SLOVENSKI INŠTITUT ZA REVIZIJO
LJUBLJANA

ZAKLJUČNO DELO
ZA PRIDOBITEV STROKOVNEGA NAZIVA
PREIZKUŠENEGA REVIZORJA INFORMACIJSKIH SISTEMOV

PREGLED DODELJEVANJA, ODVZEMANJA IN SPREMINJANJA UPORABNIŠKIH DOSTOPOV V SAP SISTEM V PODJETJU ABC

DECEMBER, 2022 SIMONA KOTAR

IZJAVA

SIMONA KOTAR, vpisana v izobraževalni program za pridobitev strokovnega naziva preizkušeni revizor informacijskih sistemov, izjavljam, da sem avtorica tega zaključnega dela in skladno s 1. odstavkom 21. člena Zakona o avtorskih in sorodnih pravicah dovoljujem objavo zaključnega dela na spletnih straneh Slovenskega inštituta za revizijo.

V Celju, 28. 11. 2022

Podpis: 

POVZETEK ZA POSLOVODSTVO

V obdobju med 1.4.2021 in 30. 4. 2021 smo izvedli pregled dodeljevanja, odvzemanja in spreminjanja uporabniških dostopov v SAP sistem v podjetju ABC za obdobje od 1. 1. 2020 do 31. 12. 2020. Pri pregledu smo se osredotočili na trenutno stanje delovanja in učinkovitosti notranjih kontrol na področju pregleda.

Cilj pregleda je bil podati neodvisno mnenje glede delovanja notranjih kontrol procesa dodeljevanja, odvzemanja in spreminjanja uporabniških dostopov v SAP sistem v dogovorjenem obdobju.

Na podlagi ugotovitev in prepoznanih tveganj smo ugotovili, da trenutno vzpostavljene notranje kontrole in upravljanje tveganj na področju dodeljevanja, odvzemanja in spreminjanja dostopov v SAP sistem v podjetju ABC **pomembno odstopajo od sodil, ki so bila uporabljena v pregledu in da notranje kontrole niso vzpostavljene oziroma ne delujejo in niso učinkovite**.

Vsa ugotovljena odstopanja posredno ali neposredno izhajajo iz ključne ugotovitve, da **podjetje ABC nima vpeljanega lastništva nad procesi in podatki ter da nima opredeljenih odgovornosti in pooblastil**, na podlagi katerih bi se lahko vzpostavile učinkovite in delujoče notranje kontrole (več v poglavju 3.1). Zaradi tega dokazano prihaja do medsebojnih posojanj in izmenjevanj uporabniških imen in gesel, zaradi česar ni zagotovljena revizijska sled konkretnega uporabnika, ki je v sistemu izvajal določene aktivnosti. Ob pomanjkljivi revizijski sledi se zabrišejo dokazi, kateri uporabnik je v sistemu izvedel določeno aktivnost ter datum in vrsta spremembe.

Zaradi šibkih varnostnih nastavitev SAP sistema je izredno povečano tveganje prevar, saj lahko nepooblaščeni zaposleni ali zunanji uporabniki izkoristijo pomanjkljive varnostne nastavitve. Nekatere najpogostejše prevare, do katerih lahko pride zaradi preohlapnega upravljanja z dostopi v SAP sistemu, so da uporabniki, ki imajo preširoko dodeljene dostope:

- ustvarijo fiktivne dobavitelje, ponaredijo vknjižbe obveznosti in izvedejo plačila fiktivnim dobaviteljem,
- ustvarijo fiktivne zaposlene, ki lahko prejemajo mesečno plačo na izbran transakcijski račun,
- spremenijo matične podatke o dobaviteljih in preusmerijo izvedena plačila prejetih računov na izbran transakcijski račun,
- v sodelovanju s strankami podjetja ABC spremenijo prodajne pogoje (višji popust, daljši plačilni rok) za doseganje prodajnih ciljev in višjega zneska izplačila nagrade za uspešnost,
- odtujijo zaloge in v sistemu spremenijo stanje zalog, in podobno,

s čimer lahko povzročijo občutno finančno in poslovno škodo podjetju in škodujejo njegovemu dobremu imenu, če splošna javnost izve za morebitne prevare.

S pregledom smo ugotovili naslednja ključna odstopanja:

- SAP vloge, ki so bile dodeljene posameznim uporabnikom, niso pregledno povezane z njihovimi delovnimi nalogami. Uporabniški dostopi ne ustrezajo potrebam poslovnih procesov, zato si uporabniki za nemoteno izvajanje nalog med seboj posojajo uporabniška imena in gesla. To lahko privede tudi do tega, da zaposleni v enem oddelku izvajajo aktivnosti, ki so v pristojnosti drugega

oddelka (na primer nabavniki lahko izvajajo plačila računov dobaviteljem, za povečanje prodaje lahko prodajniki popravljajo cenike izdelkov in višino popustov, ki jih dobijo njihove stranke, zaposleni lahko sami sebi popravljajo višino plače …). Več v točkah 3.2 in 3.6.

- Svetovalci podjetja Kr-eni so za namene oddaljene administracije ustvarili uporabnika »Kr_Eni« s SAP_ALL pravicami. Po implementaciji so strokovnjaki podjetja Kr-eni zadržali pravice do produkcijskih modulov SAP za hitrejše in učinkovitejšo podporo na daljavo kot tudi vsakoletno pomoč pri vzpostavitvi novega finančnega leta. To pomeni, da lahko neznana oseba, ki ni zaposlena v podjetju in nima pooblastil za izvajanje določenih aktivnosti v sistemu, le-te izvaja nenadzorovano in za seboj izbriše vse sledi o izvedeni aktivnosti. Več v točki 3.3.
- Dostopna gesla za predvgrajene privilegirane račune v SAPu so splošno znana v javnosti, kar pomeni, da ni mogoče nadzorovati, kdo se z uporabo teh dostopnih podatkov prijavlja v sistem, zaradi česar so takšni nepooblaščeni dostopi neopaženi. Več v poglavju 3.7.
- Nastavitve varnostnih parametrov za gesla omogočajo, da uporabnik izbere kratko, hitro ugotovljivo geslo, ki ga ni potrebno redno menjati in hkrati dajejo neomejeno število poskusov prijave. To povečuje tveganje, da bodo gesla ugotovili in uporabili nepooblaščeni uporabniki. Več v točki 3.8.
- Prepoznali smo 176 uporabnikov, ki imajo dodeljene kritične avtorizacije. Za tako veliko število uporabnikov nismo uspeli pridobiti ustrezne razlage ne v oddelku IT ne pri poslovnih uporabnikih, kar kaže na pomanjkanje rednega pregleda dodeljenih dostopov. S kritičnimi avtorizacijami dobijo uporabniki pravico do uporabe programov in nastavitev, ki so ključne za izvajanje posameznih aktivnosti in procesov, kot so na primer nastavitve matičnih podatkov (izbirni seznami možnih vnosov), kreiranje povezav med podatki, kreiranje in spreminjanje izgledov dokumentov ter določanje podatkov z obveznim vnosom, določanje formul za avtomatične izračune za posameznim poljem, vzpostavitev in spreminjanje scenarijev za odobritev in sprostitev dokumentov, nastavitve za zajemanje revizijske sledi in podobno, s čimer se povečuje tveganje nenamernega izbrisa celotnega nabora podatkov, uporabnikov ali dostopov. Več v točki 3.5.
- Pri 400 zaposlenih v podjetju ABC je v sistemu SAP aktivnih 854 uporabnikov, od katerih se jih 219 ni prijavilo v sistem v zadnjih 4 mesecih, 11 pa se jih sploh nikoli ni prijavilo v sistem. Preverili smo obstoječe uporabnike s seznamom aktivnih zaposlenih in ugotovili, da imajo aktivne dostope do SAP sistema še vedno nekdanji zaposleni ter zunanji sodelavci, katerim so potekle pogodbe o sodelovanju. Poleg tega je bil uporabnik v SAPu kreiran tudi za zaposlene na delovnih mestih, ki pri delu ne uporabljajo SAPa. Ker se za vsakega uporabnika zakupi licenca, navedeno predstavlja podvojen strošek nakupa in vzdrževanja SAP licenc, saj bi se lahko ponovno uporabile licence, ki so jih uporabljali nekdanji zaposleni. Več v točki 3.9.

Navedene ugotovljene pomanjkljivosti in šibke varnostne nastavitve so povzročile prepoznano kritično tveganje prevare, o katerem smo že med samim izvajanjem pregleda obvestili podjetje ABC in zunanjega revizorja računovodskih izkazov, ZR d. o. o., in svetovali, da se vse ugotovljene informacije predajo odgovorni osebi za preiskovanje prevar. Uporabnik, ki ga nismo mogli prepoznati, saj je za dostop v SAP uporabljal neimenskega uporabnika (LEPA_BRENA), je imel dodeljeno vlogo SAP_ALL, s katero je ustvaril fiktivnega uporabnika, s katerim je ponaredil in poravnal obveznosti do dobavitelja v skupni vrednosti 17.532€ in s tem škodoval podjetju ABC. Izvedene aktivnosti tega uporabnika nakazujejo na kršitve več načel informacijske varnosti in predstavljajo notranjo grožnjo, saj je

uporabnik zlorabil svoj dostop in s tem negativno vplival in škodoval podjetju ABC. Podrobnosti so predstavljene v točki 3.10.

Podana priporočila za odpravo pomanjkljivosti bodo prispevala k zmanjšanju prepoznanih tveganj in okrepila varnost sredstev podjetja ABC. Poslovodstvu podjetja ABC svetujemo, da v roku enega leta izvede porevizijski pregled in ugotovi stanje realizacije priporočil.

KAZALO VSEBINE

KAZALO TABEL

KAZALO SLIK

1 SPLOŠNE INFORMACIJE O PREGLEDU

Na podlagi sklenjene Listine o poslu št. 1/2021 z dne 30. 3. 2021 sta se naročnik posla Podjetje ABC in izvajalec posla Simona Kotar sporazumela o izvedbi pregleda dodeljevanja, odvzemanja in spreminjanja uporabniških dostopov v SAP sistem v podjetju ABC, d. o. o., (v nadaljevanju: podjetje ABC) za obdobje od 1. 1. 2020 do 31. 12. 2020 in poročanju o trenutnem stanju delovanja in učinkovitosti notranjih kontrol na področju dodeljevanja, odvzemanja in spreminjanja dostopov v SAP sistem.

Izvajalec se je s sklenjeno listino o poslu zavezal, da se bo pregled izvedel skladno s Hierarhijo pravil revidiranja informacijskih sistemov (Uradni list RS, št. 40/2011 z dne 27. 5. 2011 z dopolnitvami Uradni list RS, št. 47/2013 z dne 31.5.2013 ter Uradni list RS, št. 28/2015 z dne 24.4.2015). Ta hierarhija od izvajalca zahteva, da razen zakonskih podlag pri svojem delu upošteva standarde, smernice ter orodja in tehnike za strokovnjake revidiranja, kontrol in dajanja zagotovil na področju IT (ITAF: Okvir strokovnega ravnanja za dajanje zagotovil/revidiranje IS, ki ga izdaja ISACA). Standardi od izvajalca zahtevajo izpolnjevanje etičnih zahtev ter načrtovanje in izvedbo pregleda za pridobitev sprejemljivega zagotovila, da notranje kontrole naročnika nimajo nobenih bistvenih pomanjkljivosti glede na naročnikovo poslovanje, okolje, strokovne standarde in dobro prakso.

1.1 Obseg in cilj pregleda

Izvajalec je med 1. 4. 2021 in 30. 4. 2021 opravil pregled s ciljem izraziti neodvisno mnenje glede delovanja notranjih kontrol procesa dodeljevanja, odvzemanja in spreminjanja uporabniških dostopov v SAP sistem v dogovorjenem obdobju, pri čemer se je osredotočil na naslednja tveganja:

- tveganje, da imajo uporabniki dostopne pravice do sistema in informacij, ki jih pri delu ne potrebujejo;
- tveganje, da imajo nepooblaščeni zaposleni dostop do informacij zaupnega značaja;
- tveganje, da imajo nepooblaščeni zaposleni dostop do procesov ali nastavitev, ki lahko kritično vplivajo na poslovni proces;
- tveganje, da lahko zaradi preveč široko dodeljenih dostopov en zaposleni upravlja celoten proces.

Da bi dosegli zastavljen cilj smo:

- preverili skladnost postopka dodeljevanja uporabniških dostopov z internimi pravilniki in dobrimi praksami;
- pregledali procesa vzdrževanja in rednega preverjanja matrike vlog;
- pregledali izvajanje procesa razmejitve odgovornosti (SOD[1]).

Pregled je vključeval izvajanje postopkov za pridobitev revizijskih dokazov o uspešnosti delovanja naročnikovih notranjih kontrol procesa dodeljevanja, odvzemanja in spreminjanja uporabniških dostopov v SAP sistem. Izbrani postopki so bili odvisni od revizorjeve presoje.

[1] SOD – razmejitev odgovornosti (angl. segregation of duties).

Pregled je temeljil na revizijskem načrtu (glej Priloga 2), ki smo ga pripravili skladno z Listino o poslu št. 1/2021 z dne 30. 3. 2021 (glej Priloga 1). Načrt posla je naročnik potrdil dne 5. 5. 2021.

