje krovnih internih akata koji adresiraju sigurnost informacijskog sustava, zapošljavanje stručnjaka u pojedinim poslovnim procesima organizacije, uspostavljanje nadzornih tijela unutar organizacije kojima se nadzire rad informacijskog sustava (npr. Odbor za upravljanje informacijskim sustavom) i slično.
- **detektivne kontrole** koje otkrivaju pogreške, propuste ili neželjene događaje na bilo kojem dijelu informacijskog sustava. Primjer ovakvih kontrola je uspostava softvera za detekciju napada (*eng. Intrusion Detection System – IDS),* kontrola unosa podataka, nadzor mrežnog prometa, provjera zapisa rada sustava *(eng. log)* s kojih se izdvajaju zanimljivi događaji koji se poslije proučavaju (npr. provjeravanje zapisa s vatrozida kojem je cilj detektirati pokušaj napada i primjena dodatnih preventivnih kontrola za budućnost)
- **korektivne kontrole** koje, nakon što se pogreška ili neželjeni događaj već dogodio, pokušavaju smanjiti utjecaj na kritične poslovne procese unutar informacijskog sustava organizacije. Primjerice procedure ponovnog uspostavljanja procesa u najkraćem mogućem vremenu kako bi se smanjio utjecaj na kontinuitet poslovanja organizacije, procedure pričuvne pohrane podataka *(eng. backup)* i slično. [26]

Prema **načinu funkcioniranja** možemo razlikovati:

- **organizacijske kontrole** odnose na interne akte organizacije kojima se propisuje primjereno korištenje svim dijelovima informacijskog sustava. Primjeri su donošenje Opće politike informacijske sigurnosti, Metodologije upravljanja projektima i

[25] Ibid., str. 89
[26] Ibid., str. 89-90

programskim promjenama, Metodologije procjene informatičkih rizika, Strategije informacijskog sustava, Strategija kontinuiteta poslovanja i slično. U navedeno spadaju i svi interni podakti koji detaljnije razrađuju politike, metodologije i procedure na taktičnoj i operativnoj razini (pravilnici, standardi, radne upute i planovi)

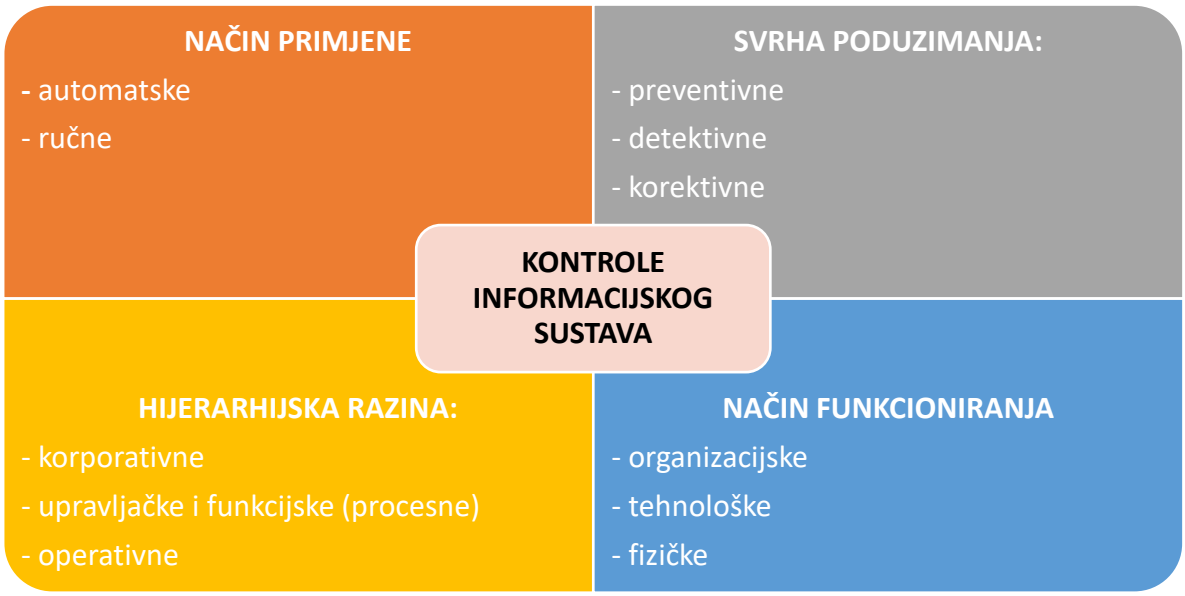
- **tehnološke kontrole** su kontrole vezane uz mrežnu infrastrukturu, podatake, opremu, alate i algoritme te su, najčešće, kao automatske kontrole ugrađene u određene dijelove informacijskog sustava kako bi nadzirale njihov rad. Primjerice, softver / alat za kontrolu kapaciteta mrežne opreme koji ima automatska pravila za slanje poruka odgovornim osobama kada na nekoj mrežnoj opremi manjka mjesta za pohranu.
- **fizičke kontrole** su kontrole koje se odnose na fizičku zaštitu pristupa informacijskom sustavu organizacije kao i planove aktivnosti u slučajevima fizičke ugroze zaštite informacijskog sustava. Primjerice, fizička zaštita podatkovnog centra (kamere, posebna kartica za ulaz) te protupožarna zaštita unutar podatkovnog centra (vatrodojavni senzori te prskalice). [27]

Prema **hijerarhijskoj razini djelovanja** možemo razlikovati:

- **korporativne kontrole** se odnose na provjeru provedbe internih akta organizacije kojima se propisuje primjereno korištenje svim dijelovima informacijskog sustava. Primjerice, uspostavljanje Odbora za informatiku i slično.
- **upravljačke kontrole i funkcijske (procesne) kontrole** se odnose kontrolu i kupovinu poslovnih softvera (aplikacija), njihovu instalaciju i kontrolu nad podacima koje te aplikacije koriste, kontrole testiranja softvera, kontrole pristupa izvornom kodu, kontorle kontinuiteta poslovanja i slično.
- **operativne kontrole** se odnose na kontrole rada poslovnih aplikacija, kontrole točnosti i potpunosti trasakcija i segregacije dužnosti, kontrole dostupnosti i funkcionalnosti mreže, infrastrukture i podataka. [28]

[27] Ibid., str. 90-92
[28] Ibid., str. 92-93

Slika 5. Podjela kontrole informacijskog sustava



Izvor: samostalna izrada autorice prema Spremić, M. (2017.) Sigurnost i revizija informacijskih sustava u okruženju digitalne ekonomije, Zagreb, Ekonomski fakultet

Glavni cilj revizije informacijskih sustava je procijeniti stanje informacijskog sustava organizacije, detektirati područja koja su rizična i dati preporuke menadžmentu organizacije kako bi poboljšalo praksu upravljanja informacijskim sustavom. [29]

Prema Spremiću, M., najvažniji koraci i faze provedbe revizije informacijskih sustava su:

1. uvodni pregled, tj. snimka trenutnog stanja informacijskog sustava,
2. određivanje objekta revizije, tj. što će se revidirati, koja područja će se uzeti u obzir i slično,
3. određivanje ciljeva kontrola za svako odabrano područje,
4. testiranje kontrola,
5. detaljno analitičko testiranje,
6. prikupljanje dokaza i procjena poslovnih rizika te donošenje preporuka,
7. priprema i prezentiranje izvještaja Upravi organizacije.[30]

Navedeno se radi sukladno metodi koje revizori koriste prilikom provedbe revizije informacijskog sustava, a to su:

[29] Ibid., str. 196
[30] Ibid., str. 212

1. **Priprema i planiranje revizije** koja se sastoji od ugovaranja revizije s klijentom, upoznavanje s poslovanjem organizacije, uočavanje ključnih poslovnih procesa, pregled prethodnih izvještaja o reviziji informacijskog sustava, ukratko rečeno, određivanja opsega revizije.
2. **Prikupljanje i detaljna analiza dokumentacije** koja se sastoji od prikupljanja zatražene dokumentacije od klijenta, određivanje plana revizije, kontrolnih područja i kontrolnih ciljeva, određivanje strategije, tj. načina provedbe revizije te odabir najpogodnijeg načina testiranja kontrola koje su u opsegu revizije.
3. **Tehnike i metode prikupljanja revizijskih dokaza** koja se sastoji od provedbe unaprijed definiranih anketa i analize rezultata istih, vođenje unaprijed definiranih intervjua s odgovornim osobama za procese koji su u opsegu revizije kako bi se prikupilo što više informacija o funkcioniranju poslovnih procesa i samih kontrola unutar njih.
4. **Provedba analitičkih testova** koja se sastoji od detaljnih postupaka kontrole koji su u skladu s planom revizije (upitnici, razgovori, tehničko testiranje).
5. **Analiza i vrednovanje revizijskih dokaza.**
6. **Priprema i predstavljanje revizorskog izvješća.** [31]

Svaka od navedenih faza, i pripadajućih metoda, oduzima određeno vrijeme. Budući da je vrlo važno pridržavati se unaprijed određenog vremena provedbe revizije i unaprijed definiranog budžeta potrebno je imati točnu predodžbu koliko ćemo vremena potrošiti na određenu fazu revizije. U nastavku se nalazi tablica s postotkom vremena koji oduzima svaka pojedina faza od ukupnog vremena trajanja revizije. Naravno, navedeno može varirati u slučajevima da klijent nije kooperativan prilikom provedbe same revizije.

Tablica 1. Faze revizije informacijskog sustava

Faza revizije informacijskog sustava	% od ukupnog vremena trajanja revizije
Priprema i planiranje	10
Analiza dokumentacije	10
Prikupljanje revizijskih dokaza: • Intervjui, ankete i neformalni razgovori • Tehničko ispitivanje i testiranje sustava	 10 15

[31] Ibid, str. 214-215

Analiza i vrednovanje revizijskih dokaza	20
Priprema revizijskog izvješća	20
Predstavljanje revizijskog izvješća	5
Postrevizijske aktivnosti	10

Izvor: Spremić, M. (2017.) Sigurnost i revizija informacijskih sustava u okruženju digitalne ekonomije, Zagreb, Ekonomski fakultet

Sve navedeno se očituje unutar izvještaja revizora informacijskog sustava koji se, prema Spremiću, M., sastoji od sljedećega:

- analizi zatečenog stanja primjene informacijskog sustava prema određenim područjima,
- procjeni poslovnih rizika koja proizlazi iz zatečenog stanja,
- preporuke menadžmentu za poboljšanje stanja uz očitovanje Uprave na nalaze i preporuke revizije.[32]

Revizija informacijskih sustava je u početku bila potpora financijskoj reviziji (tj. reviziji financijskih izvještaja), međutim, danas sve više zauzima savjetodavnu ulogu koja pomaže menadžmentu organizacija u upravljanju informacijskim sustavom.

Revizori upotrebljavaju krovne (CobIT) i izvedene standarde (ISO27000, ITIL, PCI DSS) kako bi metodološki procijenili kvalitetu informacijskog sustava neke organizacije te je time revizija postala „analitička“ komponenta strateškog upravljanja informacijskim sustavom.[33]

Krovni i izvedeni standardi će biti detaljnije obrađeni u nadolazećim poglavljima diplomskog rada.

2.3. Standardi i smjernice (metodologije) za reviziju informacijskih sustava

U narednim poglavljima će se napraviti pregled važnijih standarda i metodologija na koji se oslanjaju revizori prilikom revizije informacijskih sustava. Počet će se s krovnim standardom te će se nastaviti s izvedenim standardima i standardima koji pobliže definiraju pojedino područje sigurnosti informacijskog sustava.

[32] Ibid., str. 196
[33] Ibid.

2.3.1. Objašnjenje standarda CobIT *(Control Objective for Information and Related Technology)*

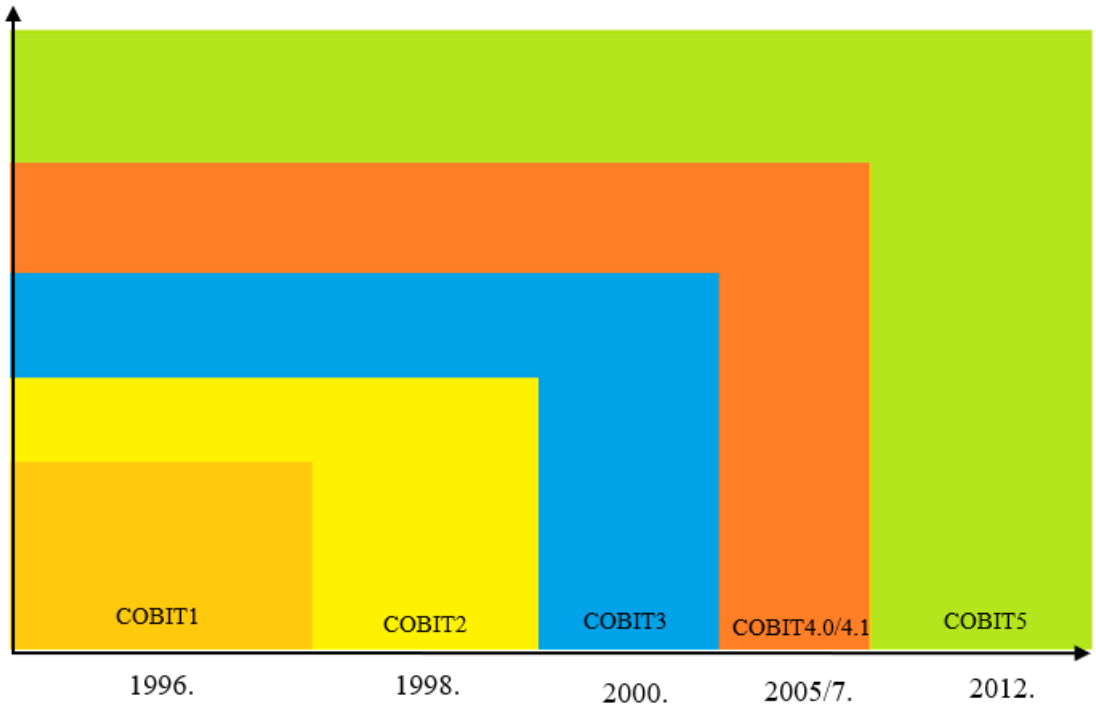
CobIT (*eng. Control Objective for Information and Related Technology)* je jedan od najrasprostranjenijih standarda za upravljanje informacijskim sustavom te predstavlja krovni standard korporativnog upravljanja informatikom.

Unutar njega se propisuju područja, procesi i kontrole koje služe za korporativno i operativno upravljanje informatikom.

Za sadržaj okvira, tj. autor samog CobIT okvira je ISACA (*eng. Information System Audit and Control Association)* koja je vodeći svjetski pružatelj znanja, certifikata i obrazovanja na područjima sigurnosti i osiguranja, korporativnog upravljanja te upravljanja informatičkim rizicima i informacijskom tehnologijom.[34]

CobIT je prvotno nastao kao alat koji bi pružio podršku provedbi financijske revizije (revizije financijskih izvještaja), ali je od 2000.-ih pa na dalje postao sve korišteniji okvir kontrole informacijskih sustava. Njegova zadnja verzija, CobIT 5 (CobIT 2019), predstavlja najvažniji okvir provedbe koncepta korporativnog upravljanja informacijskim sustavima. Razvoj CobIT-a kroz vrijeme je prikazan na slici 6.

Slika 6. Razvoj CobIT standarda kroz vrijeme



[34] ISACA (online), dostupno na: https://www.isaca.org/why-isaca/about-us/history [08. Lipnja 2021.]

Izvor: IT Governance Institute (2012): CobiT 5 – Framework, Control Objectives, Management Guidlines and Maturity Models, IT Governance Institute, Rolling Meadows, Illionis, SAD, str. 12. Dostupno u pdf formatu na: https://www.isaca.org, [08. lipnja 2021.]

Ovaj okvir se orijentira na procese te je obuhvatio sva područja korporativnog upravljanja informatikom, a osnovna funkcija mu je davanje preporuka kako bi ciljevi poslovanja bili u skladu s ciljevima informatike.[35]

Osnovna obilježja ovoga okvira su:

- U svjetskim razmjerima se smatra krovnom metodologijom upravljanja informatikom.
- Alat koji se najviše koristi za provedbu kontrole i revizije informacijskih sustava organizacija
- Daje smjernice za analizu, mjerenje i kontrolu primjene informacijskih sustava u poslovanju
- Sadrži ukupno 37 procesa, tj. 37 ciljeva kontrole (*eng. control objectives)* i više od 300 preciznih i detaljnih kontrola kao i uputa za njihovo provođenje

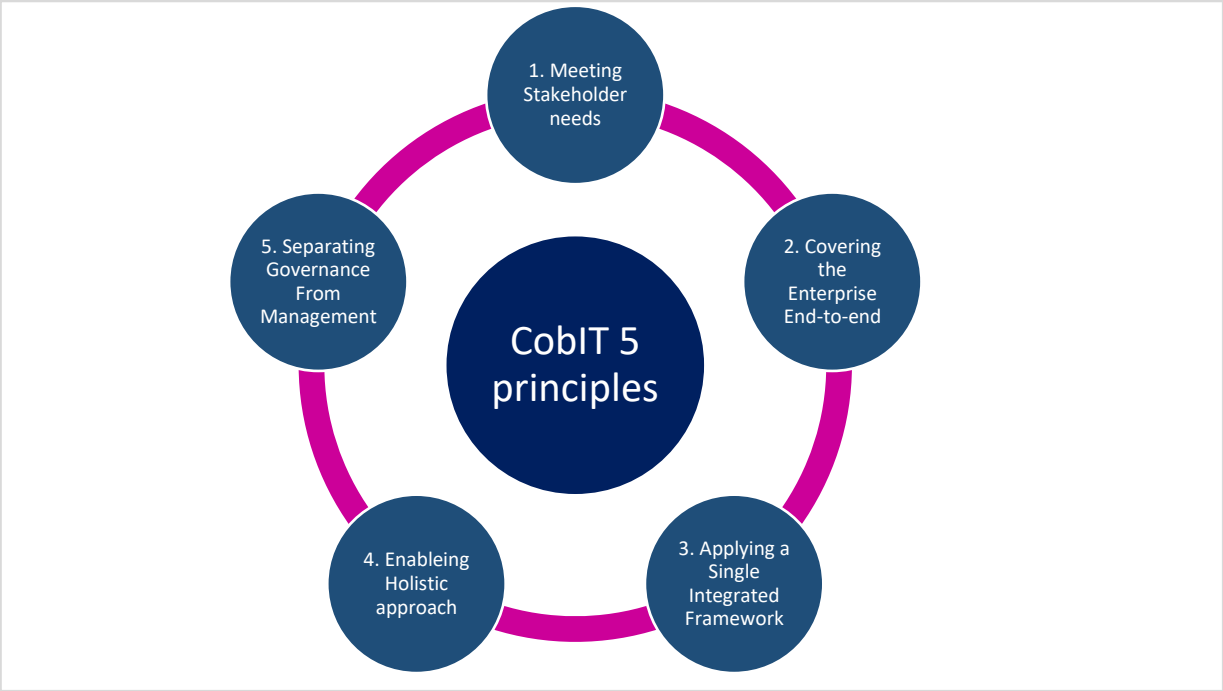
CobIT 5 pruža sveobuhvatan okvir koji pomaže poduzećima u postizanju njihovih ciljeva za korporativno upravljanje informatikom. Jednostavno rečeno, pomaže poduzećima stvoriti optimalnu vrijednost za informatiku održavajući ravnotežu između ostvarivanja koristi i optimizacije razine rizika i korištenja resursa. CobIT se bazira na 5 osnovnih principa upravljanja informatikom:

1. Zadovoljavanje potreba dionika → poduzeća postoje da bi stvorila vrijednost za svoje dionike održavajući ravnotežu između ostvarivanja koristi i optimizacije razine rizika i korištenja resursa. Okvir daje sve zahtjevane procese kako bi podržao stvaranje poslovnih vrijednosti kroz korištenje informacijskom tehnologijom.
2. End-to-end pokriće poduzeća → okvir integrira korporativno upravljanje informacijskim sustavima unutar korporativnog upravljanja.
3. Primjena jedinstvenog, integriranog okvira → CobIT objedinjuje sve smjernice i upute iz ostalih standarda u cjelokupni okvir za upravljanje informacijskim sustavima
4. Omogućavanje holističkog pristupa → efikasno upravljanje infomatikom zahtjeva interakciju svih komponenti što CobIT omogućava.

[35] Varga, M., Varga, V. (2011.) Usporedba rezultata revizije informacijskih sustava provedenih prema CobiT okviru i uvod u CobiT 5 okvir. Tehnički glasnik, 5 (2011.), str. 35 – 43

5. Odvajanje upravljanja (*eng. governance)* od rukovodstva (*eng. management)* → okvir jasno razdvaja ova dva pojma budući da isti zahtjevaju različite aktivnosti, organizacijske strukture i služe različitoj svrsi.[36]

Slika 7. Glavni principi CobIT 5 standarda



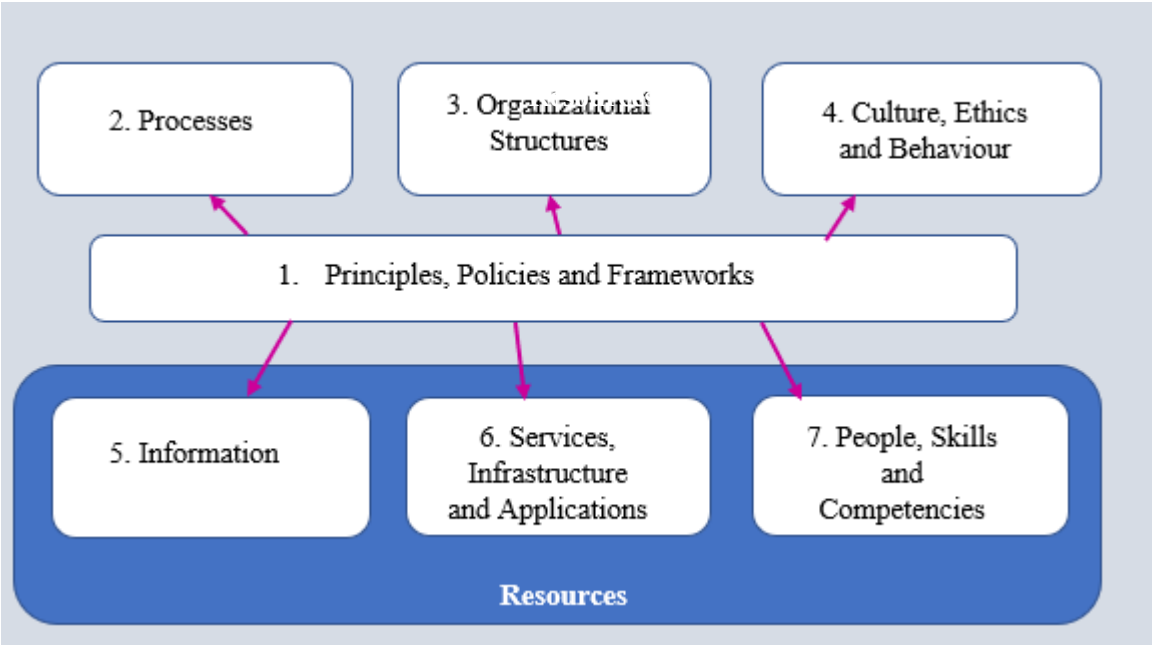
Izvor: IT Governance Institute (2012): CobiT 5 – Framework, Control Objectives, Management Guidlines and Maturity Models, IT Governance Institute, Rolling Meadows, Illionis, SAD, str. 14.

Kako bi se ostvario četvrti cilj CobIT okvir veliku pažnju pridaje pokretačima *(eng. enablers)* koji su podijeljeni u sedam kategorija:

- Principi, politike i okviri (eng. Principles, Policies and Frameworks),
- Procesi *(eng. Processes),*
- Organizacijske strukture *(eng. Organizational Structures),*
- Kultura, etika i ponašanje *(eng. Culture, Ethics and Behaviour),*
- Informacije (*eng. Information),*
- Usluge, infrastruktura i primjene (*eng. Services, Infrastructure and Applications),*
- Ljudi, vještine i kompetencije (*eng. People, Skills and Competencies)*[37]

[36]ISACA (2019) COBIT 2019 Framework: Governance and Management Objectives
[37] Ibid.

Slika 8. Pokretači prema CobIT okviru



Izvor: IT Governance Institute (2012): CobiT 5 – Framework, Control Objectives, Management Guidlines and Maturity Models, IT Governance Institute, Rolling Meadows, Illionis, SAD, str. 18.

CobIT okvir sadrži domene i procese koji predstavljaju okvir u sklopu kojeg se trebaju provesti sva informatička rješenja te služe kao jako dobar alat onima koji se bave planiranjem, uvođenjem i korištenjem informacijskih sustava, a revizor informacijskog sustava utvrđuje dosljednost primjene CobIT okvira. [38]

Među najvažnije kategorije CobIT preporuka se ubrajaju:

- Korporativno upravljanje informatikom *(eng. Governance of Enterprise IT*
    - procjena, usmjeravanje, nadzor.
- Operativno upravljanje informatikom u poslovanju (*eng. IT management)*
    - Usklađivanje, planiranje i organiziranje
    - Nadzor, provjera i procjena
    - Isporuka, usluga i podrška
    - Izgradnja, stjecanje i primjenjivanje.[39]

Domena upravljanja u sklopu CobIT okvira osigurava postizanje ciljeva poduzeća kroz procjenu potreba sudionika poslovnih procesa, uvjeta i mogućnosti, postavljanje smjera kako

[38] Spremić, M. (2005): Revizija informacijskih sustava pomoću CobiT metodologije. Časopis Hrvatske zajednice računovođa i financijskih djelatnika, 51 (2005), 11 , str. 107-112.
[39] Ibid.

bi se oblikovali prioriteti, pravilno donosile odluke i pratile performanse sustava *(eng. Evaluating, Direction, Monitoring – EDM).*[40]

Najvažniji procesi u navedenoj sferi (EDM-u) su:

- EDM 1: osiguravanje postavki i održavanja okvira za upravljanje,
- EDM 2: osiguravanje beneficija,
- EDM 3: osiguravanje optimizacije rizika,
- EDM 4: osiguravanje optimizacije resursa,
- EDM 5: osiguravanje transparentnosti.[41]

Korištenjem sljedećih procesa se unutar domene svrstavanja, planiranja i organiziranja (*eng. Align, Plan and Organize – APO)* razrađuje poslovna tehnologija koja čini osnovu uz pomoć koje se definiraju potrebe informatičke i komunikacijske tehnologije:

- APO 1: upravljanje radnim okvirom IT menadžmenta,
- APO 2: definiranje strateškog IT plana,
- APO 3: definiranje informacijske arhitekture,
- APO 4: upravljanje inovacijama
- APO 5: upravljanje portfolijom,
- APO 6: upravljanje budžetom i troškovima,
- APO 7: upravljanje ljudskim resursima,
- APO 8: upravljanje odnosima,
- APO 9: upravljanje uslugama,
- APO 10: upravljanje dobavljačima,
- APO 11: upravljanje kvalitetom,
- APO 12: upravljanje rizikom i
- APO 13 upravljanje sigurnošću.[42]

Domena za nadgledanje i evaluaciju (*eng. Monitor, Evaluate and Assess – MEA)* služi za praćenje performansi, smjerova rada sustava i poduzimanja određenih ispravaka, a procesi koji se koriste za navedeno su:

- MEA 1: nadziranje, procjena i ocjena performansi i sukladnosti,

[40] ISACA (2019.), op.cit. (bilj. 37), str. 52
[41] Ibid.
[42] Ibid.

- MEA 2: nadziranje, procjena i ocjena sustava internog nadzora,
- MEA 3: nadziranje, procjena i ocjena vanjskih zahtjeva.[43]

Za definiranje postupaka rada programa unutar informacijskog sustava i za pružanje podrške procesima koji omogućuju učinkoviti rad informacijskih sustava koristi se domena isporuke, usluge i podrške *(eng. Delivery, Service and Support – DSS)*. Procesi koji omogućuju navedeno su:

- DSS 1: upravljanje operacijama,
- DSS 2: upravljanje zahtjevima usluga i incidentima,
- DSS 3: upravljanje problemima,
- DSS 4: upravljanje kontinuitetom,
- DSS 5: upravljanje uslugama sigurnosti i
- DSS 6: upravljanje provjerama poslovnog procesa.[44]

Domena izgradnje, stjecanja i primjenjivanja (*eng. Build, Acquire and Implement – BAI)* služi za identifikaciju i alokaciju potrebne tehnologije za poslovne procese te se definiraju načini upravljanja kroz sljedeće procese:

- BAI 1: upravljanje programima i projektima,
- BAI 2: upravljanje definiranim zahtjevima,
- BAI 3: upravljanje pronalaženjem rješenja i izgradnjom,
- BAI 4: upravljanje dostupnošću i kapacitetom,
- BAI 5 :upravljanje mogućnostima mijenjanja organizacije,
- BAI 6: upravljanje promjenama,
- BAI 7: upravljanje prijelazima i prihvaćanjem promjena,
- BAI 8: upravljanje znanjem,
- BAI 9: upravljanje imovinom i
- BAI 10: upravljanje konfiguracijom.[45]

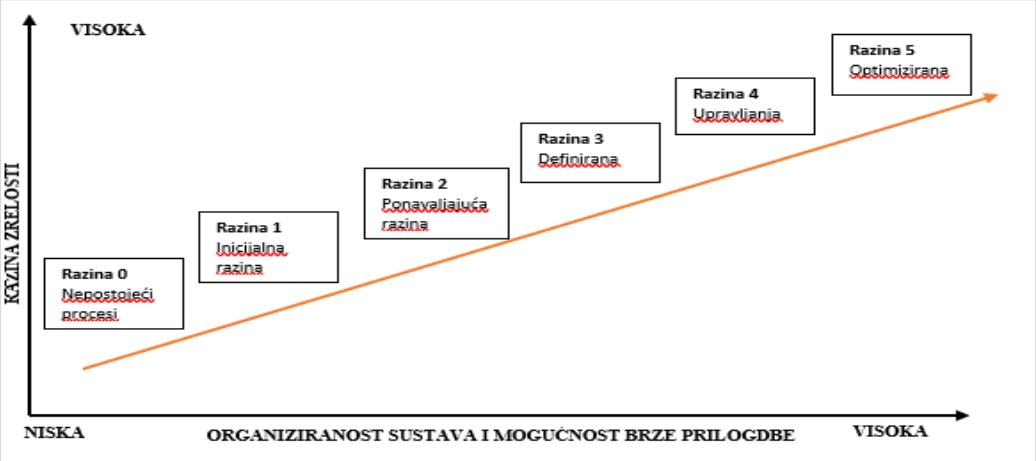
CobIT okvir poprilično jasno određuje i opisuje ključne informatičke procese, precizno određuje područja odgovornosti te ciljeve nadzora i kontrole. Uz sve navedeno, okvir nam daje i modele zrelosti, tj. ciljeve i metrike uspješnosti informatičkih procesa:

[43] Ibid., str. 53
[44] Ibid.
[45] Ibid.

- Kritične čimbenike uspjeha *(eng. CSF – Critical Success Factors),*
- Ključne indikatore ostvarenja ciljeva (*eng. KGI – Key Goal Indicators),*
- Smjernice menadžmentu za praćenje performansi i ključne indikatore performansi (*eng. KPI . Key Performance Indicators),*
- Smjernice menadžmentu za upravljanje rizicima
- Ciljeve kontrola i kontrolne testove
- Pokazatelje ostvarenja zacrtanih aktivnosti (*eng. IT activity goals)*
- Modele zrelosti za svaki poslovni proces (ocjene od 0 do 5 kojima se procjenjuje kvaliteta svakog procesa)
- Sustav kojim se može mjeriti učinkovitost informatike na poslovanje.

Na sljedećoj slici su prikazane ocjene zrelosti procesa informacijskog sustava organizacije gdje 0 označava da procesi upravljanja ne postoje dok 5 označava da su procei upravljanja informatikom optimalni.

Slika 9. Ocjene zrelosti po CobIT okviru



Izvor: prilagođeno prema Spremić, M. (2017.) Sigurnost i revizija informacijskih sustava u okruženju digitalne ekonomije, Zagreb, Ekonomski fakultet

Objašnjenja svake pojedine ocjene zrelosti nalaze se sljedećoj tablici:

Tablica 2. Ocjene zrelosti korporativnog upravljanja informatikom prema CobIT okviru

0 – ne postoji	Proces korporativnog upravljanja informatikom ne postoji te se nije prepoznala važnost istoga. Organizacija nema tijela koja su nadležna za upravljanje informatikom, odluke o ulaganjima u informatiku se donose od slučaja do slučaja bez nekog nadzora i procjene rizika.

1 – početna	Menadžment još uvijek nije osvijestio važnost korporativnog upravljanja informatikom te ne postoje nikakve formalne procedure. Upravljanje nad informatikom se provodi od slučaja do slučaja. Menadžment organizacije nije svjestan važnosti informatičkih rizika, a sam proces upravljanja se provodi unutar IT odjela dok je vrhovni menadžment uglavnom neupućen po pitanjima istoga.
2 – ponavljajuća	Procesi kroporativnog upravljanja informatikom postoje, ali nisu koordinirani te ih pokreće IT odjel ili neka druga operativna organizacijska jedinica. Ne postoji klasična segregacija dužnosti niti postoji nadzor, koordinacija i standardizirane procedure rada. Odgovornost je na pojedinu, nema edukacija zaposlenika , a politike i procedure ne postoje ili pojedinci nisu upoznati s istima.
3 – definirana	Procedure korporativnog upravljanja informatikom postoje te su zaposlenici s istima upoznati i educirani. Međutim, iste nisu prilagođene poslovanju organizacije, a odgovornost za provedbu istih je na pojedincima. Ne postoji sustav nadzora pa je mala vjerojatnost da se uoče anomalije nedjelovanja u skladu s istima.
4 – upravljana i mjerena	Politike i procedure za upravljanje informatikom postoje te je moguće nadzirati provedbu istih kao i mjeriti uspješnost i raditi potrebne prepravke u provođenju istih. Navedeno je u nadležnosti korporativnih tijela koja su odgovarajuća. Organizacije neprestano unaprjeđuju aktivnosti i procese te postavljaju jasne ciljeve upravljanja informatikom koji su usklađeni s poslovnim ciljevima. Provedba ciljeva je jasno mjerljiva te za isto koriste suvremene metode i okvire.
5 - optimalna	Proces korporativnog upravljanja informatikom je na zavidnoj razini. Uspješnost i efikasnost informatike se neprestano mjeri, a rezultati se uspoređuju s dobrim praksama i drugim organizacijama. Proces upravljanja informatikom je transparentan te korporativna tijela imaju stvaran nadzor nad istim. Prepoznala se važnost korištenja informatike u strateške svrhe, a sve informatičke aktivnosti se odvijaju prema poslovnim prioritetima koji su unaprijed i realno definirani. .

Izvor: Spremić, M. (2017.) Sigurnost i revizija informacijskih sustava u okruženju digitalne ekonomije, Zagreb, Ekonomski fakultet

2.3.2. Objašnjenje norme ISO27001

ISO / IEC 27001 međunarodni je standard o upravljanju informacijskom sigurnošću. Standard su izvorno zajednički objavili Međunarodna organizacija za standardizaciju (ISO) i Međunarodna elektrotehnička komisija (IEC) 2005.[46], a zatim revidirani 2013.[47] U njemu su detaljno navedeni zahtjevi za uspostavljanje, provedbu, održavanje i kontinuirano poboljšanje sustava upravljanja informacijskom sigurnošću (ISMS) - čiji je cilj pomoći organizacijama da informacijsku imovinu koju posjeduju učine sigurnijom. [48] Europsko ažuriranje standarda objavljeno je 2017.[49] Organizacije koje ispunjavaju zahtjeve standarda mogu odabrati da ih certificira akreditirano certifikacijsko tijelo nakon uspješnog završetka revizije.

Većina organizacija ima niz kontrola informacijske sigurnosti. Međutim, bez sustava upravljanja informacijskom sigurnošću (ISMS), kontrole su donekle neorganizirane i razdvojene, budući da su često implementirane kao rješenje neke specifične. Sigurnosne kontrole u radu obično se posebno bave određenim aspektima informacijske tehnologije (IT) ili sigurnosti podataka; ostavljajući ne-informacijsku imovinu (poput papira i vlasničkog znanja) u cjelini manje zaštićenom. Štoviše, planiranjem kontinuiteta poslovanja i fizičkom sigurnošću može se upravljati sasvim neovisno o informatičkoj ili informacijskoj sigurnosti, dok se prakse ljudskih resursa mogu malo osvrtati na potrebu definiranja i dodjeljivanja uloga i odgovornosti u informacijskoj sigurnosti u cijeloj organizaciji.

ISO / IEC 27001 standard zahtijeva da menadžment:

- Sustavno ispituje rizike informacijske sigurnosti organizacije uzimajući u obzir prijetnje, ranjivosti i utjecaje.
- Dizajnira i implementira koherentan i sveobuhvatan paket kontrola sigurnosti podataka i / ili drugih oblika adresiranja rizika (poput izbjegavanja rizika ili prijenosa rizika) kako bi se riješili oni rizici koji se smatraju neprihvatljivima; i

[46] ISO/IEC 27001 International Information Security Standard published. Dostupno na: https://www.bsigroup.com/en-GB/about-bsi/media-centre/press-releases/2005/11/ISOIEC-27001-International-Information-Security-Standard-published/ [09. lipnja 2021.]
[47] New version of iso/iecISO/IEC 27001 to better tackle it security risks“. Dostupno na: https://www.iso.org/news/2013/08/Ref1767.html [09.lipnja 2021.]
[48] ISO/IEC 27001:2013. Dostupno na: https://www.iso.org/standard/54534.html [09. lipnja 2021.]
[49] BS EN ISO/IEC 27001:2017 – what has changed? Dostupno na: https://www.bsigroup.com/en-GB/iso-27001-information-security/BS-EN-ISO-IEC-27001-2017/ [09. lipanj 2021.]

- Usvoji sveobuhvatni postupak upravljanja kako bi se osiguralo da kontrole sigurnosti informacija i dalje udovoljavaju trajnim potrebama organizacije u pogledu informacijske sigurnosti.

Standard sadrži ukupno 10 skupina kontrola kojima se reguliraju sljedeća područja:

A.5 Sigurnosna politika

A.5.1 Politika informacijske sigurnosti

A.6 Organizacija informacijske sigurnosti

A.6.1 Unutarnja organizacija

A.6.2 Vanjske stranke

A.7 Upravljanje resursima

A.7.1 Odgovornost za resurse

A.7.2 Klasifikacija informacija

A.8 Sigurnost vezana uz osoblje

A.8.1 Prije zapošljavanja

A.8.2 Tijekom rada

A.8.3 Prekid ili promjena uvjeta zapošljavanja

A.9 Fizička sigurnost i sigurnost okruženja

A.9.1 Sigurna područja

A.9.2 Zaštita opreme

A.10 Upravljanje komunikacijama i operativnim postupcima

A.10.1 Operativne procedure i odgovornosti

A.10.2 Upravljanje uslugama trećih strana

A.10.3 Planiranje i prihvaćanje sustava

A.10.4 Zaštita od zlonamjernog i mobilnog koda

A.10.4.1 Zaštita od zlonamjernog koda

A.10.4.2 Zaštita od mobilnog koda

A.10.5 Pričuvna pohrana

A.10.6 Upravljanje sigurnošću mreža

A.10.7 Upravljanje podatkovnim medijima

A.10.8 Razmjena informacija

A.10.9 Usluge elektroničke trgovine

A.10.10 Nadzor

A.11 Kontrola pristupa

A.11.1 Poslovni zahtjevi za kontrolu pristupa

A.11.2 Upravljanje pristupom korisnika

A.11.3 Odgovornosti korisnika

A.11.4 Kontrola pristupa mreži

A.11.5 Kontrola pristupa operativnom sustavu

A.11.6 Kontrola pristupa do aplikacija i informacija

A.11.7 Mobilno računarstvo i rad s udaljenih lokacija

A.12 Nabavka, razvoj i održavanje informacijskih sustava

A.12.1 Sigurnosni zahtjevi informacijskih sustava

A.12.2 Pravilno procesiranje u aplikacijama

A.12.3 Kriptografske kontrole

A.12.4 Sigurnost sistemskih datoteka

A.12.5 Sigurnost u procesima razvoja i podrške

A.12.6 Upravljanje tehničkim ranjivostima

A.13 Upravljanje incidentima informacijske sigurnosti

A.13.1 Izvješćivanje o sigurnosnim događajima i ranjivostima

A.13.2 Upravljanje incidentima informacijske sigurnosti i poboljšavanja

A.14 Upravljanje kontinuitetom poslovanja

A.14.1 Aspekti informacijske sigurnosti vezani za upravljanje kontinuitetom poslovanja

A.15 Sukladnost

A.15.1 Sukladnost sa zakonima i regulativom

A.15.2 Sukladnost sa sigurnosnim politikama i standardima, i tehnička sukladnost

A.15.3 Razmatranje pitanja audita informacijskih sustava[50]

2.3.3. Objašnjenje metodologije ITIL *(Information Technology Infrastructure Library)*

IT Infrastructure Library (ITIL) knjižnica je svezaka koji opisuju okvir najboljih praksi za pružanje IT usluga. ITIL je kroz povijest prošao kroz nekoliko revizija, a trenutno obuhvaća pet knjiga, od kojih svaka pokriva različite procese i faze životnog ciklusa IT usluga. ITIL-ov sustavni pristup upravljanju IT uslugama može pomoći tvrtkama u upravljanju rizicima, ojačati odnose s kupcima, uspostaviti isplativu praksu i izgraditi stabilno IT okruženje koje omogućuje rast, razvoj i promjene.[51]

ITIL okvir je razvila britanska Central Computer and Telecommunications Agency (CCTA) tijekom 1980.-ih, a koja danas postoji pod imenom Office of Government Commerce (OGC), tj. Cabinet Office. Tijekom osamdesetih godina izdala je prvi popis uputa za korištenje informatičkih usluga kojih su se trebale pridržavati sva tijela u javnoj administraciji u Velikoj Britaniji.[52]

ITIL je prvotno sadržavao više od trideset knjiga koje su sadržavale najbolje prakse u informacijskoj tehnologiji prikupljene s različitih izvora. OGC je odlučio usvojiti ovaj projekt

[50] ISO (2018.) ISO/IEC 27000:2018

[51] "What is ITIL? Your guide to the IT Infrastructure Library", dostupno na: https://www.cio.com/article/2439501/infrastructure-it-infrastructure-library-itil-definition-and-solutions.html, [15. lipnja 2021.]