1.2 Uporabljena sodila za presojo

Izvajalec je poleg internih pravilnikov s področja varovanja informacij pri pregledu uporabil naslednje smernice in vodila iz standarda ISO/IEC 27001:2013 (dodatek A) in ISO/IEC 27002:2013:

- A.6.1.2. Razmejitev dolžnosti: Nasprotujoče si naloge in področja odgovornosti se morajo razmejiti, da se zmanjšajo možnosti za nepooblaščeno ali nenamerno spreminjanje ali zlorabo sredstev organizacije.
- A.9.2.3. Upravljanje privilegiranih pravic dostopa: Dodelitev in uporaba privilegiranih pravic dostopa se morata omejiti in nadzorovati.
- A.9.2.5. Pregled uporabniških pravic dostopa: Lastniki sredstev morajo pregledovati uporabniške pravice dostopa v rednih časovnih presledkih.
- A.9.2.6. Preklic ali prilagoditev pravic dostopa: Pravice dostopa vseh zaposlenih in zunanjih uporabnikov do informacij in naprav za obdelavo informacij se morajo odstraniti po prekinitvi njihove zaposlitve, pogodbe ali dogovora oziroma se prilagoditi spremembam.

Kot sodila smo smiselno uporabili tudi COBIT 2019 kontrolne cilje DSS05.04 Upravljanje uporabniške identitete in logičnega dostopa (angl. Manage user identity and logical access) zrelostnega modela 2 in deloma 3[2].

1.3 Prejemniki poročila

Kot je bilo dogovorjeno z Listino o poslu so prejemniki Poročila o izvedenem poslu:

- poslovodstvo podjetja ABC,
- vodja Sektorja za informatiko podjetja ABC,
- vodja Informacijske varnosti podjetja ABC.

Končno poročilo je bilo naslovnikom poslano elektronsko.

1.4 Neodvisnost izvajalca in odgovornost naročnika

Izvajalec zagotavlja, da z opravljanjem posla za naročnika ni v navzkrižju interesov in v nasprotju z zakonskimi določili. V zadnjih dveh letih izvajalec ni sodeloval na področju izboljšanja delovanja notranjih kontrol in procesov, ki so predmet pregleda, poleg tega ni sorodstveno povezan s poslovodstvom ali vodstvom področja pregleda naročnika. Med izvajanjem posla se je izvajalec izogibal

[2] COBIT 2019 Framework: Governance and Management Objectives, izdala ISACA. DSS 05.04 Manage user identity and logical access;
Activities for Capability Level 2: Maintain user access rights in accordance with business function, process requirements and security policies. Align the management of identities and access rights to the defined roles and responsibilities, based on least-privilege, need-to-have and need-to-know principles.
Activities for Capablity Level 3: Administer all changes to access rights (creation, modifications and deletions) in a timely manner based only on approved and documented transactions authorized by designated management individuals.

nerevizijskim vlogam v pobudah, ki niso povezane z revidiranjem in zahtevajo prevzem upravljavskih zadolžitev.

Poslovodstvo naročnika sprejema in pozna svojo odgovornost za táko notranje kontroliranje, kot ga poslovodstvo opredeli kot potrebno, da bodo doseženi kontrolni cilji. Poslovodstvo je izvajalcu zagotovilo:

- dostop do vseh informacij, za katere poslovodstvo ve, da so pomembne na revidiranem področju,
- dodatne informacije, ki jih je izvajalec zahteval od poslovodstva za namen pregleda,
- neomejen dostop do vseh oseb v organizaciji, ki jih je za pridobitev revizijskih dokazov določil izvajalec.

Vsa dokumentacija, predstavitve in drugi podatki, ki jih je izvajalec prejel pri izvajanju pregleda, so obravnavani kot poslovna skrivnost. Delovno gradivo v elektronski obliki bo izvajalec predal naročniku najkasneje v štirinajstih dneh po potrditvi prejema končnega poročila.

1.5 Omejitve pri pregledu

V pregled niso bile zajete ostale informacijske rešitve naročnika in tehnološka infrastruktura, na kateri delujejo.

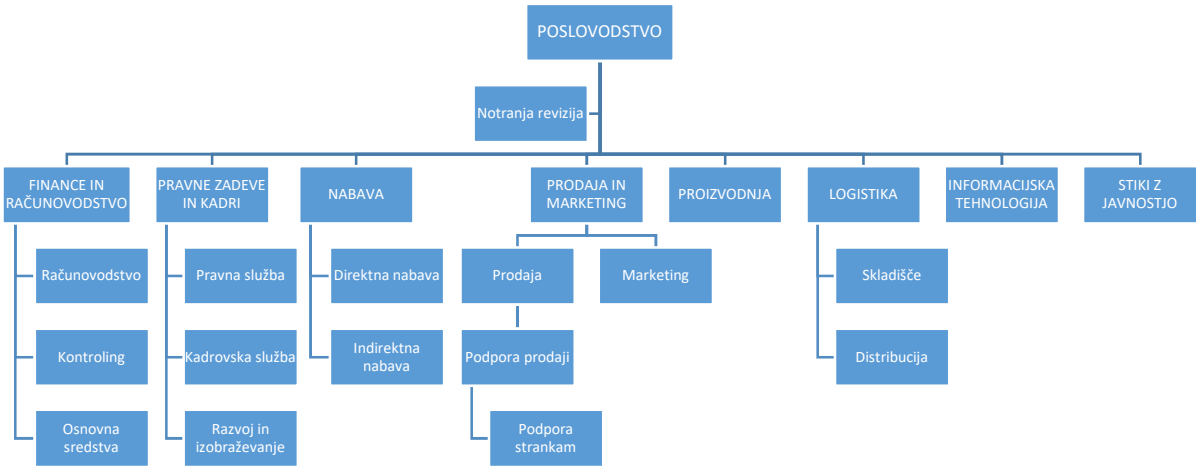
Zaradi naravnih omejitev pregleda skupaj z naravnimi omejitvami notranjega kontroliranja se ni bilo mogoče izogniti tveganju, da nismo odkrili kakšnih pomembnih pomanjkljivosti v zasnovi in delovanju notranjih kontrol, kljub temu, da je bil pregled pravilno načrtovan in opravljen v skladu s standardi, smernicami ter orodji in tehnikami za strokovnjake revidiranja, kontrol in dajanja zagotovil na področju IT.

Na podlagi izvedenih postopkov menimo, da smo pridobili zadostna dokazila za izdajo neodvisnega mnenja.

2 PREDSTAVITEV PODROČJA PREGLEDA

Podjetje ABC deluje v gospodarskem sektorju proizvodnje in se ukvarja s predelavo lokalnega mesa v mesne izdelke visoke kakovosti in z visoko dodano vrednostjo. Podjetje ima v povprečju 400 zaposlenih, meso pa odkupuje od lokalnih kooperantov.

Slika 1: Organigram podjetja ABC



Vir: Lastni prikaz.

V letu 2016 je podjetje ABC pristopilo k uvedbi informacijske rešitve SAP, s katero je nameravalo nadomestiti prej ločene informacijske rešitve, s katerimi je podpiralo področja finančnega računovodstva, človeških virov, skladiščenja, nabave in prodaje. Za stare informacijske rešitve podjetja ABC ni bilo več na voljo storitev vzdrževanja, temveč jih je moral ob spremembah zakonodaje prilagoditi kar eden izmed bivših zaposlenih informatikov, ki se je upokojil leta 2012. Področja stroškovnega poročanja in kontrolinga in osnovnih sredstev je podjetje ABC podpiralo v tabelah Excel, ki so jih razvili uporabniki.

Za izvajalca storitev uvedbe informacijske rešitve SAP je podjetje ABC izbralo podjetje Kr-eni, d. o. o., informacijske storitve in svetovanje (v nadaljevanju: podjetje Kr-eni). Podjetje Kr-eni je podjetju ABC v podpis predložilo pogodbo (v nadaljevanju: pogodba o vzpostavitvi informacijske rešitve SAP), v kateri sta se podjetji dogovorili da:

- bo podjetje Kr-eni podjetju ABC pomagalo pri pripravi funkcionalnih specifikacij za uvedbo informacijske rešitve SAP 2016 specifično za podporo organizacijskim procesom:
  - finance in računovodstvo, ki ju bo pokrival modul SAP Financial Accounting,
  - kontroling, ki ga bo podpiral modul SAP Controlling,
  - prodaja, ki jo bo podpiral modul SAP Sales and Distribution,
  - nabava in proizvodnja, ki ju bo podpiral modul SAP Production Planning,
  - skladiščenje, ki ga bo podpiral modul SAP Materials Management,
  - človeški viri, ki ga bo podpiral modul SAP Human Capital Management,
  - vzdrževanje, ki ga bo podpiral modul SAP Plant Maintenance in
  - zagotavljanje kakovosti, ki ga bo podpiral modul SAP Quality Management;

  in tehnična modula SAP BASIS in SAP ABAP;
- bo podjetje Kr-eni podjetju ABC pripravilo načrt prenosa podatkov iz ločenih informacijskih rešitev in tabel, s katerimi je podjetje prej podpiralo svoje poslovanje, vključno z obstoječimi dostopnimi pravicami v posameznih parcialnih informacijskih rešitvah;
- bo podjetje Kr-eni podjetju ABC vzpostavilo shemo standardnih SAP poslovnih vlog (angl. business roles) glede na »standard«;

- bo podjetje Kr-eni podjetju ABC uvedlo informacijsko rešitev SAP vključno s potrebnimi prilagoditvami, nadgradnjami in konfiguracijami ter da bo izvedlo prenos podatkov iz ločenih informacijskih rešitev;
- bo podjetje Kr-eni izvedlo izobraževanje za vse zaposlene v podjetju.

Podjetji ABC in Kr-eni sta se v pogodbi tudi dogovorili, da bo podjetje Kr-eni to izvedlo v 18 mesecih.

S 6 mesečno zamudo je podjetje Kr-eni, podjetju ABC predalo implementirano rešitev s prenesenimi podatki iz posameznih parcialnih rešitev. Strokovnjaki podjetja Kr-eni so zadržali pravice do produkcijskih modulov SAP, za hitrejše in učinkovitejšo podporo na daljavo, kakor tudi vsakoletno pomoč pri vzpostavitvi novega finančnega leta. Podjetje ABC ima sicer tudi lastno službo za IT, ki ima štiri zaposlene, od katerih so se trije zaposlili po uvedbi rešitve SAP.

Podjetje Kr-eni je 12 mesecev po podpisu pogodbe v 2 mesecih izvedlo 7 različnih sklopov izobraževanj na testnem okolju. Ker še ni bilo jasno, kako bo po novem organizirano delo, so vsi uporabniki dobili vse pravice.

Podjetje Kr-eni je podjetju ABC v letu 2019 pomagalo pridobiti certifikat za sistem upravljanja varovanja informacij (ISO/IEC 27001:2013) za celotno podjetje, ki ga je izdalo podjetje Everthing4You iz Moldavije. Za certifikacijo so pripravili tudi politiko varovanja, kakor tudi opisali proces upravljanja (dodeljevanja, odvzemanja, spreminjanja) uporabniških dostopov.

Podjetje ABC je imelo v zadnji dveh letih 15 % letno fluktuacijo med posameznimi oddelki. Poleg tega so kadrovska statistična poročila za zadnji dve leti izkazovala, da je bil vsak zaposleni letno v povprečju 25 dni na dopustu in 10 dni na bolniški odsotnosti. V zadnjih dveh letih so začasno zaposlili 5 delavcev, zaradi 7 sodelavk, ki so bile na daljši bolniški odsotnosti (3 porodniških). V zadnjih dveh letih se je 12 delavcev upokojilo.

3 UGOTOVITVE OPRAVLJENIH POSTOPKOV IN PREDLOGI PRIPOROČIL

V nadaljevanju predstavljamo ugotovitve, prepoznana tveganja za posamezno ugotovitev in priporočila, na podlagi katerih ocenjujemo, da se lahko prepoznano tveganje zmanjša na sprejemljivo raven. Tveganja smo ocenili na podlagi Matrike za določanje stopnje tveganja, ki je predstavljena v tabeli 1.