[52] Spremić, M., Kostić, D. (2008.), Upravljanje kvalitetom informatičke usluge: Studije slučaja primjene ITIL metode, Business Excellence; Zagreb Vol. 2, Iss. 1, 2008., str. 42

kao dio svoje misije rada s javnim sektorom Velike Britanije kako bi postigao efikasnost, dobio dodanu vrijednost u prodajnim aktivnostima i poboljšao uspješnost ispostave programa i projekta. Cilj je zapravo bio prikupiti najbolje svjetske prakse na jednom mjestu budući da se uvidjelo da javni sektor sve više ovisi informacijskoj tehnologiji kojoj manjkaju standardizirane procedure koje bi pojedine greške svele na minimum i spriječile njihovo konstantno ponavljanje, a samim time i gomilanje troškova.[53]

ITIL upute su se konstantno nadograđivale i unaprjeđivale, a sada u svijetu čine općeprihvaćeni standard za upravljanje informatičkim uslugama. Ovaj okvir pruža poslovno orijentiran pristup menadžmentu informatike koji zapravo naglašava stratešku vrijednost informatike i potrebu da se isporuči usluga visoke kvalitete. Uz sve to, ITIL okvir daje smjernice i preporuke za rad ljudi, funkcioniranje procesa i korištenje tehnologije prilikom korištenja informatike za pružanje kvalitetnih usluga. [54]

Druga verzija ITIL okvira je nastala početkom 2000-ih godina te je sadržavala osam knjiga, treća verzija okvira je sadržavala pet knjiga, tj. pet ključnih procesa: strategija usluga, oblikovanje usluga, isporuka usluge, korištenje usluge i stalno unaprjeđenje usluga.[55]

Zadnja verzija, ITIL 4, izašla 2019. godine, zadržava isti fokus na automatizaciji procesa, poboljšanju upravljanja uslugama i integriranju IT odjela u posao. Međutim, također ažurira okvir kako bi se prilagodio modernoj tehnologiji, alatima i softveru i odgovorio na njega. Od posljednjeg ažuriranja ITIL-a, odjel za informatiku postao je sastavni dio svake organizacije, a novi okvir to prilagođava agilnijim, fleksibilnijim i suradljivijim.[56]

ITIL 4 sadrži devet vodećih načela koja su usvojena na najnovijem ispitu ITIL Practitioner Exam, koji pokriva upravljanje organizacijskim promjenama, komunikaciju i mjerenje i metriku.[57]

Najnovija verzija ITIL-a usredotočena je na kulturu poduzeća i integriranje IT-a u cjelokupnu poslovnu strukturu. Potiče suradnju između IT-a i ostalih odjela, posebno jer se druge poslovne jedinice sve više oslanjaju na tehnologiju kako bi obavile posao. ITIL 4 također naglašava

[53] „What is ITIL? Your guide to the IT Infrastructure Library", loc.cit.
[54] Spremić, M., Kostić, D. (2008.), op.cit., str. 43
[55] „What is ITIL? Your guide to the IT Infrastructure Library", loc.cit.
[56] Ibid.
[57] Ibid.

povratne informacije kupaca, jer je organizacijama lakše nego ikad ranije razumjeti njihovu percepciju javnosti, zadovoljstvo i nezadovoljstvo kupaca.[58]

2.3.4. Objašnjenje metodologije PCI DSS *(Payment Card Industry Data Security Standard)*

Payment Card Industry Data Security Standard (PCI DSS) je standard informacijske sigurnosti za organizacije koje se služe kreditnim karticama u svojem poslovanju. PCI DSS zahtjevaju karičarske kuće, a njime upravlja tijelo Vijeće za sigurnosne standarde industrije platnih kartica (*Payment Card Industry Security Standards Council*) koje je sastavljeno od predstavnika kartičarskih kuća (Visa, MasterCard, American Express i ostali). Standard je stvoren kako bi se povećala kontrola podataka o vlasnicima kartica i kako bi se smanjio broj prevara s kreditnim karticama.[59]

PCI DSS razvijen je kako bi se potaknula i poboljšala sigurnost podataka vlasnika kartice i olakšalo usvajanje dosljednih mjera sigurnosti podataka na globalnoj razini. PCI DSS pruža polaznu osnovu tehničkih i operativnih zahtjeva koji su dizajnirani za zaštitu podataka računa. PCI DSS odnosi se na sve subjekte koji su uključeni u obradu platnih kartica - uključujući trgovce, procesore,stjecatelje, izdavatelje i pružatelje usluga. pregled 12 zahtjeva PCI DSS-a na visokoj razini.[60]

U tablici 3. su prikazani PCI DSS zahtjevi i dan je pregled upravljačkih kontrola:

Tablica 3. PCI DSS ciljevi i zahtjevi

CILJ	PCI DSS ZAHTJEV
Izgradnja i održavanje sigurne mrežne infrastrukture	1) Instalirati i održavati konfiguraciju vatrozida
	2) Ne koristiti predefinirane i zadane sistemske lozinke i druge sigurnosne parametre
Zaštita kartičarskih podataka	3) Zaštiti pohranjene kartične podatke
	4) Osigurati enkripciju prijenosa karticčnih podataka putem javne mreže (*data in transit)*

[58] Ibid.
[59] PCI DSS – Requirements and Security Assessment Procedures, version 3.2.1., PCI Security Standard Council, LLC, 2006-2018., str. 5
[60] Ibid.

CILJ	PCI DSS ZAHTJEV
Održavanje programa za upravljanje ranjivostima	5) Korištenje i redovno nadograđivanje antivirusnog softvera ili programa
	6) Razvijanje i održavanje sigurnosti sustava i aplikacija
Implementacija jakih mjera kontrole pristupa	7) Ograničiti pristup kartičnim podacima prema poslovnoj potrebi
	8) Identificirati i autentificirati pristup komponentama sustava
	9) Ograničiti fizički pristup kartičarskim podacima
Redoviti nadzor i kontrola / testiranje mreža	10) Praćenje i nadzor nad svim pristupom mrežnim resursima i kartičarskim podacima
	11) Redovito testiranje sustava i procesa
Održavanje opće politike sigurnosti informacijskog sustava	12) Održavanje politike koja propisuje sigurnost informacijskih sustava za sve zaposlenike

Izvor: prevedeno i prilagođeno prema PCI DSS – Requirements and Security Assessment Procedures, version 3.2.1., PCI Security Standard Council, LLC, 2006-2018., str. 5

Za svaki od navedenih ciljeva propisana je procedura testiranja te svojevrsno objašnjenje samog procesa testiranja ili pojašnjenje pojmova (tzv. *Guidance)* što znantno olakšava proces revizije informacijskog sustava u skladu s PCI DSS standardom.[61]

2.3.5. Objašnjenje NIST metodologije

NIST Cybersecurity Framework je okvir koji daje smjernice unutarnjim i vanjskim dionicima organizacija za upravljanje i smanjenje rizika kibernetičke sigurnosti. Popisuje specifične, i za organizaciju prilagodljive, aktivnosti povezane s upravljanjem kibernetičkim rizikom, a temelji se na postojećim standardima, smjernicama i praksama.[62]

[61] Ibid., str. 20
[62] NIST, Framework for Improving Critical Infrastructure Cybersecurity, version 1.1., April 2018., str. V – VI.

Okvir pruža zajednički jezik za razumijevanje, upravljanje i izražavanje kibernetičkog rizika za unutarnje i vanjske dionike. Pomoću njega može se identificirati i dati prioritet akcijama za smanjenje kibernetičkog rizika kibernetičke sigurnosti, a ujedno je i alat za usklađivanje politike, poslovanja i tehnološkog pristupa upravljanju navedenim rizikom.[63]

Okvir pruža skup aktivnosti za postizanje specifičnih rezultata kibernetičke sigurnosti i navodi primjere smjernica za postizanje tih ishoda. Predstavlja ključne ishode kibernetičke sigurnosti koje su dionici identificirali kao korisne u upravljanju kibernetičkim rizikom. Okvir se sastoji od četiri elementa: funkcije (*eng.functions)*, kategorije *(eng. categories)*, podkategorije (*eng. subcategories)* i informativne reference *(eng. informative references)* prikazane na slici :

Slika 9. Struktura NIST okvira

Izvor:preuzeto iz NIST, Framework for Improving Critical Infrastructure Cybersecurity, version 1.1., April 2018., str. 6

Svi ti elementi rade zajedno:

- **Funkcije** organiziraju glavne aktivnosti kibernetičke sigurnosti na najvišoj razini. Funkcije su Identificirati (*eng. Identify)*, Zaštiti (*eng. Protect)*, Otkriti (*eng. Detect)*, Odgovoriti (*eng. Respond)* i Oporaviti *(eng. Recover)*. Pomažu organizaciji u izražavanju

[63] Ibid., str. 6

upravljanja kibernetičkim rizikom kroz organizaciju informacija, omogućavanje donošenja odluka baziranih na procjeni rizika, adresiranju prijetnji i poboljšanju.

- **Kategorije** su podjela funkcija u grupe ishoda kibernetičke sigurnosti koji su usko vezani uz programske potrebe i određene aktivnosti. Primjeri kategorija su upravljanje imovinom, upravljanje kontrolama pristupa, načini i procesi detekcije i sl.
- **Podkategorije** dalje dijele kategorije u specifične ishode tehničkih i/ili upravljačkih aktivnosti. Daju set rezultata koji pomažu u postizanju ishoda za svaku kategoriju. Primjerice, „Postoji repozitorij vanjskih informacijskih sustava“, „Podaci u mirovanju su zaštićeni“ i „Notifikacije koje je poslao sustav za detekciju su pregledane te su poduzete odgovarajuće akcije“.
- **Informativne reference** su specifični dijelovi standarda, smjernica i praksi koje su zajedničke sektoru kritične infrastrukture koji daju upute kako postići ishode svake pojedine potkategorije. [64]

Funkcije neće dovesti do statičkog željenog stanja nego iste treba uspostaviti na način da se kontinuirano odvijaju kako bi, kroz vrijeme, stvorile operativnu kulturu koja će adresirati kibernetičke rizike unutar organizacije.

- **Funkcija identifikacije** služi za razvoj organizacijskog razumijevanja upravljanja kibernetičkim rizikom kroz sustave, ljude, imovinu, podatke i sposobnosti.
- **Funkcija zaštite** služi za razvoj i implementaciju određenih zaštitnih mjera kako bi se osigurala isporuka kritičnih usluga.
- **Funkcija otkrivanja / detekcije** služi za razvoj i implementaciju aktivnosti za otkrivanje događaja / incidenata koji bi narušili kibernetičku sigurnost.
- **Funkcija odgovora** služi za razvoj i implementaciju odgovarajućih aktivnosti za poduzimanje mjera nakon identifikacije sigurnosnog incidenta.
- **Funkcija oporavka** služi za razvoj i implementaciju odgovarajućih aktivnosti za održavanje planova otpora i povrata usluga ili servisa koji su bili predmetom sigurnosnog incidenta.[65]

U niže navedenoj tablici dan je pregled funkcija i kategorija:

[64] Ibid., str. 6 -7
[65] Ibid., str. 7

Tablica 4. Tablični prikaz funkcija i kategorija unutar NIST okvira

ID funkcije	Funkcija	ID kategorije	Kategorija
ID	Identifikacija (*Identify)*	ID.AM	Upravljanje imovinom *(Asset Management)*
		ID.BE	Poslovna okolina (*Business Environment)*
		ID.GV	Upravljanje *(Governance)*
		ID.RA	Procjena rizika (*Riska Assessment)*
		ID.RM	Strategija upravljanja rizicima (*Risk Management Strategy)*
		ID.SC	Upravljanje rizicima lanaca dobave (*Supply Chain Risk Management*)
PR	Zaštita *(Protect)*	PR.AC	Upravljanje identitetom i kontrola pristupa *(Identity Management and Access Control)*
		PR.AT	Edukacije *(Awareness and Training)*
		PR.DS	Sigurnost podataka *(Data Security)*
		PR.IP	Procesi i procedure zaštite informacija (*Information Protection Processes and Procedures)*
		PR.MA	Održavanje *(Maintenance)*
		PR.PT	Zaštitna tehnologija *(Protective Technology)*
DE	Detekcija *(Detection)*	DE.AE	Anomalije i događaji *(Anomalies and Events)*
		DE.CM	Kontinuirano sigurnosno praćenje *(Security Continuous Monitoring)*
		DE.DP	Procesi detekcije *(Detection Processes)*
RS	Odgovor *(Response)*	RS.RP	Planiranje odgovora *(Response Planning)*
		RS.CO	Komunikacije *(Communications)*
		RS.AN	Analiza *(Analysis)*
		RS.MI	Mitigacija (*Mitigation)*
		RS.IM	Poboljšanja (*Improvements)*
RC	Oporavak *(Recovery)*	RC.RP	Planiranje oporavka *(Recovery Planning)*
		RC.IM	Poboljšanja *(Improvements)*
		RC.CO	Komunikacije *(Communications)*

Izvor: NIST, Framework for Improving Critical Infrastructure Cybersecurity, version 1.1., April 2018., str. 23

2.3.6. Objašnjenje SANS metodologije

Područja kibernetičke sigurnosti, tj. upravljačke kontrole kibernetičke sigurnosti (*eng. cybersecurity controls – CSC)* su u najnovijoj verziji okvira (verziji 8) podijeljene osamnaest područja, za razliku od prethodne verzije koja je imala 20.[66]

[66] SANS Institute, CIS controls, dostupno na: https://www.sans.org/blog/cis-controls-v8/, [15. lipnja 2021.]

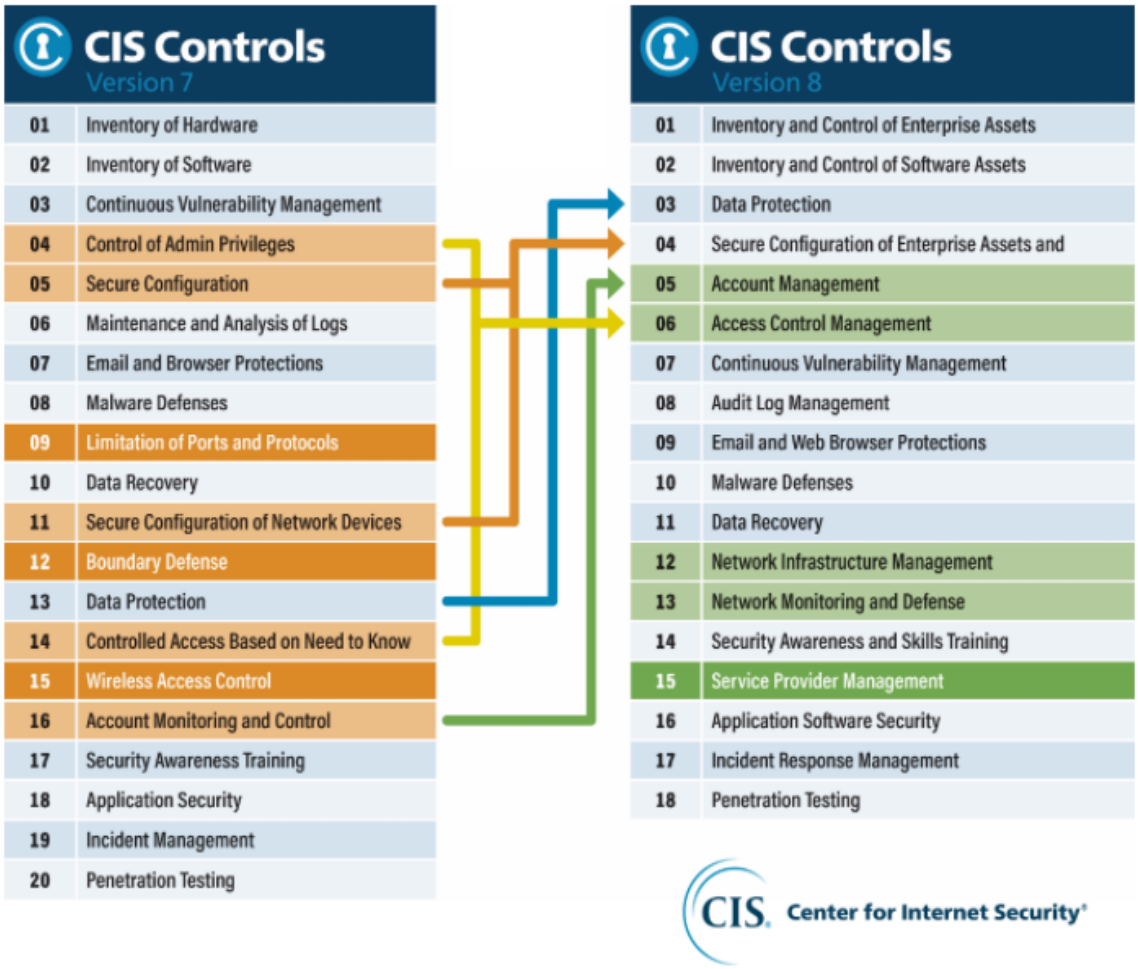
Tablica 5. SANS kontrole

CSC KONTROLE	
1	Popis i kontrola imovine Društva *(Inventory and Control of Enterprise Assets)*
2	Popis i kontrola softverske imovine *(Inventory and Control of Software Assets)*
3	Zaštita podataka *(Data Protection)*
4	Sigurna konfiguracija imovine Društva i mrežnih uređaja *(Secure Configuration of Enterprise Assets and Network Devices*
5	Upravljanje računima *(Account Management)*
6	Upravljanje kontrolama pristupa *(Access Control Management)*
7	Kontinuirano upravljanje ranjivostima *(Continuous Vulnerability Management)*
8	Upravljanje zapisima rada sustava *(Audit Log Management)*
9	Zaštita elektroničke pošte i internetskog preglednika *(Email and Web Browser Protection*
10	Zaštita od zlućudnog koda *(Malware Defenses)*
11	Povrat / oporavak podataka *(Data Recovery)*
12	Upravljanje mrežnom infrastrukturom *(Network Infrastructure Management)*
13	Nadzor i zaštita mreže *(Network Monitoring and Defense)*
14	Osvješćivanje o sigurnosti i edukacije *(Security Awareness and Skills Training)*
15	Upravljanje dobavljačima usluga *(Service Provided Management)*
16	Sigurnost aplikativnog softvera *(Application Software Security)*
17	Upravljanje incidentima *(Incident Response Management)*
18	Penetracijska testiranja *(Penetration Testing)*

Izvor: SANS Institute, CIS controls, dostupno na: https://www.sans.org/blog/cis-controls-v8/, [15. lipnja 2021.]

Razlike između verzije 7 i verzije 9 SANS okvira su prikazane na slici 10.

Slika 10. Razlike između verzije 7 i verzije 8 SANS okvira



Izvor: SANS Institute, CIS controls, dostupno na: https://www.sans.org/blog/cis-controls-v8/, [15. lipnja 2021.]

3. PREGLED TRENDOVA KORIŠTENJA POJEDINIH METODOLOGIJA U ODABRANIM VRSTAMA PODUZEĆA

U nadolazećim poglavljima će biti prikazan trend korištenja pojedinih metodologija za kontrolu i reviziju informacijskih sustava u Republici Hrvatskoj u odabranim vrstama poduzeća. Kao vrste poduzeća su odabrana telekomunikacijska industrija, kreditne institucije i osiguravajuća društva budući da navedene industrije imaju obvezu provođenja regulatornih revizija i izvještavanja prema regulatoru.

3.1. Telekomunikacijska industrija

3.1.1. eTOM

Okvir poslovnog procesa *(eng. The Business Process Framework – eTOM)* okvir je operativnog modela za pružatelje telekomunikacijskih usluga u telekomunikacijskoj industriji. Model opisuje potrebne poslovne procese pružatelja usluga i definira ključne elemente i način na koji bi isti trebali komunicirati.[67]

eTOM je standard je koji održava TM Forum, udruženje za pružatelje usluga i njihove dobavljače u telekomunikacijskoj i zabavnoj industriji.[68]

Područja u eTOM okviru su podijeljena u tri kategorije: proizvod, strategija i infrastruktura. Unutar ovih kategorija pružaju se smjernice o marketingu, uslugama, razvoju resursa, razvoju lanaca opskrbe i upravljanju u svim tim područjima. eTOM standard također obuhvaća odnose s kupcima, usluge, resurse i upravljanje odnosima s opskrbnim partnerima. Unutar okvira se mogu pronaći savjeti o strateškom i poslovnom planiranju, upravljanju rizicima te upravljanju financijama, imovinom i znanjem.[69]

Također, navedeni standard postavlja arhitekturu za stvaranje poslovnih praksi koje slijede procese usmjerene na kupca, poput početne prodaje, korisničke podrške, naplate, marketinga, daljnje korisničke podrške i podrške nakon servisa.

[67] Business Process Framework – eTOM, R17.0.0, dostupno na: https://www.tmforum.org/resources/suite/gb921-business-process-framework-etom-r17-0-1/, [18. lipnja 2021.]
[68] Ibid.
[69] Ibid.

3.2. Kreditne institucije

Sukladno definiciji Uredbe EU br. 575/2013 pojam kreditne institucije obilježava ono društvo čija je primarna djelatnost primanje depozita i/ili ostalih povratnih sredstava od javnosti te odobravanje kredita za vlastiti račun.[70] U Republici Hrvatskoj kao kreditne institucije mogu poslovati banke, štedne banke i stambene štedionice, a iste se nalaze pod nadzorom Hrvatske narodne banke (u daljnjem tekstu „HNB“).[71]

Navedene institucije su obvezne osigurati poslovanje informacijskih sustava sukladno Odluci o primjerenom upravljanju informacijskim sustavom te, ukoliko su uvrštene kao sistemski važne kreditne institucije, Uredbom o kibernetičkoj sigurnosti.

3.2.1. Odluka o primjerenom upravljanju informacijskim sustavom Hrvatske narodne banke

Odluka o primjerenom upravljanju informacijskim sustavom (u daljnjem tekstu „Odluka“) je donesena od strane HNB-a 2010. godine te definira obveze kreditnih institucija koje se odnose na upravljanje informacijskim sustavom. Odluka definira devet područja upravljanja informacijskim sustavom (ne računajući uvod i završne odredbe) koje su prikazane u tablici 6.[72]

Tablica 6. Područja koja definira Odluka o primjerenom upravljanju informacijskim sustavom

Područje u Odluci	Sažetak
1) Okvir za upravljanje informacijskim sustavom	Definira se obveza određivanja člana Uprave nadležnog za nadzor nad upravljanjem informacijskim sustavom, obveza uspostavljanja odgovarajuće organizacijske strukture, obveza donošenja strategije informacijskog sustava i usklađenosti s poslovnom strategijom, obveza donošenja internih akata koji uređuju upravljanje informacijskim sustavom, obveza izvješćivanja Uprave i nadzornog odbora, obveza imenovanja Odbora za upravljanje informacijskim sustavom, obveza propisivanja metodologije upravljanja projektima
2) Upravljanje rizikom informacijskog sustava	Definira samo da se u upravljanju rizikom kreditne institucije moraju voditi Zakonom o

[70] Uredba EU br. 575/2013, dostupno na: https://eur-lex.europa.eu/legal-content/HR/TXT/?uri=celex%3A32013R0575 [18. lipnja 2021.]
[71] Zakon o kreditnim institucijama, dostupno na: https://www.zakon.hr/z/195/Zakon-o-kreditnim-institucijama, [18. lipnja 2021.]
[72] Odluka o primjerenom upravljanju informacijskim sustavom, dostupno na: https://narodne-novine.nn.hr/clanci/sluzbeni/2010_03_37_958.html, [18. lipnja 2021.]

	kreditnim institucijama i propisima donesenima na temelju navedenog Zakona.
3) Upravljanje ugovornim odnosima	Definira obvezu procjene rizika ugovornog odnosa i nadzora načina i kvalitete pruženih usluga.
4) Unutarnja revizija	Definira sadržaj metodologije interne revizije.
5) Sigurnost informacijskog sustava	Definira obvezu donošenja internog akta koji će biti okvir za upravljanje sigurnosti informacijskog sustava, obvezu klasifikacije i zaštite informacija, obvezu kontrole pristupa resursima kreditne institucije, obvezu uspostavljanja procesa administracije korisničkih prava, obvezu izrade i čuvanja operativnih i sistemskih zapisa, obvezu zaštite resursa od malicioznog koda.
6) Održavanje informacijskog sustava	Definira obvezu uspostavljanja procesa upravljanja hardverskom imovinom te definira što isti treba obuhvatiti, obvezu uspostavljanja procesa upravljanja promjenama softverskih komponenti te što isti treba obuhvatiti, obvezu definiranja postupaka izrade, pohrane, održavanja i čuvanja dokumentacije, obvezu edukacije zaposlenika na temu informacijske sigurnosti.
7) Upravljanje kontinuitetom poslovanja	Poziva na usklađivanje s Odlukom o upravljanju rizicima. Također, definira obvezu donošenja i testiranja planova oporavka, obvezu uspostavljanja upravljanja incidentima te obvezu obavještavanja regulatora po nastanku ozbiljnijeg incidenta, obvezu uspostavljanja procesa upravljanja pričuvnom pohranom.
8) Razvoj informacijskog sustava	Definira obvezu uspostavljanja načina, kriterija i postupaka razvoja informacijskog sustava, obvezu usklađenosti navedenog procesa s metodologijom o upravljanju promjenama i projektima, obvezu dokumentiranja procesa programskog razvoja, obvezu razdvajanja programskih okolina.
9) Elektroničko bankarstvo	Definira obvezu primjene sigurnih i učinkovitih autentifikacijskih metoda i multifaktorske autentifikacije, obvezu osiguravanja odgovarajuće potvrde vlastitog identiteta, obvezu postojanja operativnih i sistemskih zapisa.

Izvor: izrada autora prema Odluci o primjerenom upravljanju informacijskim sustavom, dostupno na: https://narodne-novine.nn.hr/clanci/sluzbeni/2010_03_37_958.html, [18. lipnja 2021.]

Navedena Odluka definira obveze kreditnih institucija na višoj razini, dok Smjernice za upravljanje informacijskim sustavom u cilju smanjenja operativnog rizika (u daljnjem tekstu „Smjernice“) detaljnije razrađuju obveze i postupke ostvarenja istih. Pregled poglavlja i potpoglavlja je dan u tablici 7.[73]

Tablica 7. Područja obrađena u Smjernicama za upravljanje informacijskim sustavom u cilju smanjenja operativnog rizika

Definirana poglavlja po područjima	Potpoglavlja
1) Uvod	1.1. Temeljna načela informacijskog sustava 1.2. Ciljevi, strategije i ostali interni akti 1.3. Sigurnost informacijskog sustava 1.4. Elementi upravljanja rizikom
2) Upravljanje informacijskim sustavom	2.1. Uprava banke 2.2. Voditelj organizacijske jedinice za informacijsku tehnologiju 2.3. Voditelj sigurnosti informacijskog sustava 2.4. Odbor za upravljanje informacijskim sustavom 2.5. Upravljanje projektima
3) Upravljanje rizikom informacijskog sustava	3.1. Procjena rizika 3.2. Smanjivanje rizika 3.3. Kontrole 3.4. Klasifikacija informacija
4) Unutarnja revizija	N/A
5) Sigurnost informacijskog sustava	5.1. Politika sigurnosti informacijskog sustava 5.2. Upravljanje kontrolama pristupa 5.3. Kriptografija 5.4. Fizička sigurnost 5.5. Upravljanje operativnim i sistemskim zapisima 5.6. Zaštita od malicioznog koda
6) Održavanje informacijskog sustava	6.1. Upravljanje imovinom informacijskog sustava 6.2. Upravljanje promjenama 6.3. Upravljanje konfiguracijama 6.4. Dokumentacija 6.5. Izobrazba
7) Planiranje kontinuiteta poslovanja	7.1. Analiza utjecaja na poslovanje 7.2. Plan kontinuiteta poslovanja 7.3. Plan oporavka 7.4. Upravljanje incidentima 7.5. Upravljanje pričuvnom pohranom
8) Razvoj sustava i eksternalizacija	8.1. Razvoj informacijskog sustava

[73] Smjernice za upravljanje informacijskim sustavom u cilju smanjenja operativnog rizika, dostupno na: https://www.hnb.hr/documents/20182/639854/h-smjernice-za-upravljanje-informacijskim-sustavom.pdf/e5579931-e846-47ab-af23-6809debef700, [18. lipnja 2021.]

	8.2. Eksternalizacija (dijela) informacijskog sustava
9) E-bankarstvo	9.1. Uvod 9.2. Rizici povezani s e-bankarstvom 9.3. Upravljanje rizikom e-bankarstva

Izvor: izrada autorice prema Smjernicama za upravljanje informacijskim sustavom u cilju smanjenja operativnog rizika, dostupno na: https://www.hnb.hr/documents/20182/639854/h-smjernice-za-upravljanje-informacijskim-sustavom.pdf/e5579931-e846-47ab-af23-6809debef700, [18. lipnja 2021.]

3.2.2. Uredba o kibernetičkoj sigurnosti Vlade Republike Hrvatske

Budući da u hrvatskom kreditnom sustavu postoje i sistemski važne kreditne institucije, tj. sve one banke koje su zbog svoje veličine, međusobne povezanosti i značajnih prekograničnih aktivnosti ocjenjene kao značajne od strane HNB-a[74], na njih se još dodatno primjenjuje Uredba o kibernetičkoj sigurnosti (u daljnjem tekstu „Uredba“) koju je 2018. godine donijela Vlada Republike Hrvatske kao podzakonski akt temeljen na Zakonu o kibernetičkoj sigurnosti.[75]

Uredbom se utvrđuju mjere za postizanje visoke razine kibernetičke sigurnosti ključnih operatera usluga[76] te se navedeno odnosi na ukupno sedam sistemski važnih banaka koje je HNB kao takvima proglasio u 2020. godini, a to su: Zagrebačka banka d.d., Privredna banka Zagreb d.d., Erste&Steiermärkische Bank d.d, Raiffeisenbank Austria d.d., OTP banka Hrvatska d.d., Addiko Bank d.d. te Hrvatska poštanska banka d.d.[77]

Uredba sadrži sedam poglavlja koja obuhvaćaju različita područja kibernetičke sigurnosti, a ista su navedena u tablici 8. Poglavlja su vrlo slična gore navedenim Smjernicama, međutim ista detaljnije obrađuju određena područja od samih Smjernica.

Tablica 8. Područja sukladno Uredbi o kibernetičkoj sigurnosti

Područje	Sadržaj
1) Upravljanje sigurnošću mrežnih i informacijskih sustava	• Okvir upravljanja • Načela sigurnosti • Uspostava i dokumentiranje politike upravljanja

[74] Sistemski važne institucije, dostupno na: https://www.hnb.hr/temeljne-funkcije/financijska-stabilnost/makrobonitetne-mjere/sistemski-vazne-institucije, [18. lipnja 2021.]
[75] Uredba o kibernetičkoj sigurnosti, dostupno na: https://narodne-novine.nn.hr/clanci/sluzbeni/full/2018_07_68_1399.html, [18. lipnja 2021.]
[76] Ibid.
[77] Priopćenje o rezultatima preispitivanja sistemske važnosti kreditnih institucija u Republici Hrvatskoj, dostupno na: https://www.hnb.hr/documents/20182/2293886/h-priopcenje-preispitivanje-sistemski-vaznih-ki-u-RH_10-12-2020.pdf/283d1d22-0145-b6a4-fec3-577293ac5646?t=1607595350135, [18. lipnja 2021.]

	• Organizacijska struktura • Provedba internih nadzora
2) Upravljanje rizicima	• Uspostava sustava upravljanja rizicima • Procjena rizika • Identifikacija opreme, osoba i aktivnosti u okviru kojih se provodi procjena rizika • Sprječavanje, otkrivanje i rješavanje incidenata te ublažavanje učinka incidenata • Dokumentacija o procjeni rizika
3) Područja zaštite ključnih sustava	• Fizička sigurnost i sigurnost okruženja • Sigurnost opskrbe • Upravljanje ugovornim odnosima • Upravljanje eksternalizacijom • Kontrola pristupa prostorima • Fizičko i logičko razdvajanje ključnih sustava • Kontrola pristupa ključnom sustavu • Dnevnik aktivnosti ključnih sustava • Zaštita podataka koji se obrađuju, pohranjuju i prenose u ključnom sustavu • Zaštita od zlonamjernog programskog koda • Zaštita od narušavanja raspoloživosti ključnog sustava • Razvoj i održavanje ključnih sustava • Upravljanje projektima • Upravljanje sklopovskom imovinom • Upravljanje promjenama programske imovine • Konfiguracija ključnih sustava • Preventivne provjere ranjivosti ključnih sustava • Upravljanje kontinuitetom poslovanja • Pričuvna pohrana
4) Obvezno obavješćivanje o incidentima	• Obveza obavješćivanja • Incidenti sa znatnim učinkom na kontinuitet pružanja ključne usluge • Incidenti sa znatnim učinkom na kontinuitet pružanja digitalne usluge • Procjena učinka incidenta na kontinuitet pružanja ključne usluge • Procjena učinka incidenta na kontinuitet pružanja digitalne usluge
5) Obavijesti o incidentima sa znatnim učinkom na kontinuitet pružanja usluge	• Vrste obavijesti • Inicijalna obavijest o incidentu sa znatnim učinkom • Prijelazno izvješće o incidentu sa znatnim učinkom

	• Završno izvješće o incidentu sa znatnim učinkom • Dostava obavijesti o incidentima sa znatnim učinkom • Razmjena obavijesti
6) Postupanje po obavijestima o incidentima sa znatnim učinkom	• Rješavanje incidenata sa znatnim učinkom • Evidencije o incidentima sa znatnim učinkom
7) Obaviješćivanje o incidentima na dobrovoljnoj osnovi	N/A

Izvor: izrada autorice prema Uredbi o kibernetičkoj sigurnosti, dostupno na: https://narodne-novine.nn.hr/clanci/sluzbeni/full/2018_07_68_1399.html, [18. lipnja 2021.]

Zavod za sigurnost informacijskih sustava i Hrvatska akademska i istraživačka mreža - CARNET izradili su dokument "Okvir dobrih praksi za usklađivanje operatora ključnih usluga s mjerama Zakona o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga i provođenje ocjene sukladnosti" koji daje detaljne smjernice, preporuke i dobre prakse za ostvarivanje sukladnosti s mjerama sigurnosti propisanima u navedenoj Uredbi.[78] Ovime se uvelike olakšalo, kako organizacijama, tako i revizorima informacijskih sustava budući da je razjašnjeno koje mjere je potrebno poduzeti kako bi revizori mogli reći da je informacijski sustav organizacije u skladu s navedenim aktima.

3.3. Osiguravajuća društva

Osiguravajuća društva su ona društva koja primaju uplata premije osiguranja , a kada nastane osigurani slučaj, tj. šteta onda imaju obvezu isplate naknade za nastalu štetu.[79] Nadzor nad istima ima Hrvatska agencija za nadzor financijskih usluga (u daljnjem tekstu „HANFA“) te su osiguravajuća društva obvezna osigurati poslovanje informacijskih sustava sukladno Smjernicama za primjereno upravljanje rizicima informacijskog sustava subjekata nadzora.

3.3.1. Smjernice za primjereno upravljanje rizicima informacijskog sustava subjekata nadzora Hrvatske agencije za nadzor financijskih usluga

Smjernice za primjereno upravljanje rizicima informacijskog sustava subjekata nadzora su donesene 2014. godine od strane HANFA-e kojima je cilj razviti svijest subjekata nadzora o

[78] Okvir dobrih praksi za usklađivanje operatora ključnih usluga s mjerama Zakona o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga i provođenje ocjene sukladnosti, dostupno na: https://www.zsis.hr/UserDocsImages/Okvir_dobrih_praksi-v1.pdf, [18.lipnja 2021.]
[79] HANFA osiguranje, dostupno na: https://www.hanfa.hr/getfile.ashx/?fileId=42496, [18. lipnja 2021.]

rizicima informacijskih sustava te upoznati subjekte nadzora s dobrim praksama ublažavanja rizika informacijskih sustava.[80]

Navedenim Smjernicama su obuhvaćene dvije kategorije koje su podijeljene u područja vezanima za kontrolu i upravljanje informacijskim sustavom (tablica 10).

Tablica 9. Kategorije i područja sukladno Smjernicama za primjereno upravljanje rizicima informacijskih sustava subjekata nadzora

Kategorija	Područje
A) Ključni aspekti upravljanja rizicima informacijskog sustava	1. Osnovna načela upravljanja rizicima informacijskog sustava 2. Identifikacija, procjena i postupanje s rizicima informacijskog sustava
B) Mjere i postupci za smanjenje rizika informacijskog sustava	1. Organizacija i upravljanje informacijskim sustavom 2. Razvoj i održavanje informacijskog sustava 3. Upravljanje promjenama u informacijskom sustavu 4. Izdvajanje procesa informacijskog sustava 5. Neprekinutost poslovanja i oporavak nakon katastrofe 6. Fizička i okolišna sigurnost 7. Logičke kontrole pristupa 8. Sigurnost računalnih mreža 9. Sigurnost prijenosnih uređaja i medija za pohranu podataka 10. Upravljanje incidentima 11. Upravljanje operativnim i sistemskim zapisima 12. Zaštita od malicioznog koda

Izvor: izrada autorice prema Smjernicama za primjereno upravljanje rizicima informacijskih sustava subjekata nadzora, dostupno na: https://www.hanfa.hr/getfile/41744/7-Smjernice%20za%20primjereno%20upravljanje%20rizicima%20IS%20subjekata%20nadzora%20Agencije.pdf, [18. lipnja 2021.]

S obzirom da se navedene Smjernice raspisane na (samo) dvadeset i sedam stranica vidljivo je kako iste ne daju detaljnije upute kako bi osiguravajuća društva trebala urediti pojedina područja upravljanja informacijskim sustavom. Također, Smjernice niti ne propisuju neke uobičajene svjetske sigurnosne prakse (primjerice, redovno skeniranje ranjivosti mreže). Međutim, 2020. godine je Europsko nadzorno tijelo za osiguranje i strukovno mirovinsko osiguranje (EIOPA) donijelo Smjernice za sigurnost i upravljanje sigurnošću informacijskih i

[80] Smjernice za primjereno upravljanje rizicima informacijskih sustava subjekata nadzora, dostupno na: https://www.hanfa.hr/getfile/41744/7-Smjernice%20za%20primjereno%20upravljanje%20rizicima%20IS%20subjekata%20nadzora%20Agencije.pdf, [18. lipnja 2021.]

komunikacijskih tehnologija gdje je detaljnije nadopunila i definirala područja na koja se organizacije trebaju osvrnuti prilikom upravljanja informacijskim sustavom. Rok za implementaciju istih u lokalnu regulativu je 01. srpnja 2021. godine te se pretpostavlja kako će i HANFA tada donijeti nadopunjene Smjernice.[81]

4. ANALIZA KORIŠTENJA RAZLIČITIH METODOLOGIJA ZA PROVOĐENJE REVIZIJE INFORMACIJSKIH SUSTAVA

4.1. Cilj i metodologija istraživanja

Cilj istraživanja je bio provesti ispitivanje nad stručnjacima iz područja revizije informacijskih sustava kao i nad stručnjacima upravljanja informacijskim sustavom kojim bi se dobio uvid koju metodologiju (ili kombinaciju metodologija) stručnjaci preferiraju u praksi te koja od navedenih metodologija (ili kombinacija metodologija) najviše pokriva područje sigurnosti informacijskog sustava.

Također, htio se dobiti i uvid u to kakvo obrazovanje su ispitanici stekli (tehničko ili ekonomsko) te dobiti uvid koje od tih vještina su prihvatljivije u području revizije i upravljanja informacijskim sustavima.

Kao metoda istraživanja je odabran anketni upitnik koji je formiran putem Google Forms aplikacije. Anketa je bila podijeljena u dva dijela. U prvom dijelu se htjelo dobiti na uvid u kojoj vrsti poduzeća ispitanici rade te kakvo su obrazovanje stekli. Ovisno o njihovom odgovoru na pitanje u kojoj industriji su zaposleni anketa ih je vodila na različite setove pitanja. Drugi dio ankete se odnosio na ispitivanje mišljenja o važnosti tehnoloških i poslovnih vještina za reviziju i upravljanje informacijskim sustavima gdje su ispitanicima postavljene tvrdnje. U drugom dijelu ankete se za vrednovanje tvrdnji koristila Likertova ljestvica od 1 do 5 (1 – uopće se ne slažem s tvrdnjom; 2 – ne slažem se; 3 – niti se slažem, niti se ne slažem; 4 – slažem se; 5 – u potpunosti se slažem s navedenom tvrdnjom).

Pretragom različitih izvora nije bilo moguće pronaći previše sličnih istraživanja, međutim, istraživanje Spremića, M., u sklopu znanstvenog rada za Zbornik Ekonomskog fakulteta je bilo

[81] EIOPA finalises Guidelines on Information and Communication Technology Security and Governance, dostupno na: https://www.eiopa.europa.eu/content/eiopa-finalises-guidelines-information-and-communication-technology-security-and-governance_en, [18. lipnja 2021.]

poprilično slično, iako nije imalo isti cilj[82]. Zbog svega navedenog, autorica je kreirala anketna pitanja uz konzultaciju navedenog znanstvenog rada gdje su joj pitanja poslužila kao svojevrsna nit vodilja kako bi znala u kojem smjeru istraživanje treba krenuti. Međutim, autorica je pitanja prilagodila i nadodala vlastita pitanja kako bi ostvarila cilj istraživanja.

4.2. Objašnjenje uzorka i načina provedbe ankete

Anketa se provodila putem Google Forms aplikacije. Ciljana skupina su bili stručnjaci iz područja revizije informacijskih sustava kao i stručnjaci upravljanja informacijskim sustavom (CISO, CIO, i slično) iz telekomunikacijske industrije, kreditnih institucija i osiguravajućih kuća. Uz navedene industrije, populaciju su sačinjavali i revizori (vanjski i interni) koji se bave revizijom ovakvih organizacija.

Razlog ovako usko odabrane populacije leži u tome što navedene tri industrije podliježu regulatornim pregledima u Republici Hrvatskoj te imaju obvezu izvještavanja prema regulatornim tijelima (kako je već navedeno u trećem poglavlju ovoga rada). Anketa je poslana na otprilike 60 adresa elektroničke pošte, a vratilo se (samo) 17 korektno ispunjenih upitnika čime je stopa odgovora iznosila oko 28%. Svi vraćeni upitnici su bili korektno ispunjeni što se smatra zadovoljavajući ako uzmemo u obzir osjetljivost teme, međutim, razlog korektnom ispunjavanju se može pripisati i tome što je anketa bila u potpunosti anonimna (nisu se prikupljale mail adrese niti bilo kakvi drugi osobni podaci) kako bi udovoljavala uvjetima GDPR-a, ali i kako bi potakla ispitanike da bez ustručavanja ispune upitnik.

Istraživanja u ovakvom području su vrlo rijetka, čime svjedoči činjenica nemogućnosti pronalaska većeg broja sličnih istraživanja nego. Uz to što su rijetka, vrlo su teška za provođenje budući da se radi o osjetljivim temama o kojima uglavnom menadžment ne želi javno govoriti.

4.3. Rezultati provedenog istraživanja i diskusija

U ovom dijelu rada prikazat će se rezultati istraživanja u više dijelova. Prvo će se prikazati rezultati nekih osnovnih podataka (formalno obrazovanje, industrija rada, veličina poduzeća).

[82] Spremić, M. (2007.) Metode provedbe revizije informacijskih sustava, Zbornik Ekonomskog fakulteta Zagreb, str. 295. – 311.

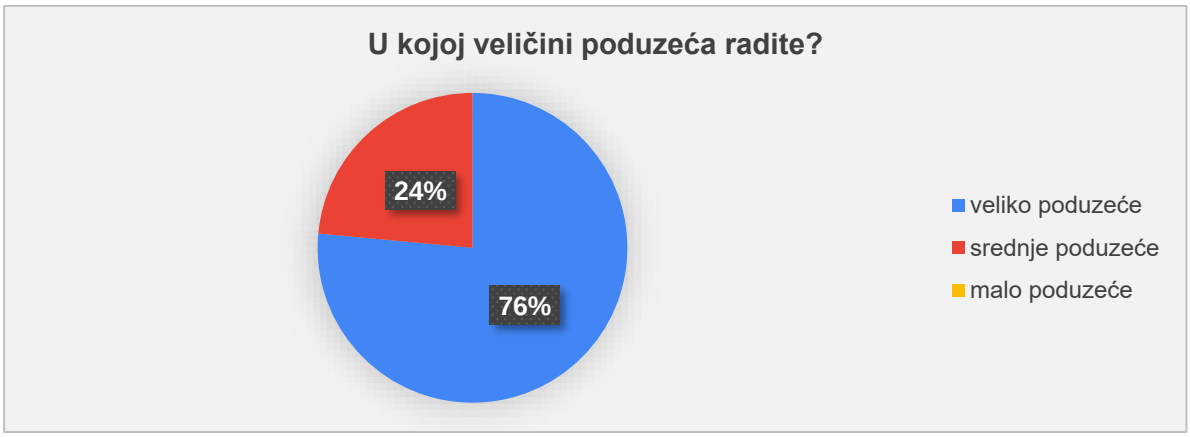
Nakon toga će se odvojeno prikazati rezultati istraživanja za kreditne institucije, osiguravajuće kuće i telekomunikacijska Društva od rezultata istraživanja za revizorske kuće. Nadalje, unutar istraživanja za revizorske kuće prikazat će se rezultati za vanjskog i internog revizora.

Na kraju će biti prikazani rezultati mišljenja o važnosti tehnoloških i poslovnih vještina za reviziju i upravljanje informacijskim sustavima te će se raspraviti ograničenja samog istraživanja i preporuke za buduću praksu.

4.3.1. Rezultati istraživanja – uvodni dio

Na grafikonu 1 vidimo kako je istraživanje je pokazalo da većina ispitanika (76,5%) radi u velikim poduzećima, dok ostatak radi u srednjim poduzećima. Ovakvi rezultati nisu iznenađujući budući da istraživanje provedeno na vrlo maloj populaciji koja je obuhvaćala one vrste organizacija koje podliježu regulatornim revizijama.