Tabela 1: Matrika za določanje stopnje tveganja

STOPNJA TVEGANJA	OPIS
Visoko tveganje	Ko ugotovitev kaže na pomembno pomanjkljivost v delovanju notranjih kontrol in/ali tveganje ni ustrezno obvladovano: • ki so v zakonodaji opredeljena kot kršitve zakonodaje najvišje stopnje (najhujše, najtežje in hujše kršitve - opredelitev glede na področno zakonodajo) ne glede na to, ali gre za namenske in nenamenske kršitve, • ki kažejo na sistemske in/ali posamične napake oziroma kršitve zunanjih in notranjih predpisov, • ko revizor oceni, da ima lahko dejanje vpliv na dolgoročno uspešnost/doseganje ciljev družbe. Sem sodijo tudi prevare, za katere lahko s pisnimi dokumenti/dokazili potrdimo sum in ki ogrožajo delovanje družbe. Ugotovitve z ocenjeno visoko stopnjo tveganja je potrebno odpraviti v čim krajšem možnem času.
Srednje tveganje	Ko ugotovitev kaže na zmerno pomanjkljivost v delovanju notranjih kontrol in/ali tveganje ni ustrezno obvladovano: • ki so v zakonodaji opredeljena kot kršitve zakonodaje (nižje od tistih, opredeljenih v visokem tveganju) ne glede na to, ali gre za namenske in nenamenske kršitve, • ki kažejo na manjše sistemske napake, manjše pomanjkljivosti v delovanju notranjih kontrol, posamične napake ali kršitve notranjih predpisov, • ko revizor oceni, da ima lahko dejanje vpliv na kratkoročno uspešnost/doseganje ciljev družbe. Sem sodijo pomanjkljivosti, katerih odprava doprinese k bistvenemu izboljšanju delovanja notranjih kontrol in s tem izvajanju procesov in ki lahko v kombinaciji z vpeljavo novih procesov ali z opustitvijo drugih kontrolnih mehanizmov vodijo do večjih tveganj.
Nizko tveganje	Ko ugotovitev kaže na: • manjše in posamične napake, pomanjkljivosti pri delovanju notranjih kontrol in neupoštevanje notranjih predpisov in • ko skoraj ni možnosti, da bi prišlo do izgube ugleda. Sem sodijo pomanjkljivosti, katerih odprava pomeni izboljšavo sistema ali procesa, ne predstavljajo pa neposredne ogroženosti doseganja zastavljenih ciljev ali neskladnosti z zakonodajo oziroma internimi pravilniki.
Ostala opažanja	Gre le za opažanja, ki bi lahko pripomogla k učinkovitejšemu in uspešnejšemu delu. Poslovodstvo mora presoditi, ali so koristi od uvedbe ukrepov na tem področju večje od vseh stroškov. Namen je predvsem pomoč vodstvu pri prepoznavanju priložnosti za izboljšavo.

Vir: Lastni prikaz.

3.1 Pravilnik o upravljanju uporabniških dostopov

UGOTOVITEV:

Postopki dodeljevanja, odvzemanja in spreminjanja uporabniških dostopov (imen) do informacijskih sistemov podjetja ABC niso zapisani v formalnem dokumentu. Ko se v podjetju ABC zaposli novi delavec, njegov nadrejeni praviloma piše v IT službo, da potrebuje zanj nove dostope. Ker pri administraciji informacijskega sistema SAP še vedno pomagajo svetovalci podjetja Kr-eni, zaposleni za pridobitev novih uporabniških imen in dostopov včasih pokličejo kar njih. Med pogovorom z revidirancem in po pregledu obstoječe dokumentacije smo ugotovili, da podjetje nima opredeljenega lastništva nad procesi in podatki, prav tako nima opredeljenih odgovornosti in pooblastil, na podlagi katerih bi se lahko vzpostavile učinkovite in delujoče notranje kontrole.

 **– VISOKO TVEGANJE:**

Zaradi formalno neopredeljenih postopkov dodeljevanja, odvzemanja in spreminjanja uporabniških dostopov je povečano tveganje, da imajo zaposleni dodeljene dostope, ki jih pri delu ne potrebujejo oziroma dodeljene dostope, ki ne zagotavljajo razmejitve odgovornosti (SOD), s čimer je povečano tveganje prevar. Najpogostejše prevare, do katerih lahko pride zaradi preširoko dodeljenih dostopov so:

- kreiranje fiktivnih dobaviteljev, ponaredba vknjižbe obveznosti in izvedba plačila fiktivnim dobaviteljem,
- kreiranje fiktivnih zaposlenih, ki prejemajo mesečno plačo na izbran transakcijski račun,
- sprememba matičnih podatkov o dobaviteljih in preusmeritev izvedenih plačil prejetih računov na izbran transakcijski račun,
- v sodelovanju s strankami podjetja ABC sprememba prodajnih pogojev (višji popust, daljši plačilni rok) za doseganje ciljev in izplačila višjega zneska nagrade za uspešnost,
- odtujitev zaloge materialov ali izdelkov in sistemska sprememba stanja zaloge skozi na primer odpis uničene/poškodovane robe, in podobno,

s čimer lahko povzročijo občutno škodo podjetju ABC, tako finančno in poslovno, kot tudi škodo dobremu imenu podjejta, v kolikor informacije o morebitnih prevarah pridejo v javnost.

PRIPOROČILO 1:

Podjetju ABC priporočamo vzpostavitev procesa upravljanja uporabniških dostopov in izdajo internega pravilnika, ki opredeljuje postopke dodeljevanja, odvzemanja in spreminjanja uporabniških dostopov, vključno s predpisanimi obrazci in koraki odobritve potrebnimi za dodelitev, odvzem ali spremembo dostopa do posameznega informacijskega sistema oziroma podatkov. Iz obrazca naj bo razvidno, kdo je zahtevek za dodelitev dostopa izdal, kakšna je poslovna potreba, katere dostope zaposleni potrebuje, časovno omejitev dostopa, v kolikor je potrebna, kdo je zahtevek odobril in kdo je v sistemu dostop zaposlenemu dodelil.

Priporočamo, da se zaradi zagotavljanja celovitosti, zaupnosti in integritete, vzpostavljeni proces izvaja izključno interno, zunanje svetovalce se pa vključuje zgolj za potrebe svetovanja in ne izvajanja procesa.

3.2 Načela razmejevanja odgovornosti

Uvedba informacijskega sistema SAP naj bi potekala po natančno vnaprej predvidenih korakih, med katerimi je faza t.i. poslovnega načrtovanja (angl. business blueprint). Del faze poslovnega načrtovanja je analiza razlik med obstoječimi organizacijskimi procesi in funkcionalnostmi informacijskega sistema SAP (angl. gap analysis) in uskladitev (angl. mapping) funkcionalnosti standardnih modulov SAP z obstoječimi poslovnimi procesi. V tej fazi naj bi lastniki poslovnih procesov vsaj okvirno opredelili tudi svojim potrebam prilagojene osnovne tipe uporabnikov in njihove uporabniške vloge oziroma skupine funkcionalnosti in dostopov. Tako opredeljeni uporabniški dostopi naj bi bili omejeni po načelu »potreba po vedenju« (angl. need-to-know) in zasnovani tako, da spoštujejo načela ločevanja dolžnosti. Fazi poslovnega načrtovanja sledi faza konfiguracije (angl. realization), kjer naj bi svetovalci ustvarili opredeljene vloge in jih uvedli v testno okolje, kjer bi naj bile na voljo za preizkušanje.

UGOTOVITEV:
Podjetje ABC pred uvedbo informacijskega sistema SAP v okviru faz poslovnega načrtovanja in realizacije ni izvedlo popisa poslovnih procesov, ki bi mu omogočilo uskladitev obstoječih poslovnih procesov s standardnimi SAP procesi in funkcionalnostmi, temveč je po nasvetu svetovalcev podjetja Kr-eni preprosto prevzelo standardne SAP procese, ki naj bi po navedbah svetovalcev predstavljali industrijsko najboljšo prakso. Zato podjetje ABC tudi ni oblikovalo svojim potrebam prilagojenih tipov uporabnikov in uporabniških vlog.

– SREDNJE TVEGANJE:

Ker podjetje ABC ni oblikovalo svojim potrebam prilagojenih tipov uporabnikov in uporabniških vlog obstaja tveganje, da imajo uporabniki dostopne pravice do delov sistema in informacij, ki jih pri delu ne potrebujejo, in tveganje, da imajo nepooblaščeni zaposleni dostop do informacij zaupnega značaja. Z dodelano vzpostavitvijo uporabniških vlog se določijo nabori aktivnosti, ki jih lahko zaposleni izvaja znotraj posamezne vloge (npr. vloga nabavnika, ki omogoča kreiranje nabavne naročilnice, vloga kontrolorja nabave, ki omogoča potrjevanje kreiranih naročilnic in nadzorovanje stroškov za posamezno skupino nabav, ali vloga računovodje, ki omogoča knjiženje prejetih računov, in vloga vodje računovodstva, ki omogoča odobritev izvedbe plačil računov), nato se vsakemu uporabniku določi, do katere vloge ima dostop, torej katere korake ali aktivnosti lahko izvaja v sistemu. Odgovornosti se razmejijo tako, da posamezni zaposleni ne morejo izvajati aktivnosti, ki so vsebinsko nezdružljive in pri katerih bi lahko prišlo do napak ali prevar, če bi jih izvajal isti zaposleni (na primer: zaposleni, ki izda nabavno naročilnico, je ne more tudi odobriti (torej, razmejitev odgovornosti znotraj funkcije nabave) ali pa zaposleni, ki izda naročilnico, ne more poknjižiti nastale obveznosti do dobavitelja (torej, razmejitev odgovornosti med dvema funkcijama – nabava in računovodstvo).

PRIPOROČILO 2:
Kljub temu, da se je podjetje ABC odločilo, da prevzame vloge prilagojene standardnim SAP procesom, priporočamo, da te standardne SAP procese uskladi z obstoječimi poslovnimi procesi, z opredeljenimi odgovornostmi in pooblastili opredeli lastništvo nad procesi in podatki, prepozna

začetek in konec posameznega SAP procesa in oblikuje vloge, ki ne omogočajo izvajanja aktivnosti, ki so odgovornost več kot enega poslovnega procesa.

3.3 Dodelitev kritične vloge SAP_ALL

UGOTOVITEV:

Ob uvedbi informacijskega sistema SAP v produkcijsko delovanje se je izkazalo, da uporabniških dostopov, ki so jih zaposleni imeli v prej uporabljanih informacijskih rešitvah, ni mogoče enostavno prenesti v novi sistem. Svetovalci podjetja Kr-eni so zato na enem izmed usklajevalnih sestankov vodje organizacijskih enot zaprosili, da jim pripravijo sezname zaposlenih in opišejo njihove naloge. Pred uvedbo informacijskega sistema SAP v produkcijsko delovanje so bodoči uporabniki sistem preizkusili v testnem okolju. Da bi se izognili dodatnemu delu s konfiguracijo uporabnikov za vsakega posameznega zaposlenega in ker sistema SAP nikoli ni sočasno preizkušalo oziroma se v njem učilo več kot 15 uporabnikov, so svetovalci podjetja Kr-eni vzpostavili 20 uporabnikov, poimenovanih Testni_uporabnik od 1 do 20. Da bi se izognili dodatnemu delu s konfiguracijo prilagojenih osnovnih tipov uporabnikov in prilagojenih uporabniških vlog, so svetovalci podjetja vsem uporabnikom v testnem okolju podelili vlogo SAP_ALL[3]. Da bi testiranje in učenje čim bolje potekala, so svetovalci podjetja Kr-eni v testnem okolju vzpostavili kopijo produkcijskih podatkov.

– VISOKO TVEGANJE:

Ker se v testnem okolju uporabljajo produkcijski (dejanski) podatki in so hkrati uporabnikom dodeljene vloge, ki omogočajo neomejene dostope (SAP_ALL), obstaja povečano tveganje razkritja zaupnih informacij, saj ni razmejenih vlog, s katerimi se omejuje dostop do izvajanja procesov in podatkov. Vsi zaposleni lahko z neomejenimi dostopi dostopajo do vseh informacij, ki so na voljo v sistemu, ne glede na to, v katerem oddelku delajo, čeprav gre za testno okolje, saj se v tesnem okolju uporabljajo dejanski podatki. Poleg tega pa v testnem sistemu ni mogoče zagotoviti omejitev dostopa do osebnih podatkov in lahko osebne podatke zaposlenih, vključno z višino plače, pregledujejo vsi zaposleni in ne le kadrovniki. To lahko vodi tudi do uhajanja informacij in izgube dobrega imena podjetja.

Poleg tega je testno okolje namenjeno preverjanju izvajanja procesov od začetka do konca, preden je nastavitev prenesena v produkcijsko okolje. Če imajo v testnem okolju vsi zaposleni vse dostope, se ne more preveriti učinkovitega izvajanja procesov od začetka do konca z uporabo vlog, kot so dodeljene v produkcijskem okolju.

PRIPOROČILO 3:

Podjetju ABC priporočamo, da v testnem sistemu uporablja izmišljene podatke, v kolikor ne more zagotoviti razmejevanja odgovornosti oz. dodeliti dostop do podatkov, ki jih uporabnik potrebuje za izvajanje procesov, za katere je odgovoren (angl. need-to-know).

[3] SAP_ALL profil vsebuje vse SAP avtorizacije, s čimer je omogočeno neomejeno izvajanje vseh aktivnosti v SAP sistemu. SAP_ALL profil je namenjen razvijalcem in administratorjem v produkcijskem okolju samo izjemoma, kadar je nujno potrebno in ni možno na drugačen način spremeniti nastavitev, ki povzročajo nedelovanje SAP sistema. Uporaba SAP_ALL profila v produkcijskem okolju mora biti odobrena s strani vodstva podjetja, dodeljena le za omejeno obdobje, vse aktivnosti pa nadzorovane (vklopljena možnost sledenja aktivnostim »Trace On«).

Ker uporabniške vloge niso usklajene s poslovnimi procesi, svetujemo, da se v testnem okolju vzpostavijo in testirajo enake vloge, kot jih podjetje uporablja v produkcijskem okolju. Tako se bo lahko pred vsako spremembo vlog omogočilo preverjanje delovanja in uporabnosti vlog in zagotovilo, da se proces nemoteno izvaja že pred uvedbo sprememb v produkcijsko okolje.

UGOTOVITEV:

Svetovalci podjetja Kr-eni so za namene oddaljene administracije ustvarili uporabnika »Kr_Eni« s SAP_ALL pravicami. Kot je predstavljeno v poglavju 2 Predstavitev področja revidiranja, so strokovnjaki podjetja Kr-eni zadržali pravice do produkcijskih modulov SAP za hitrejše in učinkovitejšo podporo na daljavo, kakor tudi vsakoletno pomoč pri vzpostavitvi novega finančnega leta.

Spletni priročnik za SAP[4] navaja, da se:

1. profil SAP_ALL ne sme dodeliti nobenemu uporabniku v organizaciji;
2. kreira naj se samo en uporabnik s profilom SAP_ALL, geslo za tega uporabnika naj bo skrito in zavarovano (zaklenjeno v sefu);
3. uporabnik s profilom SAP_ALL se naj uporabi le v nujnih primerih.

Standard ISO/IEC 27002:2013 v kontroli A.9.2.3 Upravljanje s privilegiranimi dostopnimi pravicami postavlja cilj »Dodeljevanje in uporaba privilegiranih dostopnih pravic se omeji in nadzoruje«. V nadaljevanju napotuje, da se morajo privilegirane dostopne pravice dodeljevati uporabnikom na osnovi potrebe po uporabi (angl. need-to-use) in le za posamezne dogodke (angl. event-by-event basis). Ob dodelitvi privilegiranega dostopa je potrebno opredeliti trajanje dodelitve in določiti datum poteka dodelitve, ko se bodo dostopi avtomatično onemogočili.

● **– VISOKO TVEGANJE:**

Skladno z dobrimi praksami in standardi dodelitev pravic SAP_ALL predstavlja kritično tveganje, da imajo nepooblaščeni zaposleni dostop do procesov in nastavitev, ki lahko kritično vplivajo na poslovni proces, saj lahko ti uporabniki nedovoljeno in nenadzorovano upravljajo, spreminjajo ali prilagajajo nastavitve in spreminjajo podatke, poleg tega pa predstavlja tudi tveganje, da imajo nepooblaščeni zaposleni dostop do informacij zaupnega značaja. Dejanski primer zloraba dodeljene pravice SAP_ALL je bil prepoznan med samo izvedbo pregleda in je predstavljen v točki 3.10.

Posameznik, ki sme ali lahko izvaja celotno verigo procesov, ima enostavno možnost izvajati transakcije, ki pri odsotnosti ustreznih kontrol za organizacijo pomenijo tveganje nesmotrnega ali celo škodljivega ravnanja, kar je bilo ugotovljeno tudi v tem pregledu (podrobnosti v točki 3.10). Poleg tega je omenjena vloga dodeljena zunanjemu, neimenskemu uporabniku, s čimer se ne more zanesljivo prepoznati, katera oseba in za katere namene s tem uporabnikom dostopa v sistem SAP. SAP svetovalci nudijo podporo za vzdrževanje SAPa in niso vključeni v samo izvajanje poslovnih procesov, zato ne potrebujejo dostopov v produkcijskem okolju. Skladno z dobrimi praksami[5] naj bi imeli zunanji

[4] Dosegljiv na strani https://help.sap.com/docs.

[5] ISO/IES 27001:2013 A.12.1.4 Ločevanje razvojnih, testnih in produkcijskih okolij.

svetovalci, ki nudijo pomoč pri vzdrževanju in razvoju SAPa, dostope do razvojnih sistemov. V primeru navodil, napotkov, usmeritev ali razlag delovanja sistema se naj bi uporabljal testni sistem, ki naj bi bil kopija produkcijskega sistema. Le v primeru kritičnih incidentov sme zunanji svetovalci pridobiti dostop do produkcijskega sistema, pa še to samo za **omejeno obdobje**. Tako široka dodelitev dostopov predstavlja namreč neomejen in nepooblaščen dostop do zaupnih osebnih in poslovnih podatkov, možnost kreiranja fiktivnih poslovnih dogodkov, finančnih zlorab, uničevanja podatkov in tveganj prevar.

PRIPOROČILO 4:

Skladno z dobrimi praksami priporočamo podjetju ABC, da takoj odvzame vlogo SAP_ALL vsem uporabnikom. Dodatno priporočamo, da se kreira poseben uporabnik s profilom SAP_ALL, katerega geslo je skrito in zaklenjeno v sefu in se uporablja le v nujnih primerih in izključno za obdobje, ko je tak dostop potreben za odpravljanje kritičnih napak v delovanju sistema SAP. Za posebnega uporabnika z dodeljeno vlogo SAP_ALL priporočamo, da se vklopi sledenje aktivnostim uporabnika.

Dodatno priporočamo, da se vzpostavi redno (vsaj 2x letno) izvajanje podrobnega pregleda dodeljenih pravic zunanjim uporabnikom SAP sistema. V primeru dodeljenih vlog, ki omogočajo širok obseg dostopa do podatkov in informacij, priporočamo obvezno dokumentiranje upravičenosti dodelitve vloge in kratko časovno omejitev dostopov.

3.4 SAP neimenski (generični) uporabniki

UGOTOVITEV:

V produkcijskem okolju so sicer svetovalci podjetja Kr-eni ustvarili uporabnike tako, da jih je bilo mogoče enolično povezati s posameznim zaposlenim, torej tako, da so že sama uporabniška imena vsebovala imena in priimke zaposlenih. S poročilom RSUSR000 v informacijskem sistemu SAP smo preverili seznam trenutno aktivnih uporabnikov. Med ažurnimi aktivnimi uporabniki smo našli nekatere, ki jih nismo mogli povezati z imeni in priimki zaposlenih, med drugim USER001, JAMES_BOND, PAJO_PATAK, VESELA_OMLETA in LEPA_BRENA. Poleg tega so svetovalci podjetja Kr-eni ustvarili 8 uporabnikov »Pripravnik« od 1 do 8 za sodelavce pripravnike, s čimer so se izognili zamudnemu ustvarjanju novega uporabnika ob zaposlitvi pripravnikov.

 **– VISOKO TVEGANJE:**

Uporaba neimenskih uporabnikov povečuje tveganje nepooblaščenih dostopov do izvajanja poslovnih procesov in podatkov, poleg tega je v teh primerih revizijska sled neuporabna, saj ni povezave med posameznim uporabnikom in zaposlenim, ki ga uporablja. To pomeni, da kljub dobro vzpostavljenem sledenju izvedenih aktivnosti posameznega uporabnika (na primer kdaj je bila nabavna naročilnica kreirana, kdo jo je kreiral, kdaj je bila odobrena in kdo jo je odobril) ni mogoče določiti osebo, ki je to naredila, saj ne vemo, kateri zaposleni uporablja katerega neimenskega uporabnika.

Ker se uporabniki »Pripravnik« dedujejo, obstaja tveganje, da se gesla ne menjajo, s čimer obstaja tveganje zlorab teh uporabnikov.

PRIPOROČILO 5:

Podjetju ABC priporočamo, da se ukinejo vsi uporabniki, za katere ne more jasno določiti, kateremu zaposlenemu pripadajo.

Zaradi zagotavljanja uporabne revizijske sledi in sledljivosti vnosa, spreminjanja in morebitnega brisanja podatkov v SAPu priporočamo, da se za vse uporabnike SAP sistema, tudi za pripravnike ali študente, kreirajo uporabniki tako, da jih je mogoče enolično povezati s posameznim zaposlenim.

3.5 Uporabniki s kritičnimi avtorizacijami

UGOTOVITEV:

V informacijskem sistemu SAP smo izvedli poročilo RSUSR008_009_NEW, s katerim smo dobili izpis uporabnikov, ki imajo dodeljene kritične avtorizacije. Na njem je bilo 176 uporabnikov. Za tako veliko število uporabnikov nismo uspeli pridobiti ustrezne razlage ne v oddelku IT ne pri poslovnih uporabnikih.

S kritičnimi avtorizacijami dobijo uporabniki pravico do uporabe programov in nastavitev, ki so ključne za izvajanje posameznih aktivnosti in procesov, na primer: nastavitve matičnih podatkov (izbirni seznami možnih vnosov), kreiranje povezav med podatki, kreiranje in spreminjanje izgledov dokumentov ter določanje podatkov z obveznim vnosom, določanje formul za avtomatične izračune za posameznim poljem, vzpostavitev in spreminjanje scenarijev za odobritev in sprostitev dokumentov, nastavitve za zajemanje revizijske sledi in podobno.

– VISOKO TVEGANJE:

Dodeljevanje kritičnih avtorizacij omogoča spreminjanje tabel in povezav podatkov, s čimer se povečuje tveganje nenamernega izbrisa celotnega nabora podatkov, uporabnikov ali dostopov. Poslovni (končni) uporabniki praviloma zelo redko potrebujejo dostope do kritičnih avtorizacij, načeloma jih uporabljajo tehnični skrbniki, ki vzdržujejo izglede v SAPu in povezave v ozadju, da se prikažejo pravilni podatki. Glede na to, da ne IT ne poslovni uporabniki ne morejo pojasniti, zakaj imajo dodeljene te avtorizacije, dodelitev teh avtorizacij ni potrebna, saj zunanji izvajalec izvaja razvoj in vzdrževanje SAP sistema.

PRIPOROČILO 6:

Podjetju ABC priporočamo, da odstranijo kritične avtorizacije vsem uporabnikom, ki ne morejo podati ustrezne razlage, zakaj jih potrebujejo.

3.6 Nabor dodeljenih SAP vlog uporabnikom

UGOTOVITEV:

SAP vloge, ki so bile dodeljene posameznim uporabnikom, niso pregledno povezane z delovnimi nalogami, ki jih ti opravljajo. Ob začetku produkcijskega delovanja SAPa se je namreč izkazalo, da standardne vloge oziroma profili, ki so pred vgrajeni v SAP, ne ustrezajo dejanskim delovnim potrebam zaposlenih. Svetovalci podjetja Kr-eni, ki so v začetku produkcijskega delovanja administrirali rešitev,

so bili zelo obremenjeni in so zaposlenim, ki so nujno potrebovali dodatne dostope, dodelili vlogo oziroma profil SAP_ALL. Ko so se razmere nekoliko umirile, so težavo manjkajočih dostopov reševali tako, da so posameznim uporabnikom ob njihovih obstoječih vlogah dodali še možnosti izvajanja transakcij in pravice na objekte, ki so jih v danem trenutku potrebovali. Kadar je določeno pravico potrebovalo več uporabnikov, so strokovnjaki podjetja Kr-eni ustvarili novo vlogo na podlagi obstoječih vlog in ji dodali pravice, za katere so ocenjevali, da bi jih uporabniki lahko potrebovali.

Pri razgovoru z uporabniki smo ugotovili, da tudi tri leta po končani uvedbi informacijskega sistema SAP v produkcijsko delovanje, uporabniški dostopi še vedno ne ustrezajo potrebam poslovnih procesov. Uporabniki si za nemoteno izvajanje nalog med seboj posojajo uporabniška imena in gesla. Za vseh 18 uporabnikov v računovodstvu smo preverili prijave v sistem med evidentiranim časom letnega dopusta. Na podlagi revizijskih sledi smo ugotovili, da sta dva zaposlena evidentirano izvajala knjiženje prejetih faktur v času, ko sta bila evidentirano na letnem dopustu. Po pogovoru z njima smo ugotovili, da sta svoje dostopne podatke posodila sodelavcem, ki so ju nadomeščali v času odsotnosti in niso imeli dodeljenih dostopov za knjiženje faktur. Vodja računovodstva je pojasnil, da je zunanjim strokovnjakom podjetja Kr-eni večkrat poslal zahtevek za dodelitev dostopov v času nadomeščanja, vendar so dostope dodelili prepozno, ko sta se dotična zaposlena že vrnila iz letnega dopusta. Podporno dokumentacijo, ki dokazuje izmenjavo elektronskih sporočil, smo prejeli tekom izvajanja pregleda.

Standard ISO/IEC 27002:2013 napotuje, da se odobrene in dodeljene dostopne pravice uporabniku dodelijo na način, da mu omogočajo dostop do najmanjšega nabora storitev, funkcij in informacij, ki so potrebne za nemoteno opravljanje delovnih nalog. Dve najbolj pogosti načeli pri dodeljevanju dostopov sta (ISO/IEC 27002:2013, 9.1.1.):

- potreba po vedenju (angl. need-to-know) – uporabniku je dodeljen dostop le do informacij, ki jih potrebuje za izvajanje opravil, za katere je odgovoren;
- potreba po uporabi (angl. need-to-use) – uporabniku je dodeljen dostop le do orodij za obdelavo informacij (IT oprema, aplikacije, postopki, prostori), ki jih potrebuje za izvajanje opravil/dela/vloge, za katero je odgovoren.

Standard ISO/IEC 27002:2013 v kontroli 6.1.2 Ločevanje uporabniških vlog nadalje predpisuje: »*Nasprotujoče naloge in področja odgovornosti je potrebno ločiti, da se zmanjša možnost za nepooblaščeno ali nenamerno spreminjanje ali zlorabo sredstev družbe ABC*«.