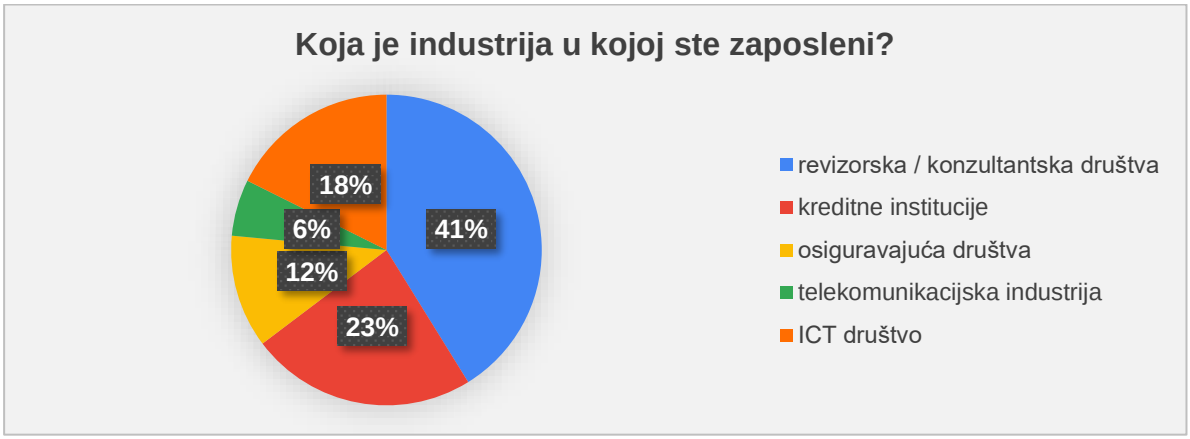
Grafikon 1. Veličina poduzeća



Izvor: samostalna obrada autorice

Nadalje, na grafikonu 2 je prikazano kako većina zaposlenika radi u revizorskoj / konzultantskoj kući, a nakon toga slijede kreditne institucije, ICT društva i osiguravajuće kuće. Najmanje ispitanika je radilo u telekomunikacijskoj industriji.

Grafikon 2. Industrija zaposlenja



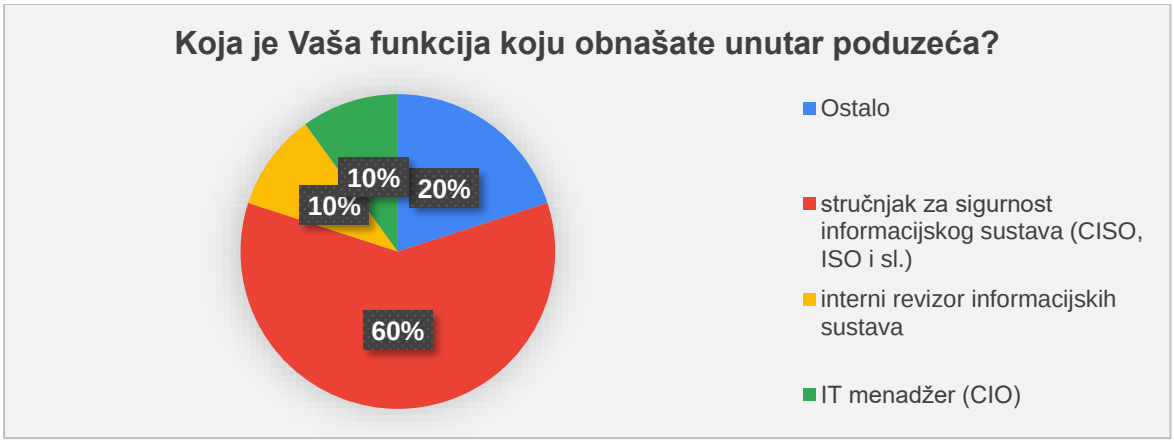
Izvor: samostalna obrada autorice

Ovisno o odgovoru na prethodno pitanje slijedio je set pitanja vezanih uz odabranu industriju te će rezultati biti razrađeni u nadolazećim potpoglavljima

4.3.2. Rezultati istraživanja – kreditne institucije, osiguravajuća društva, telekomunikacijska industrija i ostalo

Istraživanje je provedeno većim dijelom nad stručnjacima za sigurnost informacijskog sustava (CISO, ISO i slično) dok su manjim dijelom uzorak sačinjavali IT menadžeri (CIO), interni revizori informacijskih sustava i ostali (uglavnom sistem integratori).

Grafikon 3. Funkcija ispitanika unutar poduzeća

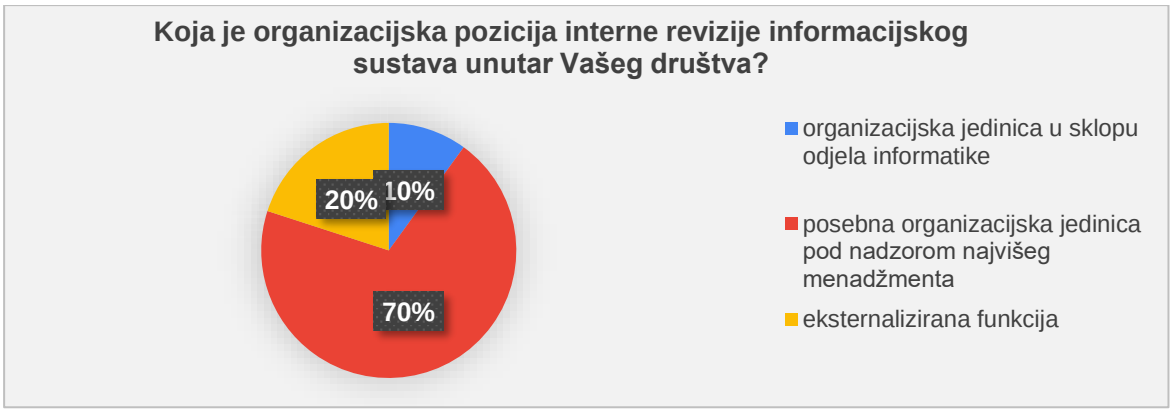


Izvor: samostalna obrada autorice

U istraživanju kreditnih institucija, osiguravajućih te telekomunikacijskih društava je Istraživanje je pokazalo kako u kreditnim institucijama, osiguravajućim društvima i telekomunikacijama interna revizija većinski zauzima mjesto posebne organizacijske jedinice pod nadzorom najvišeg menadžmenta, što je u skladu s dobrim praksama budući da se ovime osigurava da kontrole unutar organizacije budu revidirane od strane potpuno neovisnog odjela koje nije sudjelovalo u dizajniranju istih (tj. nema sukoba interesa).

U 20% slučajeva interna revizija je eksternalizirana funkcija što opet osigurava nepristranost, a u 10% slučajeva interna revizija se nalazi kao organizacijska jedinica u sklopu odjela informatike.

Grafikon 4. Pozicija interne revizije



Izvor: samostalna obrada autorice

Nadolazeći set pitanja imao je cilj uvidjeti kakav je način nadzora i kontrole informacijskih sustava, tj. koliko Društvo zapravo ima uspostavljenu kontrolu nad istim.

Istraživanje je pokazalo da sve ispitane kreditne institucije, osiguravajuća društva i telekomunikacijska društva imaju formalno usvojenu opću politiku informacijske sigurnosti. Navedena politika je krovni interni akt koji definira opseg i načine zaštite informacijskih sustava organizacije. Navedeni rezultat nije iznenađujući budući da je jedan od temeljnih zahtjeva regulatora zapravo posjedovanje ovakvog internog akta koji je formalno usvojen od strane Uprave organizacije.

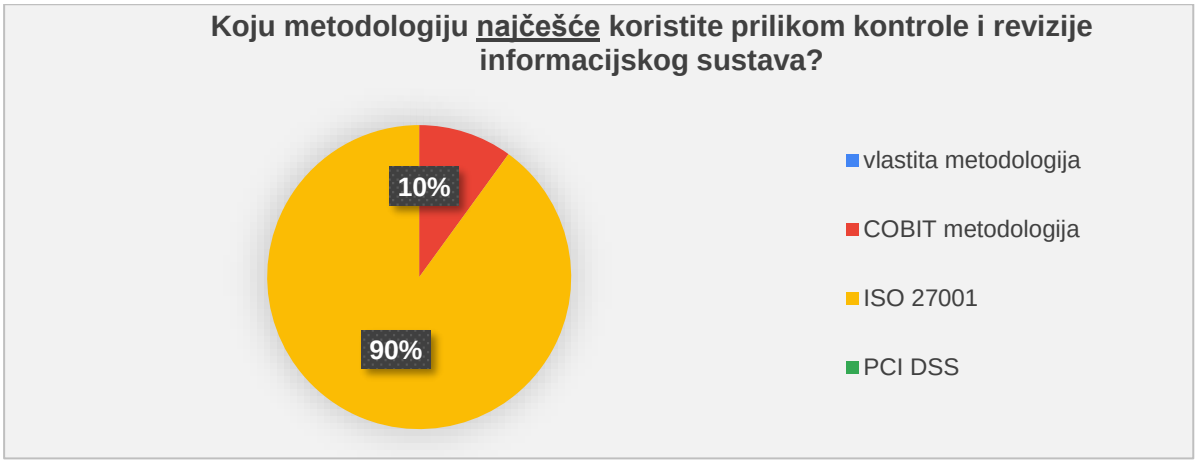
Grafikon 5. Opća politika informacijske sigurnosti

Izvor: samostalna obrada autorice

Nadalje, istraživanje je pokazalo kako većina ispitanih Društava **najčešće** koristi ISO27001 metodologiju za kontrolu i reviziju informacijskih sustava, dok manji dio (10%) koristi COBIT metodologiju. Navedeni rezultat možemo pripisati tome što se većina Društava želi certificirati kako bi mogli pokazati dionicima i vanjskim revizorima kako su u skladu s ISO27001 okvirom. U navedenom pitanju je naglas na riječ **najčešće** što znači da to nije i jedina metodologija koja se koristi prilikom kontrole i revizije informacijskih sustava.

Razlog ovakve formulacije pitanja leži u ograničenju Google Forms aplikacije koja prilikom odabira pitanja s višestrukim odgovorima ne dozvoljava postavljanje uvjeta da se ispitanik odvede na određeni dio ankete ovisno o odabranom odgovoru.

Grafikon 6. Najčešće korištena metodologija

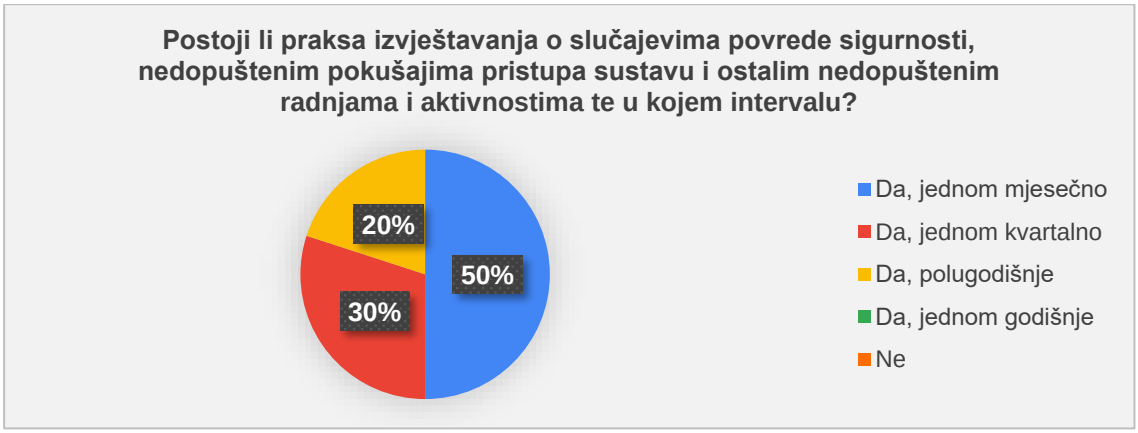


Izvor: samostalna obrada autorice

Istraživanje je pokazalo da u ovakvim vrstama organizacija postoji praksa izvještavanja o slučajevima povrede sigurnosti, nedopuštenim pokušajima pristupa sustavu i ostalim

nedopuštenim radnjama i aktivnostima i to najčešće jednom mjesečno (50%), a iz toga slijedi jednom kvartalno i polugodišnje. Ovakva praksa pokazuje kako Društva slijede dobre sigurnosne prakse budući da je ovakvo izvještavanje ključno kako bi menadžment imao pravovremeni nadzor nad sigurnošću informacijskog sustava te kako bi se mogle otkriti slabe točke zaštite istoga i pravovremeno adresirati.

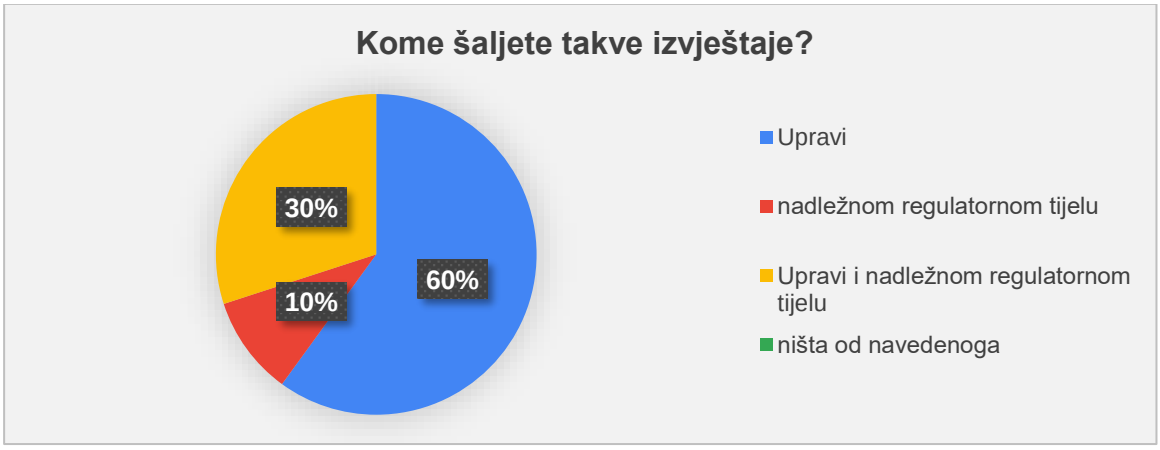
Grafikon 7. Praksa izvještavanja



Izvor: samostalna obrada autorice

Ovakvi izvještaji se većinom šalju Upravi, dok samo 30% njih ovakav izvještaj šalje Upravi i nadležnom tijelu. Ovakav rezultat se može pripisati tome da neki regulatori ne obvezuju slanje izvještaja nadležnom tijelu, međutim, slanje istoga je dobra praksa. U 10% slučajeva ovakvi izvještaji se šalju samo nadležnom regulatornom tijelu, što može dovesti do toga da sama Uprava organizacije neće pravovremeno biti upoznata s istima te neće možda ulagati previše sredstava u dodatnu informatičku infrastrukturu u svrhu zaštite informacijskih sustava od takvih napada u budućnosti.

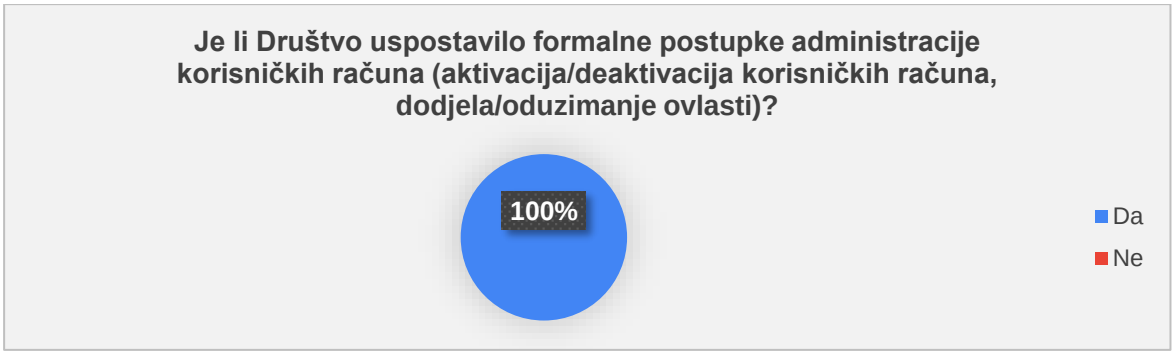
Grafikon 8. Slanje izvještaja



Izvor: samostalna obrada autorice

Nadalje, istraživanje je pokazalo da sva ispitana Društva imaju formalno uspostavljene postupke administracije korisničkih računa što znači da su uspostavili proces dodjeljivanja i oduzimanja ovlasti te proces aktivacije i deaktivacije korisničkih računa. Ovakav proces je ključan kako bi se spriječili neovlašteni pristupi informacijskom sustavi te kako bi se zaposlenicima dodijelila minimalno potrebna prava za rad i izbjegle zlouporabe ovlasti unutar informacijskog sustava.

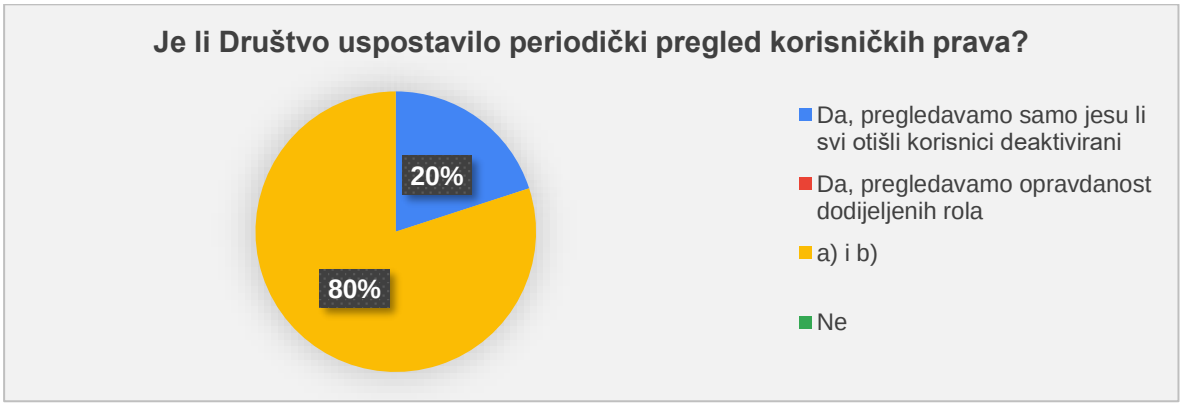
Grafikon 9. Administracija korisničkih računa



Izvor: samostalna obrada autorice

Rezultati ovog dijela istraživanja su pokazali kako još uvijek postoji mjesta za poboljšanje proces periodičkog pregleda korisničkih prava budući da 20% ispitanika pregledava samo jesu li korisnicima, koji su napustili organizaciju, deaktivirani korisnički računi. Dobre prakse nalažu kako bi kvalitetan periodički pregled prava trebao biti dizajniran na način da, uz potvrdu deaktivacije korisničkih računa, pregleda i opravdanost dodijeljenih rola trenutno aktivnim korisnicima u sustavu kako bi se izbjegle situacije u kojima korisnik prilikom promijene odjela zadrži stara prava i privilegije koje mu trenutno nisu potrebne i time posjeduje više prava od onih koja su mu minimalno potrebna čime se organizacija izlaže riziku zloupotrebe istih.

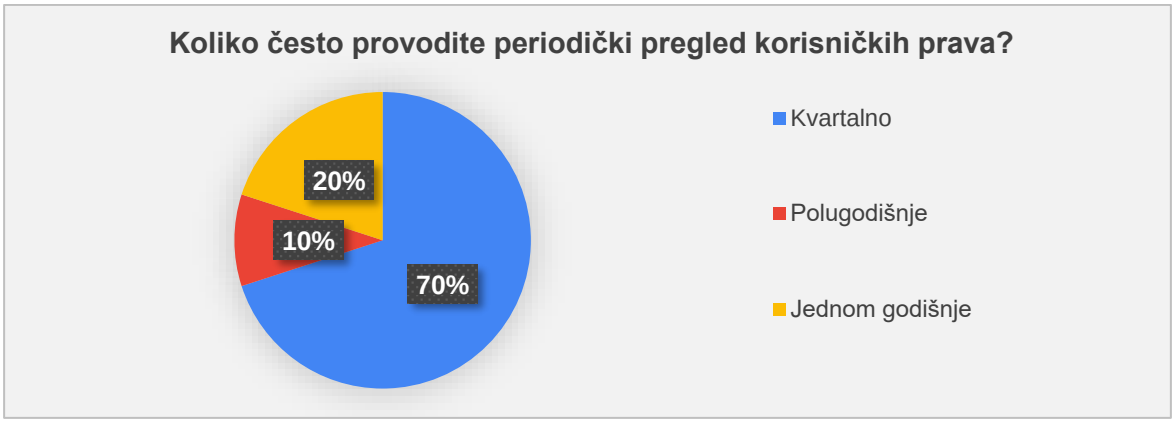
Grafikon 10. Periodički pregled korisničkih prava



Izvor: samostalna obrada autora

Također, istraživanje je pokazalo kako 70% organizacija provodi periodički pregled korisničkih prava na kvartalnoj razini dok 20% njih provodi isti samo jednom godišnje. Provođenjem periodičkog pregleda prava samo jednom godišnje organizacija se izlaže riziku da neće pravovremeno uočiti nepravilnosti u dodijeljenim rolama i deaktiviranim računima što može rezultirati neovlaštenim pristupom sustavu.

Grafikon 11. Učestalost periodičkog pregleda prava



Izvor: samostalna obrada autorice

Rezultati sljedećeg dijela istraživanja ukazuju na to da iako je donesena opća politika informacijske sigurnosti koja propisuje osnovne smjernice, zahtijevanje provođenja istih u praksi je puno opsežniji posao. Potrebno je posvetiti više pažnje realnom provođenju propisane politike kako bi informacijski sustavi organizacije bili pravovremeno zaštićeni. U tome glavnu ulogu imaju planovi kontinuiteta poslovanja *(eng. business continuity plans)* i planovi oporavka nakon katastrofe *(eng. disaster recovery plans)* koje posjeduje oko 80% anketiranih organizacija koje podliježu regulatornim revizijama. Ono što se svakako smatra pozitivnim je da niti jedna od anketiranih organizacija nije odgovorila da ne posjeduje navedene planove što pokazuje kako je svijest o važnosti istih porasla.