– VISOKO TVEGANJE:

Ker podjetje ABC nima opredeljenega koncepta lastništva procesov in podatkov ter jasno opredeljenih pristojnosti in odgovornosti vseh SAP uporabnikov, se zaradi nenadzorovanega in nesistematičnega dodajanja dostopov uporabnikom povečuje tveganje, da imajo zaposleni dostopne pravice do sistemov in informacij, ki jih pri delu ne potrebujejo. S tem se povečuje tveganje nenamernega popravka ali izbrisa podatkov. Uporabnik mora namreč imeti na voljo samo tista pooblastila, ki so potrebna za izvajanje njegovih nalog. Ker pa v podjetju ABC ni jasno opredeljeno, kdo je odgovoren za kateri proces (na primer: nabava je odgovorna za proces od prepoznane potrebe po nabavi do prevzema naročenega

materiala na skladišče) in kdo upravlja s katerimi podatki (na primer: nabava je odgovorna za pravilnost, točnost, ažurnost in popolnost matičnih podatkov, ki se nanašajo na dobavitelje in materiale), se dodajajo dostopi vsakemu, ki misli, da to potrebuje . Tako lahko uporabniki izvajajo tudi aktivnosti, ki niso v njihovi pristojnosti (na primer: nabavnik, ki kreira naročilnice, lahko izvaja tudi plačila prejetih računov), hkrati pa se jim kopičijo dostopi, ki jih pri delu ne potrebujejo. Uporabnik lahko po pomoti izbriše ali spremeni kakšen kritičen podatek, ne da bi se tega zavedal.

Izmenjevanje uporabniških imen in gesel med uporabniki predstavlja tveganje, da izvedenih aktivnosti ni mogoče zanesljivo povezati s konkretnimi uporabniki.

PRIPOROČILO 7:

Podjetju ABC priporočamo, da na podlagi vzpostavljenega lastništva nad procesi in podatki (glej Priporočilo 2) vzpostavi katalog razpoložljivih vlog, ki odražajo potrebe poslovnih procesov, in vzpostavi proces sistematičnega in dokumentiranega dodeljevanja in odstranjevanja vlog uporabnikom.

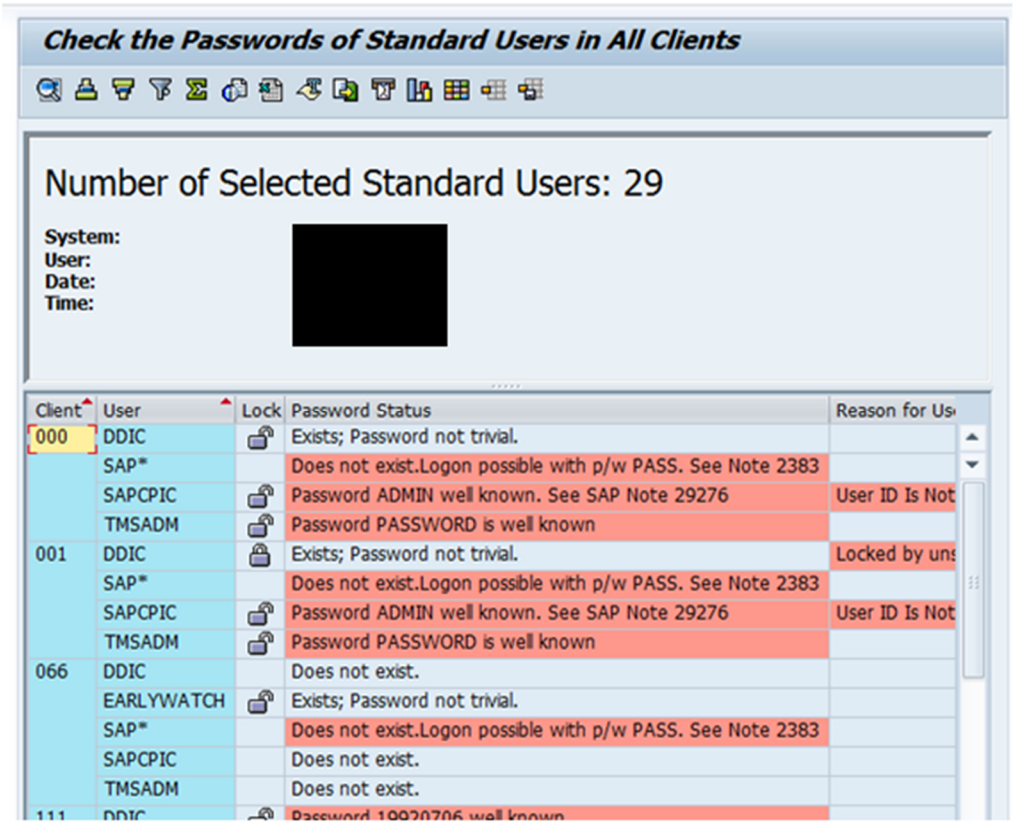
Hkrati s tem podjetju ABC priporočamo, da vzpostavi politiko upravljanja s SAP dostopi, ki bo določala način kreiranja uporabniških vlog ter postopek dodeljevanja, spreminjanja in odvzemanja SAP dostopov. Upošteva naj se načelo minimizacije in načelo ločevanja uporabniških vlog.

Politika varovanja informacij, ki jo je podjetje ABC pripravilo za potrebe certifikacije ISO/IEC 27001:2013 naj jasno opredeljuje pravilno rokovanje z dostopi ter gesli do informacijskih sistemov in vključuje primere nedovoljenih praks.

3.7 Standardni uporabniki v SAP sistemu

V produkcijskem okolju SAP smo izvedli poročilo RSUSR003, s katerim smo pridobili nastavitve za gesla za standardne uporabnike v vseh klientih. Gre za predvgrajene privilegirane račune v SAPu. Rezultati izvedenega poročila RSUSR003 so na sliki 2.

Slika 2: Kršitve varnostnih nastavitev za gesla



Vir: Lastni prikaz.

UGOTOVITEV:

Na podlagi izpisa poročila predstavljamo naslednje ugotovitve:

- **Uporabnik SAP*** je t.i. inicialni (prvotni) uporabnik, ki je kreiran ob namestitvi sistema in ima avtomatično šibkejše varnostne nastavitve. Uporabnik in pripadajoče geslo je splošno poznano. Ob prvotni namestitvi ima uporabnik pooblastila super uporabnika (angl. super user). Uporabnik se uporablja za začetne nastavitve sistemskega dostopa administratorjem. Glede na nastavitve v podjetju ABC lahko v SAP sistem dostopa kdorkoli z uporabo uporabnika SAP* in gesla PASS.
- **Uporabnik SAPCPIC** je uporabniški račun namenjen administrativnim opravilom v pripadajočih programih s standardnim geslom »ADMIN«. Pogosto ga uporabljajo razvijalci Ker je to uporabniški (in ne servisni) račun, obstaja tveganje, da lahko katerakoli oseba dostopa do SAP sistema s temi dostopnimi podatki.
- **Uporabnik TMSADM** omogoča distribucijo osnovne konfiguracije v vse SAP sisteme. Tudi ta uporabnik ima splošno znano standardno geslo »PASSWORD«, kar omogoča dostop katerikoli osebi do SAPa z uporabo teh dostopnih podatkov.
- **Uporabnik DDIC** obstaja v vseh SAP sistemih, uporablja se za administrativne namene programske opreme in ima splošno poznano geslo ter pooblastila super uporabnika. V podjetju ABC so spremenili geslo za uporabnika DDIC in ni splošno znano, zato ne predstavlja varnostnih tveganj.

● **– VISOKO TVEGANJE**

Ker gesla za uporabnike SAP*, SAPCPIC in TMSADM niso bila spremenjena in so splošno znana v javnosti, obstaja visoko tveganje, da do informacijskega sistema dostopajo nepooblaščeni posamezniki z uporabo standardnih uporabnikov.

PRIPOROČILO 8:

Podjetju ABC priporočamo takojšnjo menjavo gesel za uporabnike SAP*, SAPCPIC in TMSADM. Če standardni uporabniki niso v uporabi, priporočamo tudi preklic vseh avtorizacij in zaklenitev (lock) uporabnikov v sistemu.

3.8 Varnostne nastavitve za gesla v SAPu

Z uporabo poročila RSPARAM smo pridobili varnostne nastavitve za gesla v SAPu in jih primerjali s priporočenimi nastavitvami. Primerjavo po posamezni nastavitvi, za katero smo opazili odstopanje od dobrih praks informacijske varnosti, predstavljamo v tabeli 2.

Tabela 2: Varnostne nastavitve v SAPu

NASTAVITEV	NASTAVLJENA VREDNOST	PRIPOROČENA VREDNOST[6]	OPIS
1 login/min_password_lng	3	8[7]	Najkrajša dolžina gesla.
2 login/password_expiration_time	0	60	Število dni do menjave gesla. Po poteku časa mora uporabnik zamenjati geslo. Vrednost 0 pomeni, da ni omejitve in geslo nikoli ne poteče.
3 login/fails_to_session_end	0	3	Število poskusov vnosa napačnega gesla preden sistem onemogoči prijavo. Vrednost 0 pomeni neomejeno število poskusov.
4 login/fails_to_user_lock	0	5	Število poskusov vnosa napačnega gesla preden sistem zaklene uporabnika in onemogoči nadaljnje poskuse prijave. Vrednost 0 pomeni neomejeno število poskusov.
5 rdisp/gui_auto_logout	0	1800 sec	Število sekund nedejavnosti seje, preden sistem samodejno odjavi uporabnika. Vrednost 0 pomeni, da sistem ne odjavlja samodejno ob neaktivnosti uporabnika.
9 auth/rfc_authority_check	0	1	Dovoljenje za oddaljen priklic funkcij znotraj programov ABAP.
11 login/no_automatic_user_sap*	0	1	Onemogoči posebne lastnosti za uporabnika SAP*, ko je ta parameter nastavljen na vrednost, večjo od nič. Vrednost parametra 0 omogoča prijave uporabnika SAP* z uporabo privzetega gesla in neomejenimi pravicami dostopa do sistema.

Vir: Lastni prikaz.

[6] Povzeto po priporočenih nastavitvah na strani https://blogs.sap.com/2013/08/30/important-security-parameters-helpful-for-basis/.

[7] Vir: https://davintechgroup.com/toolkit/password-requirements-gdpr-iso-27001-27002-pci-dss-nist-800-53/.

UGOTOVITEV:

Na podlagi nastavljenih vrednosti varnostnih nastavitev predstavljamo naslednje ugotovitve:

1. omogočena so prekratka gesla (najkrajša dolžina gesla je 3 mesta, priporočena dolžina je 8 mest);
2. nastavitev v SAPu omogoča, da gesla ne potečejo in jih ni potrebno menjati;
3. sistem ne omejuje števila poskusov vnosa napačnega gesla;
4. sistem ne zaklene uporabnika in ne omeji nadaljnjih poskusov prijave v primeru večkratnega vnosa napačnega gesla;
5. ob nedejavnosti uporabnika sistem samodejno ne odjavi uporabnika;
6. sistem omogoča prijavo uporabnika SAP* z uporabo privzetega gesla in neomejenimi pravicami dostopa do sistema.

● **– VISOKO TVEGANJE**

Šibke nastavitve varnostnih parametrov za gesla predstavljajo povečano tveganje nepooblaščenih dostopov in zlorab sistema. Trenutne nastavitve varnostnih parametrov za gesla omogočajo, da uporabnik izbere kratko, hitro ugotovljivo geslo, ki ga ni potrebno redno menjati, in hkrati omogočajo neomejeno število poskusov prijave. To povečuje tveganje, da bodo gesla ugotovili in uporabili nepooblaščeni uporabniki, ki lahko izkoristijo dostop tudi za odtujitev sredstev ali informacij podjetja.

PRIPOROČILO 9:

Podjetju ABC priporočamo, da ponovno preveri vse nastavitve kontrolnih parametrov, ki se nanašajo na gesla v sistemu SAP.

Priporočamo tudi, da se izdela interni pravilnik, ki predpisuje politiko gesel, vključno z omejitvami glede dolžine in kompleksnosti gesel ter števila neuspešnih poskusov vnosa gesla, zaklepanje uporabnika po določenem številu neuspešnih poskusov vnosa gesla, samodejno odjavo uporabnika po določenem časovnem intervalu neaktivnosti in periodiko spreminjanja gesel. Parametri, določeni z internim pravilnikom, naj se implementirajo v informacijske sisteme. S politiko naj se evidentno seznanijo vsi zaposleni, ki uporabljajo informacijske storitve podjetja ABC.

3.9 Aktivni uporabniki SAPa

Na podlagi rezultatov izvedenega poročila RSUSR200, s katerim smo pridobili seznam uporabnikov glede na datum zadnje prijave in spremembe gesla, smo ugotovili, da:

- je v sistemu SAP aktivnih 854 uporabnikov,
- se 11 uporabnikov ni nikoli prijavilo v informacijski sistem SAP,
- se 219 uporabnikov v informacijski sistem SAP ni prijavilo več kot 120 dni.