Grafikon 12. Plan kontinuiteta poslovanja i plan oporavka od katastrofe

Izvor: samostalna obrada autorice

Međutim, istraživanje je pokazalo kako testiranje navedenih planova nije uvijek redovito. Od anketiranih organizacija njih 60% provodi testiranja planova kontinuiteta poslovanja i planova oporavka od katastrofe jednom godišnje. Njih 30% testiranja provodi jednom u dvije godine dok 10% uopće ne provodi navedena testiranja.

Grafikon 13. Testiranje plana kontinuiteta poslovanja i plana oporavka of katastrofe

Izvor: samostalna obrada autorice

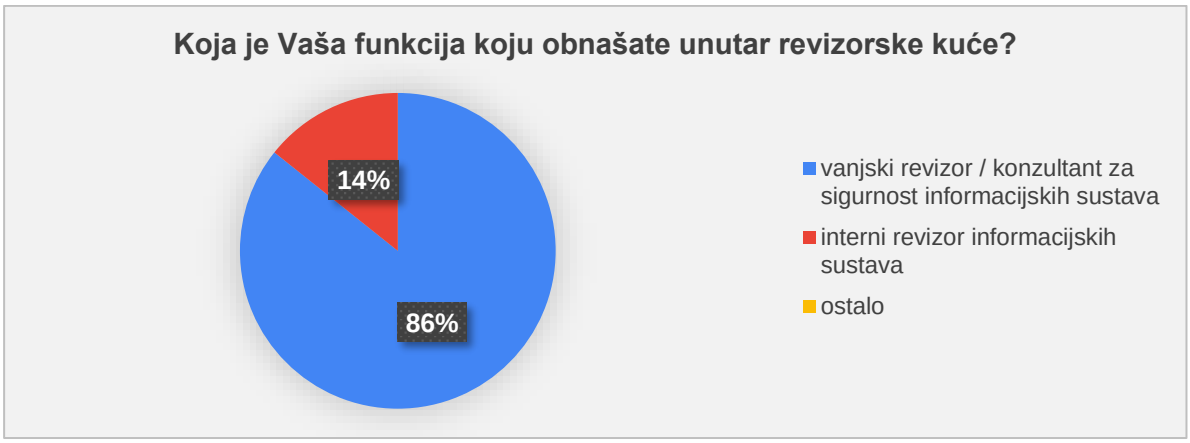
Iako regulatori navode da je testiranje istih potrebno provoditi u redovitim intervalima, ne specificirajući koji su to intervali, dobre prakse pokazuju kako je najbolje testirati navedene planove minimalno jednom godišnje kako bi se osiguralo da, u slučaju potrebe, kontinuitet poslovanja bude netaknut. Testiranjem planova jednom u dvije godine, ili čak njihovim netestiranjem, organizacija neće biti u mogućnosti prepoznati može li sustave i servise, ključne za poslovanje, ponovno uspostaviti u zadanom vremenskom intervalu (koji je sama propisala).

Svrha testiranja je simulirati scenarije najgoreg mogućeg slučaja i detektirati potencijalne probleme u provođenju plana kontinuiteta i plana oporavka od katastrofe. Ovo se pokazalo izrazito važnim u 2020. godini kada je svijet pogodila pandemija korona virusa koja je natjerala većinu poslovanja na udaljeni rad te kada su Hrvatsku pogodila dva jaka potresa.

4.3.3. Rezultati istraživanja – revizorska društva

Istraživanje je pokazalo kako su anketni upitnik većinom ispunili vanjski revizori / konzultanti za sigurnost informacijskog sustava dok su ostatak činili interni revizori unutar revizorskog društva.

Grafikon 14. Funkcija ispitanika unutar revizorskog društva



Izvor: samostalna obrada autorice

U nadolazećim potpoglavljima će se analizirati rezultati ovisno o funkciji koju ispitanici obnašaju unutar revizorske kuće. Set pitanja za internog revizora i za vanjske revizore / konzultante je bio drugačiji budući da je pogled na samu reviziju drugačiji.

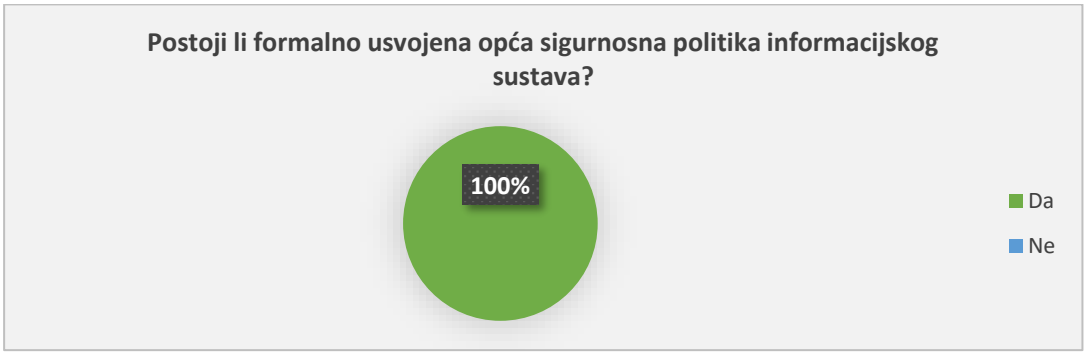
Interni revizor je mogao ispunjavati pitanja koja su se odnosila na samo revizorsko društvo i cilj je bio pokazati jesu li revizorska društva u skladu sa standardima i dobrim sigurnosnim praksama.

Vanjski revizor je odgovarao na pitanja vezana uz provođenje revizije nad trećim stranama (klijentima) te je cilj bilo dobiti uvid u korištene metodologije te stav o propisanim standardima i smjernicama u Republici Hrvatskoj kojih su se revizori dužni pridržavati prilikom provođenja revizije informacijskih sustava.

4.3.3.1. Rezultati istraživanja – revizorska društva – interni revizori

Rezultati istraživanja pokazuju kako sva anketirana revizorska društva posjeduju usvojenu opću politiku informacijske sigurnosti koja je krovni interni akt.

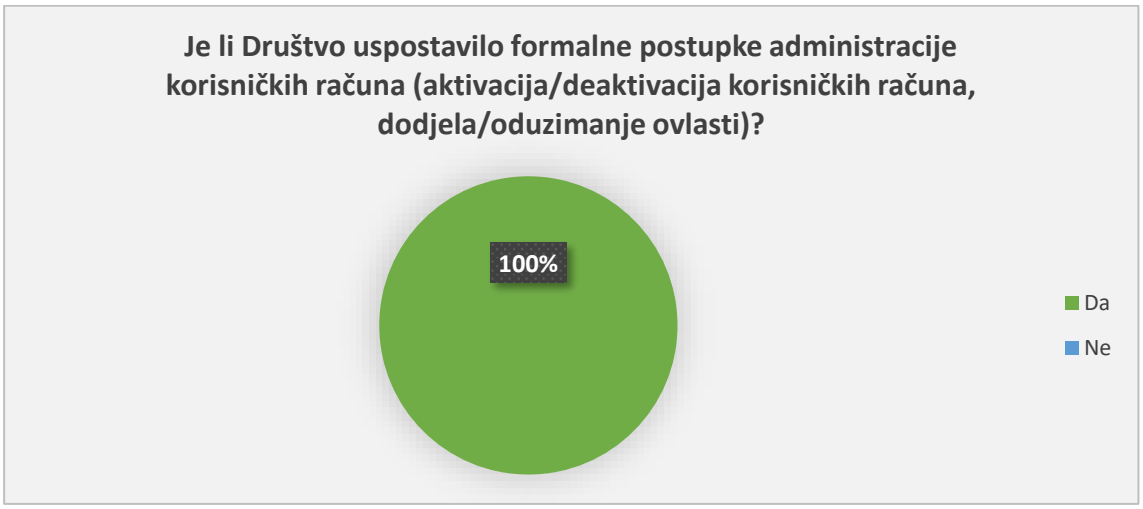
Grafikon 15. Opća politika informacijske sigurnosti



Izvor: samostalna obrada autorice

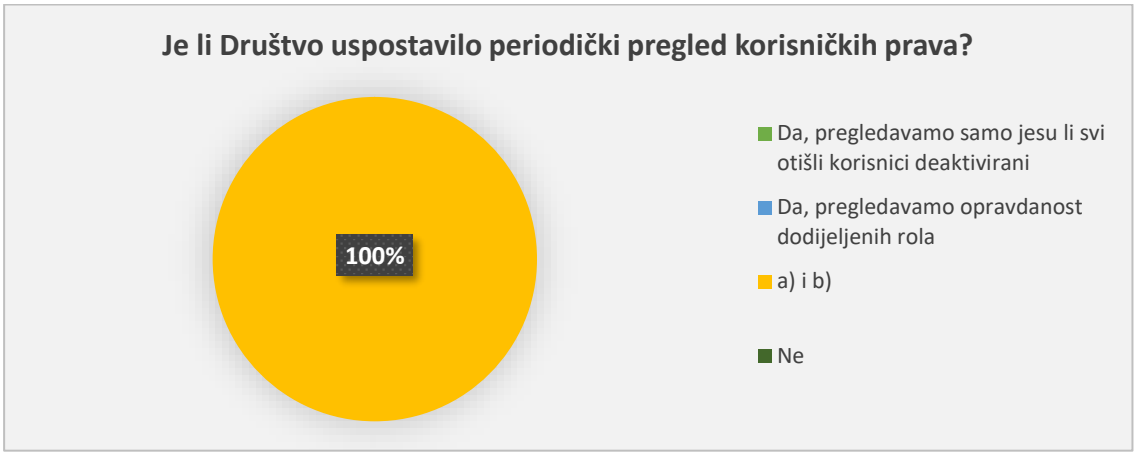
Također, sva anketirana revizorska društva imaju formalno uspostavljene postupke administracije korisničkih računa te periodički pregled korisničkih prava koji se provodi svakih šest mjeseci, a sastoji se od pregleda dodijeljenih rola trenutno aktivnim korisnicima i provjerom je li svim zaposlenicima, koji su napustili društvo, pravovremeno deaktiviran korisnički račun. Navedeno je prikazano na grafikonima 16, 17 i 18.

Grafikon 16. Postupak administracije korisničkih računa



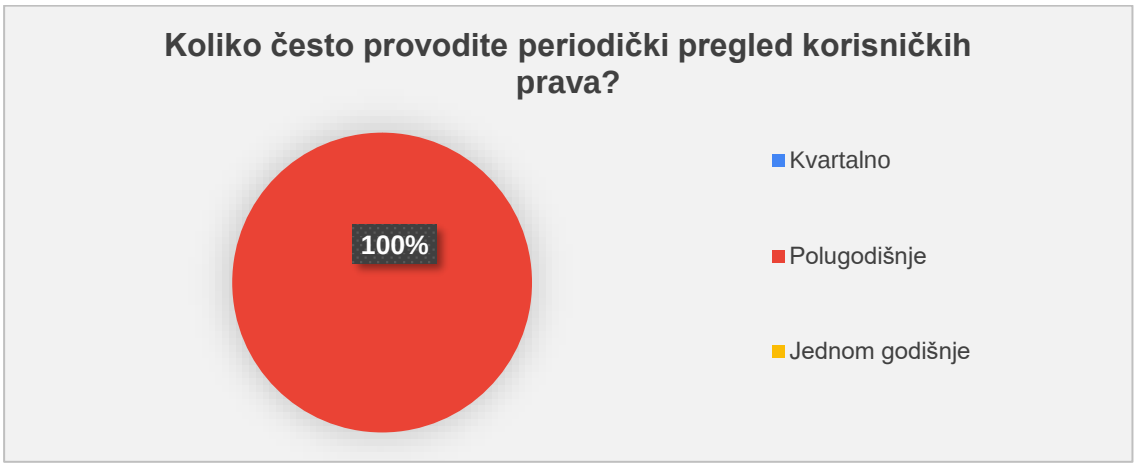
Izvor: samostalna obrada autorice

Grafikon 17. Način provođenja periodičkog pregleda korisničkih prava



Izvor: samostalna obrada autorice

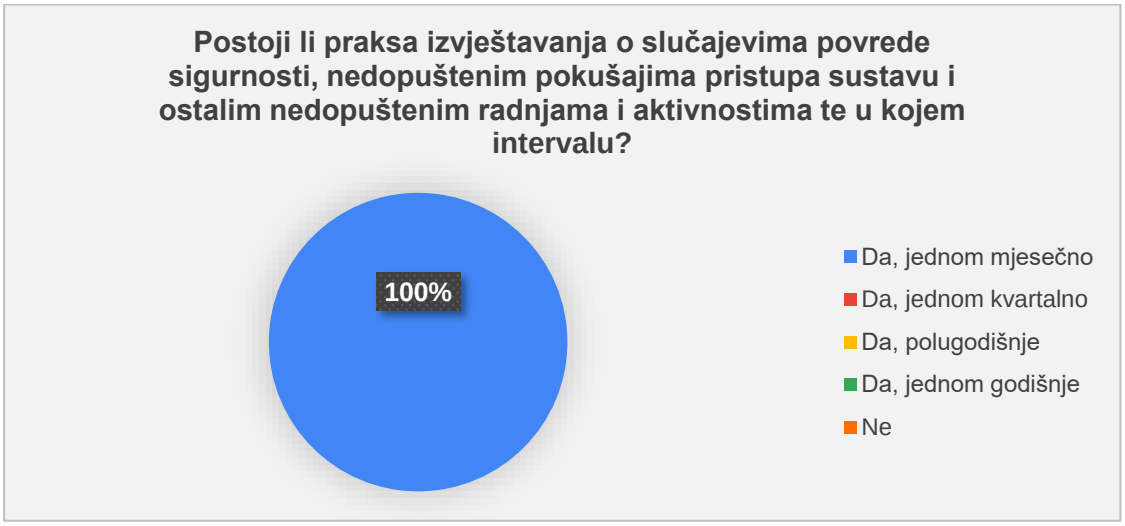
Grafikon 18. Učestalost provođenja periodičkog pregleda korisničkih prava



Izvor: samostalna obrada autorice

Revizorska Društva isto tako redovito izvještaju svoju Upravu o slučajevima povrede sigurnosti, nedopuštenim pokušajima pristupa sustavu i ostalim nedopuštenim radnjama i aktivnostima i to jednom mjesečno.

Grafikon 19. Izvještavanje o slučajevima povrede sigurnosti



Izvor: samostalna obrada autorice

Nadalje, imaju i usvojene planove kontinuiteta poslovanja i planove oporavka od katastrofe koji se redovito testiraju, tj. testiraju se minimalno jednom godišnje kako i nalažu dobre sigurnosne prakse.

Grafikon 20. Plan kontinuiteta poslovanja i plan oporavka od katastrofe

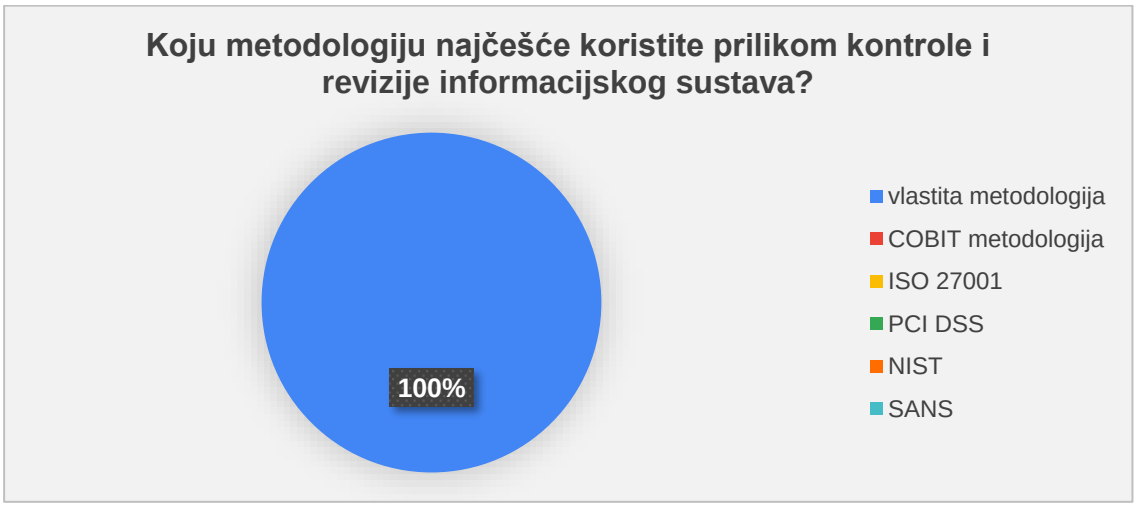
Izvor: samostalna obrada autorice

Grafikon 21. Testiranje plana kontinuiteta poslovanja i plana oporavka od katastrofe

Izvor: samostalna obrada autorice

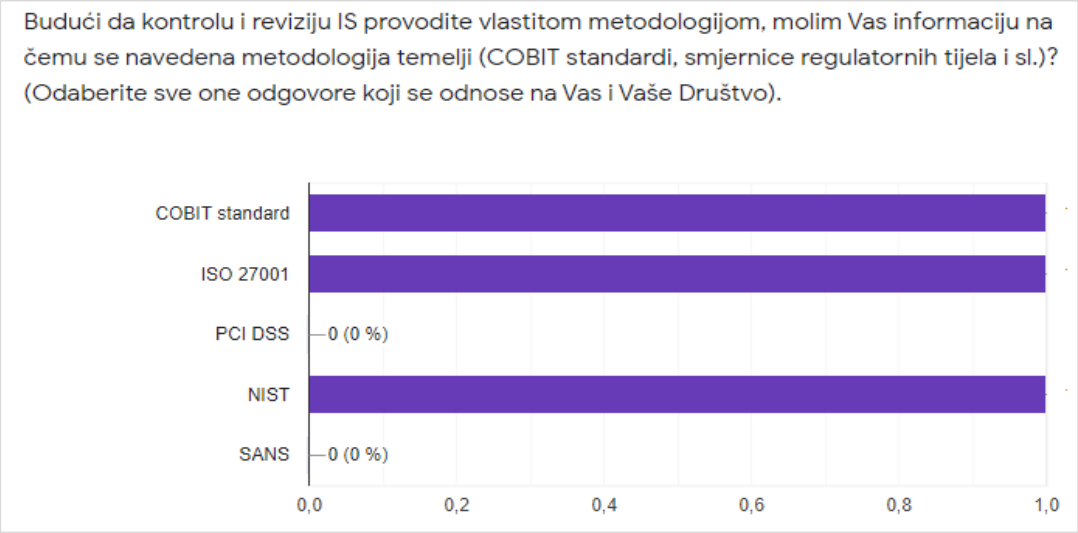
Istraživanje je pokazalo kako za reviziju informacijskih sustava interni revizori revizorskih društava najčešće koriste metodologiju koja je razvijena od same revizorske kuće, a koja se temelji na CobIT, ISO 27001 i NIST metodologiji.

Grafikon 22. Metodologija kontrole i revizije informacijskih sustava



Izvor: samostalna obrada autorice

Grafikon 23. Temelj vlastite metodologije



Izvor: samostalna obrada autorice

Ovakvi rezultati nisu uopće iznenađujući budući da je bilo očekivano da će društva kojima je primarna djelatnost pružanje usluga revizije biti i sama u skladu s dobrim svjetskim praksama. Također, vlastita metodologija se temelji na krovnom CobIT standardu te se pretpostavlja da preuzima dijelove sigurnosti informacijskih sustava koji su detaljnije razrađeni u ISO 27001 i NIST okviru.

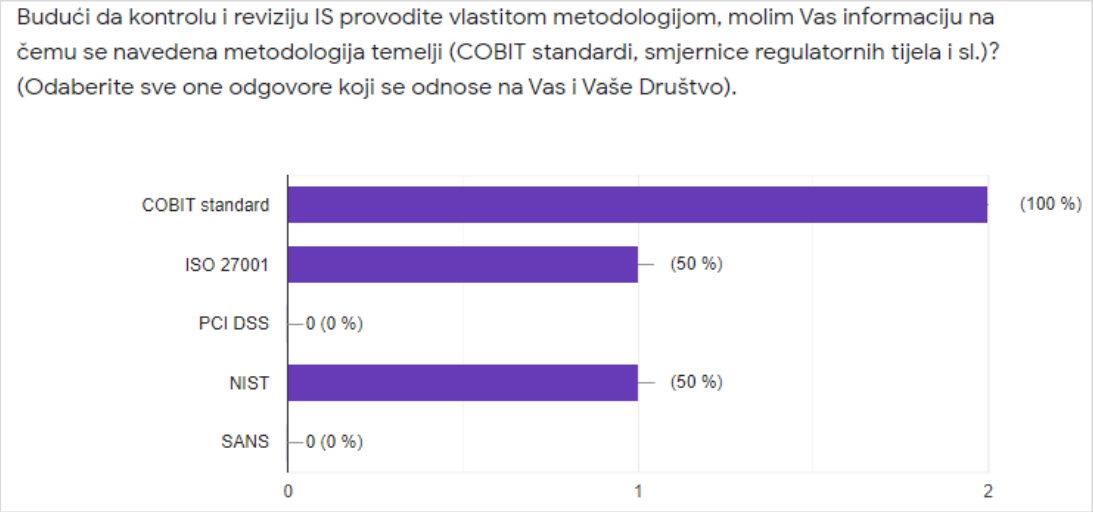
4.3.3.2. Rezultati istraživanja – revizorska društva – vanjski revizor

Istraživanje je pokazalo kako vanjski revizori, tj. konzultanti za sigurnost informacijskih sustava u 67% slučajeva koriste CobIT metodologiju za reviziju i kontrolu informacijskih sustava dok u 33% slučaja koriste vlastitu metodologiju razvijenu od strane revizorskog društva koja se uglavnom temelji na CobIT, ISO 27001 i NIST standardu Navedeno je vidljivo na grafikonima 24 i 25.

Grafikon 24. Vanjski revizori - metodologija revizije informacijskih sustava

Izvor: samostalna obrada autorice

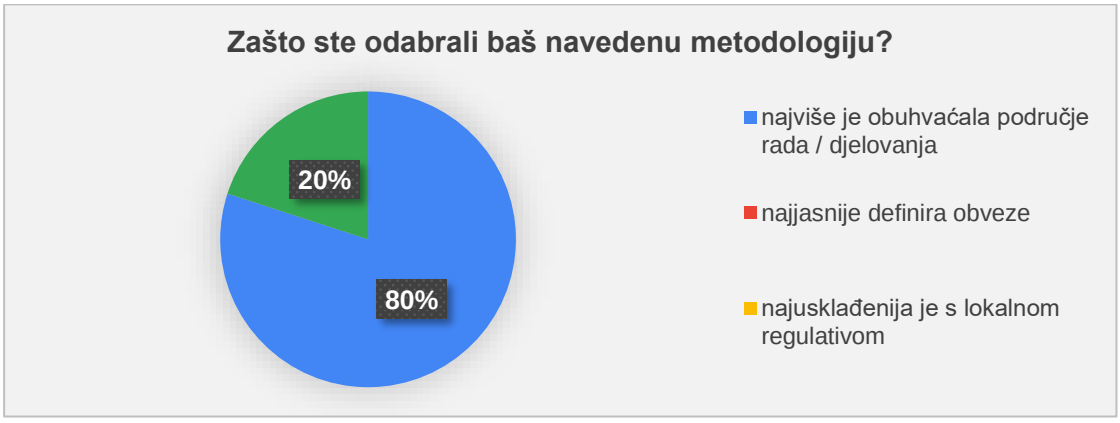
Grafikon 25. Temelj vlastite metodologije



Izvor: samostalna obrada autorice

Na pitanje koji je razlog korištenja odabranih metodologija, 80% anketiranih osoba je odgovorilo kako je ista najviše obuhvaćala područje rada / djelovanja, dok je 20% njih izjavilo kako imaju obvezu biti usklađeni s metodologijom matičnog Društva čak iako ista ne odgovara u potpunosti području rada / djelovanja.

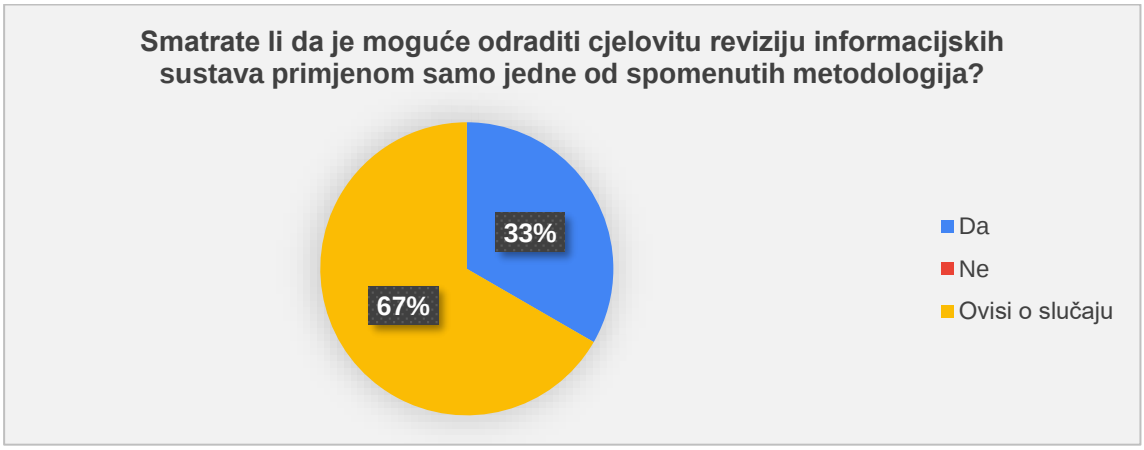
Grafikon 26. Razlog korištenja odabranih metodologija



Izvor: samostalna obrada autorice

Nadalje, 33% ispitanika je smatralo kako je moguće odraditi cjelovitu reviziju informacijskih sustava primjenom samo jedne od spomenutih metodologija dok je ostatak smatrao kako navedeno ovisi o samom klijentu i zahtjevima regulative. Sasvim je logično da cjelovita revizija u nekim slučajevima neće moći biti izvedena prateći samo jednu metodologiju, pa čak i ako je ta metodologija ona krovna, budući da su neke sfere detaljnije razrađene u ostalim metodologijama (primjerice u NIST okviru koji pruža detaljniju razradu kontrola za kibernetičku sigurnost).

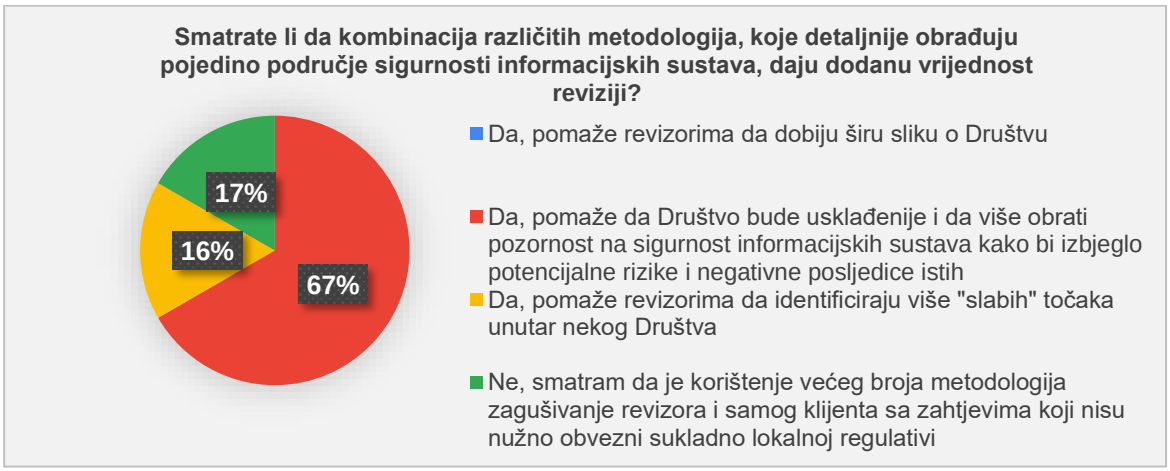
Grafikon 27. Odrađivanje cjelovite revizije primjenom samo jedne metodologije



Izvor: samostalna obrada autorice

Istraživanje je pokazalo kako čak 67% ispitanika smatra kako kombinacija različitih metodologija koje detaljnije obrađuju pojedino područje sigurnosti informacijskih sustava pomaže da revidirano Društvo bude usklađenije i više obrati pozornost na upravljanje sigurnošću informacijskih sustava kako bi izbjeglo potencijalne rizike i negativne posljedice istih. Njih 16% smatra kako navedeno pomaže revizorima da identificiraju više „slabih" točaka unutar nekog Društva, što je očekivano budući da su pojedine metodologije rađene na višoj razini koja ne daje detalje na koje bi revizori trebali obratiti pozornost. Međutim, 17% ispitanika smatra da ovakav pristup zapravo zagušuje revizore i samog klijenta sa zahtjevima koji nisu nužno obvezni sukladno lokalnoj regulativi. Ovakvi rezultati zapravo pokazuju da je potrebno, prilikom revizije, uzeti u obzir i veličinu Društva budući da pojedini zahtjevi metodologija ponekad nisu troškovno isplativi za implementaciju, pogotovo u nekim manjim organizacijama, budući da omjer razine rizika i uloženih sredstava nije proporcionalan.

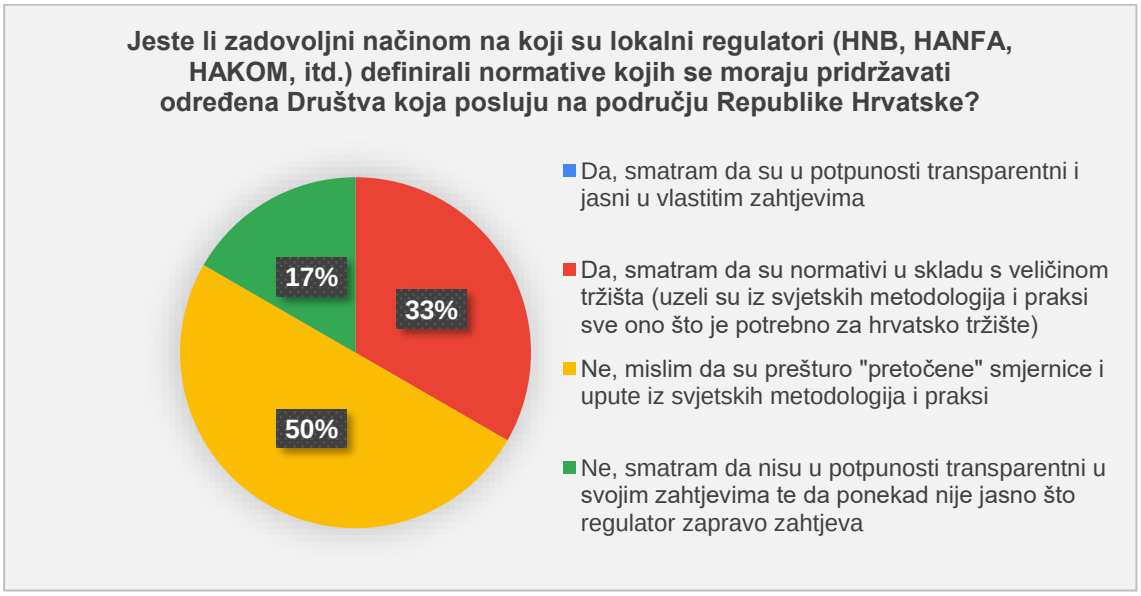
Grafikon 28. Dodana vrijednost reviziji kombinacijom različitih metodologija



Izvor: samostalna obrada autorice

Istraživanje pokazuje kako 50% ispitanika smatra kako su regulatori prešturo implementirali smjernice i upute iz svjetskih metodologija i praksi u domaće okvire, dok njih 33% smatra da su normativi u skladu s veličinom tržišta, tj. da su regulatori preuzeli iz svjetskih okvira sve ono što je bilo potrebno za lokalno tržište.

Grafikon 29. Zadovoljstvo normativima nadzornih tijela (regulatora)



Izvor: samostalna obrada autorice

Zanimljivo je vidjeti da na pitanje jesu li revizori zadovoljni način na koji su regulatori definirali normative kojih se moraju pridržavati određene organizacije koje posluju na području Republike Hrvatske, niti jedan ispitanik nije odgovorio da smatra kako su regulatori u potpunosti transparentni i jasni u vlastitim zahtjevima.

Grafikon 30. Provedbeni akti / upute uz regulativu

Izvor: samostalna obrada autorice

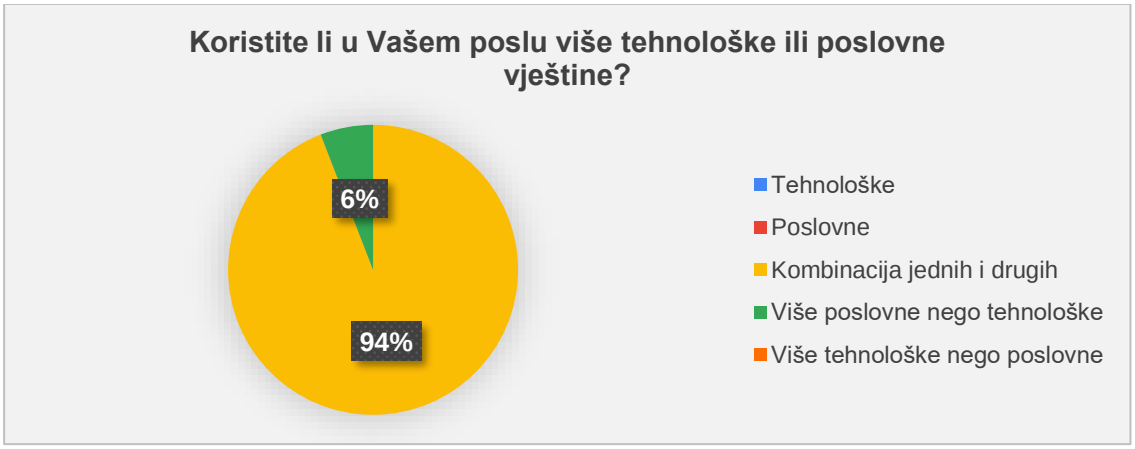
Ovakav rezultat je posljedica nedostataka nekakvih provedbenih akata i / ili uputa koji bi pojasnili propisane odredbe / smjernice te dali jasniju sliku o tome što regulator zapravo zahtjeva (osim u slučaju Uredbe o kibernetičkoj sigurnosti, kao što je opisanu u poglavlju 3.2.2. ovoga rada). Prethodnu tvrdnju potvrđuje i rezultat istraživanja gdje je 100% ispitanika odgovorilo kako bi provedbeni akti ili upute uz regulativu pomogli u provedbi revizije (vidljivo na grafikonu 30) te gdje 17% ispitanika smatra da lokalni regulatori nisu u potpunosti transparentni u svojim zahtjevima (vidljivo na grafikonu 29).

4.3.4. Rezultati istraživanja – mišljenje o važnosti tehnoloških i poslovnih vještina

Budući da revizije informacijskih sustava sadrži područja tehnološke prirode, svaki IT revizor bi trebao biti upoznat s osnovnim pojmovima informacijske tehnologije i s tehnološkom terminologijom kako bi lakše razumio i odradio reviziju.

Cilj ovog dijela istraživanja je bio prikazati koje vještine su zastupljenije u području upravljanja i revizije informacijskih sustava te dobiti uvid u mišljenje o važnosti tehnoloških i poslovnih vještina u obavljanju navedenog posla.

Grafikon 31. Korištenje vještina u obavljanju posla



Izvor: samostalna obrada autorice

Istraživanje je pokazalo da čak 94% svih ispitanika koristi kombinaciju poslovnih i tehnoloških vještina u obavljanju vlastitog posla. To se odnosi na ispitanike koji rade u kreditnim institucijama, osiguravajućim i telekomunikacijskim društvima na upravljanju informacijskim sustavom te na ispitanike koji rade kao revizori (interni / vanjski) informacijskih sustava.

U nastavku su prikazane tvrdnje vezane uz mišljenje o važnosti tehnoloških i poslovnih vještina prilikom upravljanja i revizije informacijskih sustava. U skladu s navedenim, u tablici 9 su prikazane ocjene slaganja, tj. neslaganja (u apsolutnim vrijednostima) s navedenim tvrdnjama i njihove aritmetičke sredine, pri čemu su aritmetičke vrijednosti podijeljene u subskale: od 1,00 do 2,50 – ne slažem se s tvrdnjom, od 2,51 – 3,50 -niti se slažem niti se ne slažem s tvrdnjom te od 3,51 do 5,00 – slažem se s tvrdnjom.

Tablica 10. Ljestvica mišljenja o važnosti tehnoloških i poslovnih vještina

Tvrdnja	**Ocjena (stupanj slaganja; 1 – uopće se ne slažem; 5 – u potpunosti se slažem**					**Aritmetička sredina**
	1	**2**	**3**	**4**	**5**	
Smatram da posjedovanje tehnoloških znanja pomaže da se posao odradi temeljito.	0	0	1	7	9	**4,47**
Smatram da posjedovanje poslovnih znanja pomaže da se posao odradi temeljitije.	0	0	1	10	6	**4,29**
Smatram da je posjedovanje tehnoloških znanja neophodan uvjet za rad u području revizije i kontrole informacijskih sustava.	0	3	6	6	2	**3,41**
Smatram da je posjedovanje poslovnih znanja neophodan uvjet za rad u području revizije i kontrole informacijskih sustava.	0	0	4	9	4	**4,0**
Smatram da je važnije steći tehnološka znanja, a da poslovne vještine dolaze naknadno.	0	2	10	5	0	**3,18**
Smatram da je balans između tehnoloških i poslovnih vještina važan uvjet za uspješno obavljanje revizije i kontrole informacijskih sustava.	0	0	0	2	15	**4,88**
Smatram da se tehnološka znanja mogu naučiti u bilo kojem periodu bez prethodnog tehnološkog usmjerenja u obrazovanju.	0	0	11	2	4	**3,59**

Izvor: samostalna obrada autorice

Najveće vrijednosti aritmetičkih sredina su imale tvrdnje *Smatram da je balans između tehnoloških i poslovnih vještina važan uvjet za uspješno obavljanje revizije i kontrole informacijskih sustava* s vrijednosti aritmetičke sredine 4,88, *Smatram da posjedovanje tehnoloških znanja pomaže da se posao odradi temeljito* s vrijednosti aritmetičke sredine 4,47, *Smatram da posjedovanje poslovnih znanja pomaže da se posao odradi temeljitije* s vrijednosti aritmetičke sredine 4,29, *Smatram da je posjedovanje poslovnih znanja neophodan uvjet za rad u području revizije i kontrole informacijskih sustava* s vrijednosti aritmetičke sredine 4,00, *Smatram da se tehnološka znanja mogu naučiti u bilo kojem periodu bez prethodnog tehnološkog usmjerenja u obrazovanju* s vrijednosti aritmetičke sredine 3,59.

Tvrdnje sa srednjim aritmetičkim sredinama su bile *Smatram da je posjedovanje tehnoloških znanja neophodan uvjet za rad u području revizije i kontrole informacijskih sustava* s aritmetičkom sredinom 3,41, *Smatram da je važnije steći tehnološka znanja, a da poslovne vještine dolaze naknadno* s aritmetičkom sredinom 3,18.

Ispitanici su pokazali da je kombinacija poslovnih i tehnoloških vještina važan uvjet za obavljanje kontrole i revizije informacijskih sustava te da je posjedovanje poslovnih znanja neophodan uvjet za rad u navedenom području budući da takav posao iziskuje neprestanu komunikaciju s klijentima koji su nekada više tehnološki usmjereni, a nekada poslovno usmjereni te je važno poznavati oba područja i posjedovati tzv. meke vještine (*eng. soft skills).* Također, ispitanici smatraju kako se tehnološke vještine, koje su potrebne za rad u području revizije i kontrole informacijskih sustava, mogu naučiti u bilo kojem trenutku bez prethodnog tehnološkog obrazovanja što je vrlo ohrabrujuće budući da ljudi nerijetko imaju dojam kako reviziju i kontrolu informacijskih sustava rade osobe isključivo tehnološkog usmjerenja.

Također, ispitanici su pokazali da su neutralniji stav prema mišljenju da su tehnološke vještine neophodne za rad u području revizije i kontrole informacijskih sustava te da je važnije steći tehnološka znanja nego poslovne vještine.

Nadalje, vidljivo je kako nije bilo najnižih aritmetičkih sredina, tj. nije bilo strogog neslaganja niti sa jednom od postavljenih tvrdnji.

4.3.5. Ograničenja istraživanja i preporuke za buduću praksu

Rezultati istraživanja pokazuju znatnije poboljšanje o svijesti upravljanja informacijskim sustavima od istraživanja koje je proveo Spremić, M. 2007. godine, što je i očekivano budući da se od tada svijest o sigurnosti informacijskih sustava podigla na višu razinu.

Svakako, ovakvo istraživanje je imalo nekoliko ograničenja. Prvo je bila uska populacija, tj. anketa je poslana samo na one osobe koje su radile u točno određenom sektoru. Proširenjem populacije i sektora mogli bi se dobiti rezultati za cjelokupno hrvatsko tržište te bi se mogao dobiti uvid o korištenim metodologijama i stanju svijesti u svim većim hrvatskim organizacijama.

Nadalje, anketa nije imala veliki broj pitanja te bi se povećanjem broja pitanja mogao dobiti detaljniji uvid u praksu upravljanja i revizije informacijskih sustava. Također, osjetljivost područja istraživanja je bilo jedno od vodećih ograničenja. Kao što je već navedeno, istraživanja u ovom području su rijetka te većina osoba nije voljna iznositi u javnost informacije o svojim organizacijama, pogotovo ako takve informacije nisu uvijek zadovoljavajuće. Posljednje ograničenje je bio vremenski okvir provođenja ankete koji je bio kraći radi mogućnosti predaje i obrane diplomskog rada. Povećanjem vremenskog okvira postoji mogućnost da bi se prikupio veći broj odgovora.

5. ZAKLJUČAK

Budući da danas gotovo i ne postoji organizacija koja se ne koristi nekim vidom informacijske tehnologije kojom se ostvaruju mnogobrojne poslovne koristi logičan je zaključak da se takve organizacije istodobno izlažu i novim prijetnjama, neželjenim posljedicama i brojnim novim rizicima.

Kako bi se osigurala kvaliteta informacijskog sustava kroz koji organizacije ostvaruju svoje uspješno poslovanje te kako bi se identificirali svi oni potencijalni rizici i prijetnje koje organizacija nije odmah uočila, danas se sve veći naglasak stavlja na reviziju informacijskih sustava.

Revizija informacijskih sustava je proces provjere uspješnosti informacijskih sustava obzirom na to što poslovanje od njih očekuje odnosno obzirom na mogućnosti koje njihova promjena u poslovanju pruža. Područje revizije informacijskih sustava je uređeno brojnim metodologijama, okvirima i standardima među kojima se ističe CobIT kao krovni standard, a slijede ga ISO 27001, PCI DSS, NIST, SANS i ITIL.

Cilj istraživanja je bio dobiti uvid koju metodologiju (ili kombinaciju metodologija) stručnjaci preferiraju u praksi te koja od navedenih metodologija (ili kombinacija metodologija) najviše pokriva područje sigurnosti informacijskog sustava. Također, htio se dobiti i uvid u to kakvo obrazovanje su ispitanici stekli (tehničko ili ekonomsko) te dobiti uvid koje od tih vještina su prihvatljivije u području revizije i upravljanja informacijskim sustavima.

Istraživanje je pokazalo kako većina ispitanih kreditnih institucija, osiguravajućih i telekomunikacijskih društava, najčešće koristi ISO27001 metodologiju za kontrolu i reviziju informacijskih sustava dok manji dio koristi krovnu, CobIT metodologiju.

Nadalje, istraživanje je pokazalo kako većina revizorskih društava kao metodologiju koriste CobIT, ISO 27001 i NIST okvir koji uređuje područje kibernetičke sigurnosti. Ovakvi rezultati nisu iznenađujući budući da unutar CobIT i ISO 27001 okvira nisu detaljnije definirana područja kibernetičke sigurnosti.

Do važnijih zaključaka se došlo ispitivanjem mišljenja o važnosti tehnoloških i poslovnih vještina za područje kontrole i revizije informacijskog sustava ispitanici su pokazali kako većina njih koristi kombinaciju poslovnih i tehnoloških vještina u obavljanju svog posla te su pokazali da je kombinacija poslovnih i tehnoloških vještina važan uvjet za obavljanje kontrole

i revizije informacijskih sustava. Ovakvi rezultati su vrlo ohrabrujući budući da ukazuju na to kako za obavljanje posla upravljanja i revizije informacijskog sustava nije nužno tehnološko predznanje, ali je svakako poželjno posjedovati neke osnove radi lakše komunikacije s osobama koje operativno odrađuju poslove upravljanja informacijskim sustavom (sistem integratori, mrežni administratori i slično). Također, rezultati su pokazali da je posjedovanje poslovnih znanja neophodan uvjet za rad u navedenom području.