UGOTOVITEV:

Podjetje ABC ima v povprečju 400 zaposlenih in 854 aktivnih SAP uporabnikov, od katerih se 219 uporabnikov ni prijavilo v SAP v zadnjih 4 mesecih, 11 uporabnikov pa se v SAP ni prijavilo nikoli. Preverili smo obstoječe uporabnike s seznamom aktivnih zaposlenih in ugotovili, da ima dostope do sistema SAP še vedno 186 nekdanjih zaposlenih ter 33 zunanjih sodelavcev, katerim so potekle

pogodbe o sodelovanju. Poleg tega je bil uporabnik v SAPu kreiran tudi za 11 zaposlenih na delovnih mestih, ki pri delu ne uporabljajo SAPa (9 čistilk in 2 vzdrževalca objekta). Posledica prevelikega števila SAP uporabnikov je povečan strošek nakupa in vzdrževanja SAP licenc, ki se zakupijo za vsakega uporabnika.

Vzrok za tako visoko število aktivnih uporabnikov je v pomanjkljivih in nejasnih pravilih dodeljevanja, odvzemanja in spreminjanja uporabniških dostopov ter odsotnosti procesa rednega pregledovanja dodeljenih dostopov in ukinjanja neaktivnih uporabnikov.

Standard ISO/IEC 27002:2013 v kontroli A.9.2.6. Preklic ali prilagoditev pravic dostopa opredeljuje, da se morajo pravice dostopa vseh zaposlenih in zunanjih uporabnikov do informacij in naprav za obdelavo informacij odstraniti po prekinitvi njihove zaposlitve, pogodbe ali dogovora oziroma se prilagoditi spremembam.

– VISOKO TVEGANJE

Nenadzorovano in nekontrolirano kreiranje uporabnikov povečuje tveganje, da imajo nepooblaščeni zaposleni dostop do sistemov in informacij, ki jih pri delu ne potrebujejo. Če je vsako kreirano uporabniško ime ločena SAP licenca, potem je strošek z naslova nakupa licenc vsaj podvojen. Prav tako pomanjkanje postopka odstranjevanja dostopov neaktivnim uporabnikom in zaposlenim, ki so podjetje že zapustili, povečuje tveganje nepotrebnega in prevelikega števila uporabnikov.

PRIPOROČILO 10:

Podjetju ABC priporočamo, da na podlagi usklajenih obstoječih poslovnih procesov ter opredeljenega lastništva nad procesi in podatki (glej Priporočilo 2) preveri potrebo po dostopu do SAPa za vsakega zaposlenega in odstrani oziroma zaklene podvojene in nepotrebne uporabnike.

Vpeljavo internega pravilnika, ki opredeljuje postopke dodeljevanja, odvzemanja in spreminjanja uporabniških dostopov, smo podali v priporočilu 1 (poglavje 3.1).

3.10 Ugotovljena kršitev in prepoznano tveganje prevare

UGOTOVITEV:

Med pregledom sistema in analizo podatkov smo ugotovili, da je imel uporabnik LEPA_BRENA dodeljeno vlogo SAP_ALL[8]. Kreiral je novega uporabnika JAKA_RACMAN. Ta je v obdobju od 1. 1. 2020 do vključno 31. 12. 2020 v saldokontih dobaviteljev kreiral 21 faktur za storitve masažnega salona Happy place v skupni višini 17.532 evrov. Uporabnik LEPA_BRENA je potrdil izplačilo faktur in te so se uvrstile med redna plačila dobaviteljem in so bile tudi plačane. Uporabnik LEPA_BRENA je uporabnika JAKA_RACMAN zbrisal. Prav tako nismo našli dnevniških zapisov v tabelah, v katerih bi morali biti evidenčni zapisi o kreaciji uporabnika, izbrisu uporabnika in izvedenih transakcijah uporabnika.

[8] Kritičnost dodeljene vloge SAP_ALL in s tem povezana tveganja so predstavljena v poglavju 3.3.

– VISOKO TVEGANJE

Izvedene aktivnosti upravljanja z dostopi nakazujejo na kršitve več načel informacijske varnosti in predstavljajo notranjo grožnjo, saj je uporabnik zlorabil svoj dostop in s tem negativno vplival in škodoval podjetju ABC:

- kreirano uporabniško ime ni bilo imensko, torej ga ni možno povezati s konkretnim uporabnikom in ugotoviti, kdo je s tem uporabniškim dostopom upravljal (glej točko 3.4);
- uporabnik je imel dodeljeno vlogo SAP_ALL, ki omogoča neomejen dostop do vseh podatkov in procesov, s čimer niso upoštevana načela dobre prakse informacijske varnosti Standarda ISO/IEC 27002:2013 (glej točko 3.3);
- uporabnik je z vlogo SAP_ALL kreiral navidezne uporabnike in dodajal vloge, s katerimi so se izvajali fiktivni poslovni procesi, z namenom poneverjanja obveznosti dobaviteljem in plačevanja le-teh;
- uporabnik je imel zaradi neomejenega dostopa možnost spreminjanja nastavitev spremljanja in zapisovanja revizijske sledi, s čimer je lahko zabrisal revizijske sledi in s tem prikril izvedeno kršitev.

Okvir strokovnega ravnanja za dajanje zagotovil/revidiranje informacijskih sistemov (ITAF, 3. izdaja) v izvedbenem standardu 1207 napotuje revizorja informacijskih sistemov k pravočasnem sporočanju o vsaki ugotovljeni ali pridobljeni informaciji, da lahko obstaja pomembna nepravilnost ali nezakonito dejanje. V smernici 2207 Nepravilnosti in nezakonita dejanja ta okvir podrobneje opredeljuje ravnanje v primeru ugotovljene nepravilnosti oziroma nezakonitega ravnanja in sicer: »*Ugotovitev, da je določeno dejanje nezakonito, naj na splošno temelji na nasvetu poučenega strokovnjaka, ki ima pravno izobrazbo, ali pa je treba počakati na končno odločitev sodišča. Strokovnjaki naj predvsem upoštevajo učinek ali morebitni učinek nepravilnega ravnanja ne glede na to, ali gre za sum ali dokaz nezakonitega dejanja*«. V nadaljevanju smernice pravijo, da je revizor informacijskih sistemov dolžan poročati o obstoju nepravilnosti ali nezakonitega dejanja, kadar naleti na te informacije. Specifično naj revizor informacijskih sistemov »*obvesti poslovodstvo in pristojne za upravljanje, kadar prepoznajo stanje ali razmere povečanega tveganja za morebitno nepravilnost ali nezakonito dejanje, pa čeprav to še ni odkrito*«.
O odkritju nepravilnosti in nezakonitih dejanj mora revizor informacijskih sistemov »*(pisno ali ustno) pravočasno obvestiti ustrezne ljudi v podjetju. Obvestilo mora biti naslovljeno na raven vodenja, ki je nadrejena tisti, za katero obstaja sum pojava nepravilnosti. Poleg tega je treba o nepravilnostih in nezakonitih dejanjih poročati pristojnim za upravljanje v podjetju, kot so nadzorni svet ali upravni odbor, skrbniki, revizijska komisija ali tem enakovreden organ*«.

Skladno s smernicami smo o predstavljenem kritičnem tveganju obvestili poslovodstvo podjetja ABC že med samim izvajanjem pregleda in priporočili, da se vse ugotovljene informacije predajo odgovorni osebi za preiskovanje prevar oziroma vključijo zunanje organe, ki se ukvarjajo s preiskovanjem nepravilnosti oziroma nezakonitih dejanj. Ker zaradi zabrisanih revizijskih sledi ni bilo možno ugotoviti, na kateri ravni je zaposlen uporabnik, ki je izvedel ugotovljene nepravilnosti, niti če je uporabnik zaposleni podjetja ABC, smo s seznanitvijo celotnega poslovodstva zagotovili, da je obveščena najvišja raven vodenja in da je hkrati obveščenih več predstavnikov poslovodstva, v kolikor bi bil v sumljivo

aktivnost vpleten član poslovodstva. Hkrati smo o tem obvestili tudi zunanjega revizorja računovodskih izkazov, ZR d. o. o., kot napotuje ITAF v smernici 2207.

PRIPOROČILO 11:

Podjetju ABC priporočamo, da v formalnem internem pravilniku (glej Priporočilo 1) vzpostavi postopek upravljanja uporabniških dostopov, ki vključuje redno periodično pregledovanje dodeljenih uporabniških dostopov in odstranjevanje dostopov, ki ne upoštevajo načel minimizacije in ločevanja vlog.

Da bi zagotovili razmejitev odgovornosti SAP administratorjev priporočamo ločevanje administratorskih funkcij v SAPu:

- razmejitev odgovornosti za kreiranje in vzdrževanje SAP vlog/profilov, dodeljevanje SAP vlog/profilov ter kreiranje in vzdrževanje SAP uporabnikov;
- omejitev dostopa SAP administratorjem do kreiranja in vzdrževanja kadrovskih matičnih podatkov.

3.11 Dodatne ugotovitve, ki se ne navezujejo na predmet pregleda

Glede na navedbe revidiranca so v letu 2019 pridobili certifikat za sistem upravljanja varovanja informacij (ISO/IEC 27001:2013) za celotno podjetje, ki ga je izdalo podjetje Everthing4You iz Moldavije. Kljub temu, da gre za mednarodni standard, Uredba ES št. 765/2008 Evropskega parlamenta in sveta (sprejeta dne 9. 7. 2008) določa, da »vsaka država članica imenuje enotni nacionalni akreditacijski organ, ki organom za ugotavljanje skladnosti izda Certifikat o akreditaciji«, podjetje Everthing4You ni na seznamu akreditiranih organov Slovenske akreditacije (www.slo-akreditacija.si).

Pridobitev certifikata ISO/IEC 27001:2013 naj bi med drugim zagotavljalo skladnost podjetja z varstvom podatkov, zasebnostjo in učinkovitim poslovnim tveganjem. Države članice Evropske unije (angl: European Union, v nadaljevanju: EU) so zavezane k bolj striktnim zahtevam varovanja informacij, kot veljajo v drugih (ne-EU) državah, kot je na primer Splošna uredba o varstvu podatkov[9]. Pridobitev certifikata v državi, ki ni članica EU, ne zagotavlja skladnosti z zahtevami informacijske varnosti, ki veljajo v EU.

Prav tako podjetje ABC po preteku enega leta od pridobitve certifikata ni opravilo kontrolne presoje. Ker v letu 2022 minevajo 3 leta od pridobitve certifikata, je potrebno do konca leta izvesti postopek recertifikacije. Podjetju ABC svetujemo, da postopek recertifikacije izvede pri akreditiranem organu Slovenske akreditacije in od recertifikacije naprej poskrbi za izvedbo rednih letnih kontrolnih presoj.

[9] GDPR (angl. General Data Protection Regulation), Uredba (EU) 2016/679, sprejeta 27. 4. 2016.

4 MNENJE

V skladu z listino o poslu smo za podjetje ABC izvedli pregled dodeljevanja, odvzemanja in spreminjanja uporabniških dostopov v SAP sistem v podjetju ABC za obdobje od 1. 1. 2020 do 31. 12. 2020, in poročanje o trenutnem stanju delovanja in učinkovitosti notranjih kontrol na področju dodeljevanja, odvzemanja in spreminjanja dostopov v SAP sistem.

Pri pregledu delovanja in učinkovitosti notranjih kontrol na področju dodeljevanja, odvzemanja in spreminjanja dostopov v SAP sistem smo, glede na sodila dogovorjena s podjetjem ABC v Listini o poslu, ugotovili več nepravilnosti in tveganj, ki jih podajamo v nadaljevanju.

COBIT 2019 kontrolni cilj DSS05.04 Upravljanje uporabniške identitete in logičnega dostopa podaja ključna vodila kako zagotoviti, da imajo vsi uporabniki dodeljene pravice dostopa do informacij v skladu s poslovnimi potrebami. Predpisane aktivnosti na najnižjem zrelostnem modelu (Capability level 2) so:

- vzdrževanje uporabniških dostopnih pravic v skladu s poslovno funkcijo, potrebami procesov in varnostnimi politikami;
- uskladitev upravljanja identitet in dostopnih pravic z opredeljenimi vlogami in odgovornostmi, ki temeljijo na načelih najmanj privilegijev (angl. least-privilege), potreba po vedenju (angl. need-to-know) in kar uporabnik potrebuje (angl. need-to-have).

Pri pregledu smo ugotovili:

- Podjetje ABC nima vpeljanega lastništva nad procesi in podatki, prav tako nima opredeljenih odgovornosti in pooblastil, na podlagi katerih bi se lahko vzpostavile učinkovite in delujoče notranje kontrole.
- Postopki dodeljevanja, odvzemanja in spreminjanja uporabniških dostopov (imen) do informacijskih sistemov podjetja ABC niso zapisani v formalnem dokumentu. Dostopi se dodajajo na podlagi elektronskih sporočil ali telefonskih klicev. Ni opredeljenega lastništva nad procesi in podatki.
- Podjetje ABC ni oblikovalo svojim potrebam prilagojenih tipov uporabnikov in uporabniških vlog. Tudi 3 leta po končani uvedbi informacijskega sistema SAP v produkcijsko delovanje, uporabniški dostopi še vedno ne ustrezajo potrebam poslovnih procesov.
- Med ažurnimi aktivnimi uporabniki smo prepoznali nekatere neimenske (generične) uporabnike.

Standard ISO/IEC 27001:2013 v poglavju A.6. Organizacija informacijske varnosti, A.6.1. Notranja organizacija, A.6.1.2. Razmejitev dolžnosti opredeljuje kontrolo: »Nasprotujoče si naloge in področja odgovornosti se morajo razmejiti, da se zmanjšajo možnosti za nepooblaščeno ali nenamerno spreminjanje ali zlorabo sredstev organizacije«.

Pri pregledu smo ugotovili:

- SAP vloge, ki so bile dodeljene posameznim uporabnikom, niso pregledno povezane z delovnimi nalogami, ki jih ti opravljajo;
- uporabniški dostopi ne ustrezajo potrebam poslovnih procesov, zato si uporabniki za nemoteno izvajanje nalog med seboj posojajo uporabniška imena in gesla.

Standard ISO/IEC 27001:2013 v poglavju A.9. Nadzor dostopa, A.9.2. Upravljanje uporabniškega dostopa, A.9.2.3. Upravljanje privilegiranih pravic dostopa opredeljuje kontrolo: »Dodelitev in uporaba privilegiranih pravic dostopa se morata omejiti in nadzorovati«.
Pri pregledu smo ugotovili:

- Svetovalci podjetja Kr-eni so za namene oddaljene administracije ustvarili uporabnika »Kr_Eni« s pravicami SAP_ALL. Po implementaciji so strokovnjaki podjetja Kr-eni zadržali pravice do produkcijskih modulov SAP za hitrejše in učinkovitejšo podporo na daljavo ter za vsakoletno pomoč pri vzpostavitvi novega finančnega leta.
- Dostopna gesla za predvgrajene privilegirane račune v SAPu so splošno znana v javnosti, kar pomeni, da lahko vsak, ki te dostopne podatke pozna, nenadzorovano dostopa do SAPa in ni mogoče nadzorovati, kdo te dostope uporablja.
- Neimenski uporabnik LEPA_BRENA je imel dodeljeno vlogo SAP_ALL, s katero je zlorabil svoj dostop in s tem oškodoval podjetje ABC.

Standard ISO/IEC 27001:2013 v poglavju A.9. Nadzor dostopa, A.9.2. Upravljanje uporabniškega dostopa, A.9.2.5. Pregled uporabniških pravic dostopa opredeljuje kontrolo »Lastniki sredstev morajo pregledovati uporabniške pravice dostopa v rednih časovnih presledkih«.
Pri pregledu smo ugotovili:

- Na podlagi poročila RSUSR005 smo prepoznali 176 uporabnikov, ki imajo dodeljene kritične avtorizacije. Za tako veliko število uporabnikov nismo uspeli pridobiti ustrezne razlage ne v oddelku IT ne pri poslovnih uporabnikih, kar kaže na pomanjkanje rednega pregleda dodeljenih dostopov.

Standard ISO/IEC 27001:2013 v poglavju A.9. Nadzor dostopa, A.9.2. Upravljanje uporabniškega dostopa, A.9.2.6. Preklic ali prilagoditev pravic dostopa opredeljuje kontrolo »Pravice dostopa vseh zaposlenih in zunanjih uporabnikov do informacij in naprav za obdelavo informacij se morajo odstraniti po prekinitvi njihove zaposlitve, pogodbe ali dogovora oziroma se prilagoditi spremembam«.
Pri pregledu smo ugotovili:

- Pri 400 zaposlenih v podjetju ABC je v sistemu SAP aktivnih 854 uporabnikov, 219 od teh se ni prijavilo v sistem v zadnjih 4 mesecih, 11 uporabnikov se ni nikoli prijavilo v sistem. To nakazuje, da se uporabniški dostopi ne odstranjujejo po prekinitvi zaposlitve oziroma po prenehanju potrebe po dostopu.

Glede na predstavljene ugotovitve in tveganja ugotavljamo, da trenutno vzpostavljene notranje kontrole in upravljanje tveganj na področju dodeljevanja, odvzemanja in spreminjanja dostopov v SAP sistem v podjetju ABC pomembno odstopajo od sodil, ki so bila uporabljena v pregledu, in da notranje kontrole ali niso vzpostavljene ali pa ne delujejo in niso učinkovite.

5 ZAKLJUČEK

Z listino o poslu sta se podjetje ABC in izvajalec Simona Kotar dogovorila o izvedbi pregleda dodeljevanja, odvzemanja in spreminjanja uporabniških dostopov v SAP sistem v podjetju ABC za obdobje od 1. 1. 2020 do 31. 12. 2020, in za poročanje o trenutnem stanju delovanja in učinkovitosti notranjih kontrol na področju dodeljevanja, odvzemanja in spreminjanja dostopov v SAP sistem.

Cilj opravljenega pregleda je bil podati neodvisno mnenje glede delovanja notranjih kontrol procesa dodeljevanja, odvzemanja in spreminjanja uporabniških dostopov v SAP sistem v dogovorjenem obdobju, pri čemer smo se osredotočili na naslednja tveganja:

- tveganje, da imajo uporabniki dostopne pravice do sistema in informacij, ki jih pri delu ne potrebujejo;
- tveganje, da imajo nepooblaščeni zaposleni dostop do informacij zaupnega značaja;
- tveganje, da imajo nepooblaščeni zaposleni dostop do procesov ali nastavitev, ki lahko kritično vplivajo na poslovni proces;
- tveganje, da lahko zaradi preveč široko dodeljenih dostopov en zaposleni upravlja celoten proces.

Na podlagi ugotovitev in prepoznanih tveganj smo ugotovili, da trenutno vzpostavljene notranje kontrole in upravljanje tveganj na področju dodeljevanja, odvzemanja in spreminjanja dostopov v SAP sistem v podjetju ABC, **pomembno odstopajo od sodil**, ki so bila uporabljena v pregledu, **notranje kontrole niso vzpostavljene oziroma ne delujejo in niso učinkovite**. Vsa ugotovljena odstopanja posredno ali neposredno izhajajo iz ključne ugotovitve, da **podjetje ABC nima vpeljanega lastništva nad procesi in podatki, prav tako nima opredeljenih odgovornosti in pooblastil**, na podlagi katerih bi se lahko vzpostavile učinkovite in delujoče notranje kontrole. Podana priporočila za odpravo pomanjkljivosti bodo prispevala k zmanjšanju prepoznanih tveganj in okrepila varnost sredstev podjetja ABC. Poslovodstvu podjetja ABC svetujemo, da v roku enega leta izvede porevizijski pregled in ugotovi stanje realizacije priporočil.

6 PRILOGE

6.1 Listina o poslu

Podjetje ABC, Ulica 15, 1000 Ljubljana, DŠ: 12345678, ki ga zastopa Ime Priimek, generalni direktor (v nadaljevanju: »**naročnik**«)
in
Simona Kotar, Ulica 3, 3000 Celje (v nadaljevanju: »**izvajalec**«)
Sklepata

LISTINO O POSLU št. 1/2021

1. člen
Področje in predmet posla

Predmet listine je izvedba pregleda dodeljevanja, odvzemanja in spreminjanja uporabniških dostopov v SAP sistem v podjetju ABC za obdobje od 1. 1. 2020 do 31. 12. 2020 in poročanje o trenutnem stanju delovanja in učinkovitosti notranjih kontrol na področju dodeljevanja, odvzemanja in spreminjanja dostopov v SAP sistem.

2. člen
Obseg posla

Izvajalec bo opravil pregled s ciljem izraziti neodvisno mnenje glede delovanja notranjih kontrol procesa dodeljevanja, odvzemanja in spreminjanja uporabniških dostopov v SAP sistem v dogovorjenem obdobju, pri čemer se bo osredotočil na naslednja tveganja:

- tveganje, da imajo uporabniki dostopne pravice do sistema in informacij, ki jih pri delu ne potrebujejo;
- tveganje, da imajo nepooblaščeni zaposleni dostop do informacij zaupnega značaja;
- tveganje, da imajo nepooblaščeni zaposleni dostop do procesov ali nastavitev, ki lahko kritično vplivajo na poslovni proces;
- tveganje, da lahko zaradi preveč široko dodeljenih dostopov en zaposleni upravlja celoten proces.

3. člen
Cilj posla

Cilj pregleda je izraziti neodvisno mnenje glede delovanja notranjih kontrol dodeljevanja, odvzemanja in spreminjanja uporabniških dostopov v SAP sistem v dogovorjenem obdobju. Da bi dosegli zastavljeni cilj bomo:

- preverili skladnost postopka dodeljevanja uporabniških dostopov z internimi pravilniki in dobrimi praksami;
- pregledali procesa vzdrževanja in rednega preverjanja matrike vlog;
- pregledali izvajanja procesa razmejitve odgovornosti (SOD[10]).

[10] SOD – razmejitev odgovornosti (angl. segregation of duties)

Pregled vključuje izvajanje postopkov za pridobitev revizijskih dokazov o uspešnosti delovanja naročnikovih notranjih kontrol procesa dodeljevanja, odvzemanja in spreminjanja uporabniških dostopov v SAP sistem. Izbrani postopki so odvisni od revizorjeve presoje.

4. člen

Sodila za presojo

Izvajalec bo pri načrtovanju pregleda kot smernice in vodila smiselno uporabil:

- COBIT 2019 kontrolne cilje DSS05.04 Upravljanje uporabniške identitete in logičnega dostopa (Manage user identity and logical access);
- ISO/IEC 27002:2013 izbrane kontrolne cilje in kontrole znotraj A.9 Access control;
- NIST Okvir za izboljšanje kritične infrastrukture kibernetske varnosti verzija 1.1. – kontrole v kategoriji PR.AC-1 in PR.AC-4;
- interne pravilnike s področja varovanja informacij.

Zgoraj naštete smernice in vodila so podlaga za oblikovanje sodil, ki jih bo v procesu načrtovanja posla izvajalec dorekel in potrdil z naročnikom.

5. člen

Neodvisnost

Neodvisnost je osvobojenost od okoliščin, ki ogrožajo objektivnost in zaznano objektivnost. Izvajalec zagotavlja, da z opravljanjem posla za naročnika ni v navzkrižju interesov in v nasprotju z zakonskimi določili. V zadnjih dveh letih izvajalec ni sodeloval na področju izboljšanja delovanja notranjih kontrol in procesov, ki so predmet pregleda, in s poslovodstvom ali vodstvom področja pregleda naročnika ni sorodstveno povezan.

Med izvajanjem posla se bo izvajalec izogibal nerevizijskim vlogam v pobudah, ki niso povezane z revidiranjem in zahtevajo prevzem upravljavskih zadolžitev.

V kolikor bi bila med izvajanjem posla zaznana ali dejansko oslabljena neodvisnost, bo izvajalec to nemudoma razkril naročniku in se z njim posvetoval. Če se bo izvajanje posla kljub oslabitvi neodvisnosti nadaljevalo, bo izvajalec v poročilu vključil vse informacije za razumevanje narave morebitne oslabitve.

6. člen

Standardne določbe

Pregled se bo izvedel skladno s Hierarhijo pravil revidiranja informacijskih sistemov (Uradni list RS, št. 40/2011 z dne 27. 5. 2011). Ta hierarhija od izvajalca zahteva, da razen zakonskih podlag pri svojem delu upošteva standarde, smernice ter orodja in tehnike za strokovnjake revidiranja, kontrol in dajanja zagotovil na področju IT (ITAF: Okvir strokovnega ravnanja za dajanje zagotovil/revidiranje IS, ki ga izdaja ISACA). Standardi od izvajalca zahtevajo izpolnjevanje etičnih zahtev ter načrtovanje in izvedbo pregleda za pridobitev sprejemljivega zagotovila, da notranje kontrole naročnika nimajo nobenih bistvenih pomanjkljivosti glede na naročnikovo poslovanje, okolje, strokovne standarde in dobro prakso.

Pri pripravi ocene tveganj bo izvajalec proučil upravljanje in obvladovanje tveganj na revidiranem področju z namenom, da bi izrazil neodvisno in nepristransko mnenje.

Izvajalec se zavezuje, da bo pri obdelavi osebnih podatkov ravnal skladno z Zakonom o varstvu osebnih podatkov (Uradni list RS, št. 86/04 z dne 5. 8. 2004) ter skladno z veljavnimi pravili naročnika o varstvu osebnih podatkov. V procesu obdelave bo izvajalec upošteval ustrezne tehnične in organizacijske ukrepe, ki preprečujejo nedovoljeno in nezakonito obdelavo osebnih podatkov, kot tudi ukrepe, ki preprečujejo naključno izgubo, uničenje ali spremembo osebnih podatkov.

7. člen

Omejitve

V pregled niso zajete ostale informacijske rešitve naročnika in tehnološka infrastruktura, na kateri delujejo.

Zaradi naravnih omejitev pregleda skupaj z naravnimi omejitvami notranjega kontroliranja se ni mogoče izogniti tveganju, da se kakšnih pomembnih pomanjkljivosti v zasnovi in delovanju notranjih kontrol morda ne bo odkrilo, kljub temu, da bo pregled pravilno načrtovan in opravljen v skladu s Standardi, smernicami ter orodji in tehnikami za strokovnjake revidiranja, kontrol in dajanja zagotovil na področju IT.