Navedeni rezultati su i očekivani budući da takav posao iziskuje neprestanu komunikaciju s klijentima koji su nekada više tehnološki usmjereni, a nekada poslovno usmjereni te je važno poznavati oba područja i posjedovati tzv. meke vještine koje će olakšati komunikaciju i provedbu same revizije i kontrole informacijskih sustava.

6. POPIS LITERATURE

1. Bosilj Vukšić, V. et al. (2020.) Osnove poslovne informatike, Zagreb, Ekonomski fakultet
2. BS EN ISO/IEC 27001:2017 – what has changed?, dostupno na: https://www.bsigroup.com/en-GB/iso-27001-information-security/BS-EN-ISO-IEC-27001-2017/, [09. lipnja 2021.]
3. Business Process Framework – eTOM, R17.0.0, dostupno na: https://www.tmforum.org/resources/suite/gb921-business-process-framework-etom-r17-0-1/, [18. lipnja 2021.]
4. EIOPA finalises Guidelines on Information and Communication Technology Security and Governance, dostupno na: https://www.eiopa.europa.eu/content/eiopa-finalises-guidelines-information-and-communication-technology-security-and-governance_en, [18. lipnja 2021.]
5. „Hakerski napad na INU pokrenut je iz Mađarske i zaključao je podatke o poslovanju potrebne Lazardu“ (2020., online), dostupno na: https://www.nacional.hr/hakerski-napad-na-inu-pokrenut-je-iz-madarske-i-zakljucao-je-podatke-o-poslovanju-potrebne-lazardu/, [7. svibnja 2021.]
6. HANFA osiguranje, dostupno na: https://www.hanfa.hr/getfile.ashx/?fileId=42496, [18. lipnja 2021.]
7. ISACA (2019) COBIT 2019 Framework: Governance and Management Objectives
8. ISACA (online), dostupno na: https://www.isaca.org/why-isaca/about-us/history, [08. lipnja 2021.]
9. ISO (2018.) ISO/IEC 27000:2018
10. ISO/IEC 27001 International Information Security Standard published, dostupno na: https://www.bsigroup.com/en-GB/about-bsi/media-centre/press-releases/2005/11/ISOIEC-27001-International-Information-Security-Standard-published/, [09. lipnja 2021.]
11. ISO/IEC 27001:2013, dostupno na: https://www.iso.org/standard/54534.html, [09. lipnja 2021.]
12. IT Governance Institute (2012): CobiT 5 – Framework, Control Objectives, Management Guidlines and Maturity Models, IT Governance Institute, Rolling Meadows, Illionis, SAD,
13. „New version of iso/iecISO/IEC 27001 to better tackle it security risks“, dostupno na: https://www.iso.org/news/2013/08/Ref1767.html, [09.lipnja 2021.]
14. NIST, Framework for Improving Critical Infrastructure Cybersecurity, version 1.1., April 2018.
15. Odluka o primjerenom upravljanju informacijskim sustavom, dostupno na: https://narodne-novine.nn.hr/clanci/sluzbeni/2010_03_37_958.html, [18. lipnja 2021.]
16. Okvir dobrih praksi za usklađivanje operatora ključnih usluga s mjerama Zakona o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga i provođenje ocjene sukladnosti, dostupno na: https://www.zsis.hr/UserDocsImages/Okvir_dobrih_praksi-v1.pdf, [18.lipnja 2021.]
17. PCI DSS – Requirements and Security Assessment Procedures, version 3.2.1., PCI Security Standard Council, LLC, 2006-2018.

18. Priopćenje o rezultatima preispitivanja sistemske važnosti kreditnih institucija u Republici Hrvatskoj, dostupno na: https://www.hnb.hr/documents/20182/2293886/h-priopcenje-preispitivanje-sistemski-vaznih-ki-u-RH_10-12-2020.pdf/283d1d22-0145-b6a4-fec3-577293ac5646?t=1607595350135, [18. lipnja 2021.]
19. Sistemski važne institucije, dostupno na: https://www.hnb.hr/temeljne-funkcije/financijska-stabilnost/makrobonitetne-mjere/sistemski-vazne-institucije, [18. lipnja 2021.]
20. Smjernice za primjereno upravljanje rizicima informacijskih sustava subjekata nadzora, dostupno na: https://www.hanfa.hr/getfile/41744/7-Smjernice%20za%20primjereno%20upravljanje%20rizicima%20IS%20subjekata%20nadzora%20Agencije.pdf, [18. lipnja 2021.]
21. Smjernice za upravljanje informacijskim sustavom u cilju smanjenja operativnog rizika, dostupno na: https://www.hnb.hr/documents/20182/639854/h-smjernice-za-upravljanje-informacijskim-sustavom.pdf/e5579931-e846-47ab-af23-6809debef700, [18. lipnja 2021.]
22. Spremić, M. (2017.) Digitalna transformacija poslovanja, Zagreb, Ekonomski fakultet
23. Spremić, M. (2005): Revizija informacijskih sustava pomoću CobiT metodologije. Časopis Hrvatske zajednice računovođa i financijskih djelatnika, 51 (2005), 11 , str. 107-112.
24. Spremić, M. (2007.) Metode provedbe revizije informacijskih sustava, Zbornik Ekonomskog fakulteta Zagreb, str. 295. – 311.
25. Spremić, M. (2008): Krovni standardi upravljanja poslovnim informacijskim sustavima, Časopis Hrvatske zajednice računovođa i financijskih djelatnika, 54 (2008), 10, str. 148-154.
26. Spremić, M. (2017) Sigurnost i revizija informacijskih sustava u okruženju digitalne ekonomije, Zagreb, Ekonomski fakultet, str. 195
27. Spremić, M., Kostić, D. (2008.), Upravljanje kvalitetom informatičke usluge: Studije slučaja primjene ITIL metode, Business Excellence; Zagreb Vol. 2, Iss. 1, 2008., str. 42
28. Uredba EU br. 575/2013, dostupno na: https://eur-lex.europa.eu/legal-content/HR/TXT/?uri=celex%3A32013R0575, [18. lipnja 2021.]
29. Uredba o kibernetičkoj sigurnosti, dostupno na: https://narodne-novine.nn.hr/clanci/sluzbeni/full/2018_07_68_1399.html, [18. lipnja 2021.]
30. Varga, M. (1994.) Baze podataka: konceptualno, logičko i fizičko modeliranje podataka, Zagreb, Društvo za razvoj informacijske pismenosti (DRIP)
31. Varga, M. et al. (2016.) Informacijski sustavi u poslovanju, Zagreb, Ekonomski fakultet
32. Varga, M. et al. (2012.) Upravljanje podacima, Zagreb, Element
33. Varga, M., Varga, V. (2011.) Usporedba rezultata revizije informacijskih sustava provedenih prema CobiT okviru i uvod u CobiT 5 okvir. Tehnički glasnik, 5 (2011.), str. 35 – 43
34. What is ITIL? Your guide to the IT Infrastructure Library", dostupno na: https://www.cio.com/article/2439501/infrastructure-it-infrastructure-library-itil-definition-and-solutions.html, [15. lipnja 2021.]
35. Zakon o kreditnim institucijama, dostupno na: https://www.zakon.hr/z/195/Zakon-o-kreditnim-institucijama, [18. lipnja 2021.]

7. POPIS SLIKA

8. POPIS GRAFIKONA

9. POPIS TABLICA

10. PRILOZI

ANKETNI UPITNIK

Istraživanje provođenja revizije informacijskih sustava primjenom različitih metodologija

Poštovani,

Ovo istraživanje provodi se u svrhu izrade diplomskog rada na temu "Provedba revizije informacijskih sustava primjenom različitih metodologija".

Cilj istraživanja je dobiti uvid koju metodologiju (ili kombinaciju metodologija) stručnjaci preferiraju u praksi te koja od navedenih metodologija (ili kombinacija metodologija) najviše pokriva područje sigurnosti informacijskog sustava.

Popunjavanje anketnog upitnika je u potpunosti anonimo te je za popunjavanje istog potrebno nekoliko minuta, stoga Vas molim da na pitanja odgovorite iskreno i u cijelosti.

Ukoliko Vas zanimaju rezultati istraživanja slobodno me kontaktirajte na mvisnjic1@net.efzg.hr.

Hvala unaprijed na uloženom vremenu!

PITANJA:

1. Koje je Vaše formalno obrazovanje?
    a. Ekonomsko – smjer Menadžerska informatika
    b. Ekonomsko – ostali smjerovi
    c. Inženjersko
    d. Elektrotehničko
    e. Ostalo:_____

2. U kojoj veličini poduzeća radite?
    a. malo poduzeće
    b. srednje poduzeće
    c. veliko poduzeće

3. Koja je industrija u kojoj ste zaposleni?
    a. Kreditne instituacije
    b. Osiguravajuća društva
    c. Telekomunikacijska industrija
    d. Revizorska / konzultantska društva
    e. Ostalo:_____

KREDITNE INSTITUCIJE, OSIGURANJA, TELEKOMUNIKACIJE i OSTALO

4. Koja je Vaša funkcija koju obnašate unutar poduzeća?
    a. interni revizor informacijskih sustava
    b. stručnjak za sigurnost informacijskog sustava (CISO, ISO i sl.)
    c. IT menadžer (CIO)
    d. Ostalo:_____

5. Na koji način se provodi revizija informacijskog sustava kao organizacijska funkcija?
    a. posebna organizacijska jedinica pod nadzorom najvišeg menadžmenta (pr. odjel interne revizije)
    b. organizacijska jedinica u sklopu odjela informatike
    c. eksternalizirana usluga

6. Postoji li formalno usvojena opća sigurnosna politika informacijskog sustava?
    a. Da
    b. Ne
    c. U pripremi je

7. Koju metodologiju koristite prilikom kontrole i revizije informacijskog sustava?
    a. vlastita metodologija
    b. COBIT metodologija
    c. ISO 27001
    d. PCI DSS
    e. NIST
    f. SANS
    g. ostalo (metodologija vanjske revizorske kuće)

Ukoliko je odgovor na pitanje 4. a):

7a. Budući da kontrolu i reviziju IS provodite vlastitom metodologijom, molim Vas informaciju na čemu se navedena metodologija temelji (COBIT standardi, smjernice regulatornih tijela i sl.)? (više mogućih odgovora)

a. COBIT metodologija
b. ISO 27001
c. PCI DSS
d. NIST
e. SANS
f. Ostalo(metodologija vanjske revizorske kuće)

Nakon 7a se nastavlja sljedeće (ili se prebacuje se sljedeće ako je u pitanju 4 odabran bilo koji drugi odgovor osim a))

8. Postoji li praksa izvještavanja o slučajevima povrede sigurnosti, nedopuštenim pokušajima pristupa sustavu i ostalim nedopuštenim radnjama i aktivnostima te u kojem intervalu?
    a. Da, jednom mjesečno
    b. Da, jednom kvartalno
    c. Da, polugodišnje
    d. Da, jednom godišnje
    e. Ne

9. Kome šaljete takve izvještaje?
    a. Upravi
    b. Nadležnom regulatornom tijelu
    c. Upravi i nadležnom regulatornom tijelu
    d. Ništa od navedenog

10. Je li Društvo uspostavilo formalne postupke administracije korisničkih računa (aktivacija/deaktivacija korisničkih računa, dodjela/oduzimanje ovlasti)'
    a. Da
    b. Ne

11. Je li Društvo uspostavilo periodički pregled korisničkih prava?
    a. Da, pregledavamo samo jesu li svi otišli korisnici deaktivirani
    b. Da, pregledavamo opravdanost dodijeljenih rola
    c. a) i b)

d. Ne, ne smatramo navedeno važnim.

12. Koliko često provodite periodički pregled korisničkih prava
    a. Kvartalno
    b. Polugodišnje
    c. Jednom godišnje
    d. Jednom u 2 godine
    e. Vremenski period između dva pregleda korisničkih prava je veći od 2 godine

13. Je li Društvo formalno usvojilo Plan kontinuiteta poslovanja (Business Continuity Plan) i Plan oporavka od katastrofe (Disaster Recovery Plan)?
    a. Da
    b. Ne
    c. U pripremi

14. Testirali Društvo periodički plan kontinuiteta poslovanja i plan oporavka od katastrofe
    a. Da, barem jednom godišnje
    b. Da, barem jednom u 2 godine
    c. Ne

REVIZORSKA KUĆA

Ako je odgovor na 3. pitanje d) onda:

4. Koja je Vaša funkcija koju obnašate unutar poduzeća?
    a. interni revizor informacijskih sustava
    b. vanjski revizor/konzultant za sigurnost informacijskih sustava
    c. ostalo: _____

INTERNI REVIZOR U REVIZORSKOJ KUĆI / OSTALO

Ako je odgovor na gornje (4) pitanje a):

5. Postoji li formalno usvojena opća sigurnosna politika informacijskog sustava?
    a. Da
    b. Ne
    c. U pripremi je

6. Koju metodologiju koristite prilikom kontrole i revizije informacijskog sustava?
    a. vlastita metodologija

b. COBIT metodologija
c. ISO 27001
d. PCI DSS
e. NIST
f. SANS

Ukoliko je odgovor na 6. pitanje a):

6a. Budući da kontrolu i reviziju IS provodite vlastitom metodologijom, molim Vas informaciju na čemu se navedena metodologija temelji (COBIT standardi, smjernice regulatornih tijela i sl.)? (više mogućih odgovora)

a. COBIT metodologija
b. ISO 27001
c. PCI DSS
d. NIST
e. SANS
f. ostalo: _____

Nakon 6a se nastavlja sljedeće (ili se prebacuje se sljedeće ako je u pitanju 6 odabran bilo koji drugi odgovor osim a))

7. Postoji li praksa izvještavanja o slučajevima povrede sigurnosti, nedopuštenim pokušajima pristupa sustavu i ostalim nedopuštenim radnjama i aktivnostima te u kojem intervalu?
    a. Da, jednom mjesečno
    b. Da, jednom kvartalno
    c. Da, polugodišnje
    d. Da, jednom godišnje
    e. Ne

8. Je li Društvo uspostavilo formalne postupke administracije korisničkih računa (aktivacija/deaktivacija korisničkih računa, dodjela/oduzimanje ovlasti)'
    a. Da
    b. Ne

9. Je li Društvo uspostavilo periodički pregled korisničkih prava?
    a. Da, pregledavamo samo jesu li svi otišli korisnici deaktivirani
    b. Da, pregledavamo opravdanost dodijeljenih rola

c. a) i b)
d. Ne, ne smatramo navedeno važnim.

10. Koliko često provodite periodički pregled korisničkih prava
    a. Kvartalno
    b. Polugodišnje
    c. Jednom godišnje
    d. Jednom u 2 godine

11. Je li Društvo formalno usvojilo Plan kontinuiteta poslovanja (Business Continuity Plan) i Plan oporavka od katastrofe (Disaster Recovery Plan)?
    a. Da
    b. Ne
    c. U pripremi

12. Testira li Društvo periodički plan kontinuiteta poslovanja i plan oporavka od katastrofe
    a. Da, barem jednom godišnje
    b. Da, barem jednom u 2 godine
    c. Ne

VANJSKI REVIZOR U REVIZORSKOJ KUĆI

Ako je odgovor na gornje (4.) pitanje b):

5. Koju metodologiju koristite prilikom kontrole i revizije informacijskog sustava kod svojih klijenata?
    a. vlastita metodologija
    b. COBIT metodologija
    c. ISO 27001
    d. PCI DSS
    e. NIST
    f. SANS

Ukoliko je odgovor na 5.pitanje a):

5a. Budući da kontrolu i reviziju IS provodite vlastitom metodologijom, molim Vas informaciju na čemu se navedena metodologija temelji (COBIT standardi, smjernice regulatornih tijela i sl.)? (više mogućih odgovora)

a. COBIT metodologija
b. ISO 27001
c. PCI DSS
d. NIST
e. SANS
f. ostalo: _____

Nakon toga se nastavljaju pitanja (ili se prebacuje odmah na 5. pitanje ukoliko odgovor nije a)):

6. Zašto ste odabrali baš navedenu / e metodologiju / e?
   a. najviše je obuhvaćala područje rada / djelovanja
   b. najjasnije definira obveze
   c. najusklađenija je s lokalnom regulativom
   d. imamo obvezu biti usklađeni s metodologijom matičnog Društva
   e. Drugo: _____

7. Smatrate li da je moguće odraditi cjelovitu reviziju informacijskih sustava primjenom samo jedne od spomenutih metodologija?
   a. Da
   b. Ne
   c. Ovisi o slučaju

8. Smatrate li da kombinacija različitih metodologija, koje detaljnije obrađuju pojedino područje sigurnosti informacijskih sustava, daju dodanu vrijednost reviziji informacijskih sustava?
   a. Da, pomaže revizorima da dobiju širu sliku o Društvu
   b. Da, pomaže revizorima da identificiraju više "slabih" točaka unutar nekog Društva
   c. Da, pomaže da Društvo bude usklađenije i da više obrati pozornost na sigurnost informacijskih sustava kako bi izbjeglo potencijalne rizike i negativne posljedice istih
   d. Ne, smatram da je korištenje većeg broja metodologija zagušivanje revizora i samog klijenta sa zahtjevima koji nisu nužno obvezni sukladno lokalnoj regulativi

9. Jeste li zadovoljni načinom na koji su lokalni regulatori (HNB, HANFA, HAKOM, itd.) definirali normative kojih se moraju pridržavati određena Društva koja posluju na području Republike Hrvatske?
   a. Da, smatram da su normativi u skladu s veličinom tržišta (uzeli su iz svjetskih metodologija i praksi sve ono što je potrebno za hrvatsko tržište)

b. Da, smatram da su u potpunosti transparentni i jasni u vlastitim zahtjevima
c. Ne, mislim da su prešturo "pretočene" smjernice i upute iz svjetskih metodologija i praksi
d. Ne, smatram da nisu u potpunosti transparentni u svojim zahtjevima te da ponekad nije jasno što regulator zapravo zahtjeva

10. Smatrate li da bi provedbeni akti ili upute uz regulative pomogli u provedbi revizije?
    a. Da
    b. Ne

DRUGI DIO ANKETE

Koristite li u Vašem poslu više tehnološke ili poslovne vještine?

a. Tehnološke

b. Poslovne

c. Kombinacija jednih i drugih

d. Više poslovne nego tehnološke

e. Više tehnološke nego poslovne

U ovom dijelu anketnog upitnika nalaze se tvrdnje koje ćete ocjenjivati brojevima od 1 do

5, ovisno o razini slaganja s tvrdnjom.

Ispred Vas se nalaze određene tvrdnje vezane uz tehnološke i poslovne vještine koje su označene brojevimaod 1 do 5. S obzirom na slaganje s određenim tvrdnjama molim Vas da zaokružite broj (1 – uopće sene slažem s tvrdnjom; 2 – ne slažem se; 3 – niti se slažem, niti se ne slažem; 4 – slažem se; 5 – upotpunosti se slažem s navedenom tvrdnjom).

a) Smatram da posjedovanje tehnoloških znanja pomaže da se posao odradi temeljito.
b) Smatram da posjedovanje poslovnih znanja pomaže da se posao odradi temeljitije.
c) Smatram da je posjedovanje tehnoloških znanja neophodan uvjet za rad u području revizije i kontrole informacijskih sustava.
d) Smatram da je posjedovanje poslovnih znanja neophodan uvjet za rad u području revizije i kontrole informacijskih sustava.
e) Smatram da je važnije steći tehnološka znanja, a da poslovne vještine dolaze naknadno.

f) Smatram da je balans između tehnoloških i poslovnih vještina važan uvjet za uspješno obavljanje revizije i kontrole informacijskih sustava.
g) Smatram da se tehnološka znanja mogu naučiti u bilo kojem periodu bez prethodnog tehnološkog usmjerenja u obrazovanju .

11. ŽIVOTOPIS

Ime i prezime: Marija Višnjić

Datum rođenja: 28.12.1994.

E-mail: m.visnjic77@gmail.com

RADNO ISKUSTVO:

- **PRIPRAVNIK U IT REVIZIJI –** studeni 2019. – trenutno, PricewaterhouseCoopers Hrvatska
    - Provođenje revizije informacijskih sustava i testiranje ITGC-a (Information Technology General Controls)
    - Pružanje konzultantskih usluga vezanih za:
        - Regulatornu usklađenost (usklađenost sa smjernicama HNB-a i HANFA-e)
        - Usklađenost sa standardima / metodologijama (CobIT, ISO27001, ISAE 3000, IFRS15 i slično)
- **ASISTENT U MARKETINGU –** siječanj 2019. – studeni 2019., Robert Bosch d.o.o.
    - unos i ažuriranje CRM-a, administrativni poslovi
    - upravljanje odnosa sa klijentima
    - organizacija događaja i službenih putovanja
    - oglašavanje na društvenim mrežama, izrada
    - newslettera i cover lettera, PR članci za časopise
- **AGENT U SLUŽBI ZA KORISNIKE –** listopad 2015. – siječanj 2019., Blitz-Cinestar d.o.o.
    - telefonski, Faceboook i e-mail upiti korisnika
    - rezervacija ulaznica telefonskim putem
    - organizacija rođendana i školskih projekcija
    - administracija
    - arhiviranje poslovne dokumentacije
- **RADNIK U TRGOVINI –** listopad 2014. – listopad 2015., Pittarosso, Zagreb
    - slaganje robe i inventure
    - ljepljenje deklaracija

- rad na POS blagajni

OBRAZOVANJE

- listopad 2015. – trenutno → Ekonomski fakultet Sveučilišta u Zagrebu, Integrirani preddiplomski i diplomski studij Poslovne ekonomije, smjer Menadžerska informatika. Trg J.F. Kennedya 6, Zagreb
- 2009. – 2013. → XVI. Gimnazija, Križanićeva 4a, Zagreb

VJEŠTINE

- Windows i Linux OS
- MS Office i LibreOffice
- Alteryx
- SAP CRM
- ACL Analytics
- MS SQL
- Visual Studio 2019
- C#
- Vozačka dozvola – B kategorija

JEZICI

- Engleski jezik: Govor C1 – Razumijevanje C1 – Pisanje C1
- Španjolski jezik: Govor B2 – Razumijevanje B2 – Pisanje B2