8. člen

Odgovornost poslovodstva in notranjega revizorja

Dogovorjeni pregled bo opravljen ob predpostavki, da poslovodstvo sprejema in pozna svojo odgovornost za takšno notranje kontroliranje, kot ga poslovodstvo opredeli kot potrebno, da bodo doseženi kontrolni cilji, ter da izvajalcu zagotovi:

- dostop do vseh informacij, za katere poslovodstvo ve, da so pomembne na revidiranem področju,
- dodatne informacije, ki jih izvajalec utegne zahtevati od poslovodstva za namen pregleda,
- neomejen dostop do vseh oseb v organizaciji, katere določi izvajalec, da mora od njih pridobiti revizijske dokaze.

Kot del poteka pregleda bo izvajalec od odgovorne osebe revizijskega področja zahteval pisno potrditev predstavitev, ki so bile podane v zvezi s pregledom.

Dodatno se pričakuje, da bo naročnik izvajalcu omogočil dostop do ugotovitev in poročil notranje revizije iz predmetnega področja pregleda ter poročil in delovnega gradiva morebitnih prejšnjih revizij dodeljevanja uporabniških dostopov.

Vsa dokumentacija, predstavitve in drugi podatki, ki jih bo izvajalec prejel pri izvajanju pregleda, bodo obravnavani kot poslovna skrivnost. Delovno gradivo v elektronski obliki bo izvajalec predal naročniku najkasneje v štirinajstih dneh po potrditvi prejema končnega poročila.

9. člen

Poročanje

O vseh pomembnih ugotovitvah, do katerih bo izvajalec prišel med izvajanjem posla, bo poročal v poročilih. V primeru kritičnih ugotovitev mora izvajalec naročnika seznaniti takoj, ko jih prepozna.

S strani naročnika bodo osnutek poročila prejeli:
- vodja Sektorja za informatiko podjetja ABC,
- vodja Informacijske varnosti podjetja ABC.

Končno poročilo bodo prejeli:
- Poslovodstvo podjetja ABC,
- Vodja Sektorja za informatiko podjetja ABC,
- Vodja Informacijske varnosti podjetja ABC.

Prejemniki povzetka poročila bodo:
- Poslovodstvo podjetja ABC,
- Revizijska komisija nadzornega sveta podjetja ABC.

Tako osnutek kot končno poročilo in povzetek bodo poslani elektronsko.

10. člen

Izvedba posla in cena

Pregled bo s strani izvajalca izvedla Simona Kotar, vključena v izobraževanje za pridobitev strokovnega naziva preizkušeni revizor informacijskih sistemov.

Datum začetka izvajanja nalog je 1. 4. 2021. Rok za izdelavo osnutka poročila je 30. 4. 2021. Datum izdaje končnega poročila je odvisen od zaključnega sestanka med izvajalcem in naročnikom ter morebitnih dodatnih dokaznih gradivih, ki bi jih naročnik predstavil naknadno. Pregled bo predvideno obsegal 20 revizor dni, pri čemer 1 revizor dan vključuje 8 ur.

Cena opravljene storitve se določi na podlagi porabljenih ur in vrednosti XX EUR na uro brez DDV. Cena urne postavke vsebuje vse materialne, potne in druge stroške izvajalca.

Naročnik se zavezuje, da bo pogodbeno ceno poravnal na osnovi izstavljenega računa s priloženo specifikacijo opravljenega dela na transakcijski račun izvajalca št. SI56 xxxx xxxx xxxx xxx, odprt pri UniCredit banki Slovenija. V primeru zamude pri plačilu lahko izvajalec obračuna zakonske zamudne obresti.

11. člen

Okoliščine povečanega obsega dela in višja sila

Izvajalec ni odgovoren za delno ali celotno neizpolnjevanje pogodbenih obveznosti, če je to posledica višje sile. Kot višja sila se razumejo vse okoliščine izjemnega značaja, ki so se pojavile po sklenitvi pogodbe in jih sodna praksa priznava za višjo silo. Če je izvedba storitve delno ali v celoti motena

oziroma preprečena, je izvajalec o tem dolžan nemudoma obvestiti naročnika. Prav tako ga je dolžan sproti obveščati o prenehanju takih okoliščin.

12.člen

Končne določbe

Pogodbeni stranki bosta morebitne medsebojne spore reševali sporazumno, če pa to ne bo mogoče, bo za reševanje njunih medsebojnih sporov pristojno sodišče v Ljubljani.

Naročnik si pridružuje pravico, da v primeru neustrezne kakovosti izvedenih storitev predčasno prekine pogodbo.

Listina o poslu je sestavljena v dveh izvodih, od katerih prejme vsaka pogodbena stranka po en izvod.

S podpisom listine naročnik posla potrjuje dogovore in soglaša z določili, povezanimi s pregledom dodeljevanja uporabniških dostopov v SAP sistem, vključno z odgovornostjo izvajalca, povezano s pregledom.

NAROČNIK:	IZVAJALEC:
Podjetje ABC	Simona Kotar
Ime Priimek, Generalni direktor	
Ljubljana, 30. 3. 2021	Celje, 30. 3. 2021

6.2 Revizijski načrt

NAČRT PREGLEDA DODELJEVANJA, ODVZEMANJA IN SPREMINJANJA UPORABNIŠKIH DOSTOPOV V SAP SISTEM V PODJETJU ABC

1. Revizijski cilji

Cilj pregleda je izraziti neodvisno mnenje glede delovanja notranjih kontrol dodeljevanja, odvzemanja in spreminjanja uporabniških dostopov v SAP sistem v podjetju ABC za obdobje od 1. 1. 2020 do 31. 12. 2020 in poročanje o trenutnem stanju delovanja in učinkovitosti notranjih kontrol na področju dodeljevanja, odvzemanja in spreminjanja dostopov v SAP sistem. Da bi dosegli zastavljeni cilj bomo:

- preverili skladnost postopka dodeljevanja, odvzemanja in spreminjanja uporabniških dostopov z internimi pravilniki in dobrimi praksami;
- pregledali procesa vzdrževanja in rednega preverjanja matrike vlog;
- pregledali izvajanja procesa razmejitve odgovornosti (SOD[11]).

Pregled vključuje izvajanje postopkov za pridobitev revizijskih dokazov o uspešnosti delovanja naročnikovih notranjih kontrol procesa dodeljevanja, odvzemanja in spreminjanja uporabniških dostopov v SAP sistem. Izbrani postopki so odvisni od revizorjeve presoje.

2. Tveganja

- Tveganje, da imajo zaposleni dostopne pravice do sistemov in informacij, ki jih pri delu ne potrebujejo.
- Tveganje, da imajo nepooblaščeni zaposleni dostop do informacij zaupnega značaja.
- Tveganje, da imajo nepooblaščeni zaposleni dostop do procesov ali nastavitev, ki lahko kritično vplivajo na poslovni proces.
- Tveganje, da lahko zaradi preveč široko dodeljenih dostopov en zaposleni upravlja celoten proces.

3. Tveganje revizijskega posla

- Zaradi naravnih omejitev pregleda skupaj z naravnimi omejitvami notranjega kontroliranja se ni mogoče izogniti tveganju, da se kakšnih pomembnih pomanjkljivosti v zasnovi in delovanju notranjih kontrol morda ne bo odkrilo, kljub temu, da bo pregled pravilno načrtovan in opravljen v skladu s Standardi, smernicami ter orodji in tehnikami za strokovnjake revidiranja, kontrol in dajanja zagotovil na področju IT.
- Pri pregledu bodo uporabljeni postopki, ki temeljijo na naključnem vzorčenju, zato obstaja določeno tveganje, da ugotovitve na podlagi vzorčenja ne odražajo dejanskega stanja.
- Ker bodo ugotovitve pregleda pridobljene na podlagi dejanskih podatkov, ki so na voljo v informacijskih sistemih podjetja, je izraženo tveganje sprejemljivo oziroma minimalno. Ugotovitve lahko pomembno odstopajo od dejanskega stanja predvsem v primeru posredovanja nejasnih in/ali zavajajočih pojasnil glede izvajanja revidiranega procesa ter napak ali goljufij sodelujočih.

[11] SOD – razmejitev odgovornosti (angl. segregation of duties)

4. Neodvisnost

- Izvajalec zagotavlja, da z opravljanjem posla za naročnika ni v navzkrižju interesov in v nasprotju z zakonskimi določili. V zadnjih dveh letih izvajalec ni sodeloval na področju izboljšanja delovanja notranjih kontrol in procesov, ki so predmet pregleda, in da s poslovodstvom ali vodstvom področja pregleda naročnika ni sorodstveno povezan.
- Med izvajanjem posla se bo izvajalec izogibal nerevizijskim vlogam v pobudah, ki niso povezane z revidiranjem in zahtevajo prevzem upravljavskih zadolžitev.
- V kolikor bi bila med izvajanjem posla zaznana ali dejansko oslabljena neodvisnost, bo izvajalec to nemudoma razkril naročniku in se z njim posvetoval. Če se bo izvajanje posla kljub oslabitvi neodvisnosti nadaljevalo, bo izvajalec v poročilu vključil vse informacije za razumevanje narave morebitne oslabitve.

5. Obseg posla/predmet pregleda

V pregled so vključeni dodeljeni, odstranjeni in spremenjeni dostopi uporabnikov do SAP sistema v podjetju ABC v obdobju od 1. 1. 2020 do 31. 12. 2020 in poročanje o trenutnem stanju delovanja in učinkovitosti notranjih kontrol na področju postopkov za dodeljevanje, spreminjanje in odvzemanje dostopov v SAP sistem.

6. Sodila (zakonodaja, pravilniki, navodila)

Poleg internih pravilnikov s področja varovanja informacij se bodo pri pregledu uporabile naslednje smernice in vodila iz standarda ISO/IEC 27001:2013 (dodatek A):

- A.6.1.2. Razmejitev dolžnosti: Nasprotujoče si naloge in področja odgovornosti se morajo razmejiti, da se zmanjšajo možnosti za nepooblaščeno ali nenamerno spreminjanje ali zlorabo sredstev organizacije.
- A.9.2.3. Upravljanje privilegiranih pravic dostopa: Dodelitev in uporaba privilegiranih pravic dostopa se morata omejiti in nadzorovati.
- A.9.2.5. Pregled uporabniških pravic dostopa: Lastniki sredstev morajo pregledovati uporabniške pravice dostopa v rednih časovnih presledkih.
- A.9.2.6. Preklic ali prilagoditev pravic dostopa: Pravice dostopa vseh zaposlenih in zunanjih uporabnikov do informacij in naprav za obdelavo informacij se morajo odstraniti po prekinitvi njihove zaposlitve, pogodbe ali dogovora oziroma se prilagoditi spremembam.

Kot sodila bomo, v kolikor jih bo potrdil naročnik, smiselno uporabili tudi COBIT 2019 kontrolne cilje DSS05.04 Upravljanje uporabniške identitete in logičnega dostopa (Manage user identity and logical access) zrelostnega modela 1 in deloma 2[12].

[12] COBIT 2019 Framework: Governance and Management Objectives, izdala ISACA. DSS 05.04 Manage user identity and logical access; Activities for Capability Level 2: Maintain user access rights in accordance with business function, process requirements and security policies. Align the management of identities and access rights to the defined roles and responsibilities, based on least-privilege, need-to-have and need-to-know principles.
Activities for Capablity Level 3: Administer all changes to access rights (creation, modifications and deletions) in a timely manner based only on approved and documented transactions authorized by designated management individuals.

7. Omejitve

- V pregled niso zajete ostale informacijske rešitve naročnika in tehnološka infrastruktura, na kateri delujejo.
- Zaradi naravnih omejitev pregleda skupaj z naravnimi omejitvami notranjega kontroliranja se ni mogoče izogniti tveganju, da se kakšnih pomembnih pomanjkljivosti v zasnovi in delovanju notranjih kontrol morda ne bo odkrilo, kljub temu, da bo pregled pravilno načrtovan in opravljen v skladu s Standardi, smernicami ter orodji in tehnikami za strokovnjake revidiranja, kontrol in dajanja zagotovil na področju IT.

8. Izvajalec

Pregled bo izvedla Simona Kotar, vključena v izobraževanje za pridobitev strokovnega naziva preizkušeni revizor informacijskih sistemov.

9. Časovni načrt

FAZA	DATUM	ŠT. REVIZOR DNI
NAČRTOVANJE	1. 4. 2021 – 6. 4. 2021	3
IZVAJANJE	7. 4. 2021 – 27. 4. 2021	14
POROČANJE (osnutek poročila)[13]	28. 4. 2021 – 30. 4. 2021	3

10. Revizijski postopki

a) Seznanitev z revizijskem okoljem: pregled uradne SAP dokumentacije – katalog vseh obstoječih transakcij po posameznem sistemu, katalog razmejitev odgovornosti, ki jih ima SAP v svoji zasnovi (SAP design), katalog vlog in pripadajočih transakcij znotraj vloge, pravilnik/mehanika/način dodeljevanja SAP dostopov uporabnikom.

b) Preizkus obstoja in delovanja notranjih kontrol z vidika upravičenosti dostopa uporabnika do SAPa:
   - Potrebne evidence:
     1. evidenca kadrovskih podatkov za vse zaposlene v podjetju ABC (ime, priimek, delovno mesto, sektor/služba, oddelek, datum zasedbe delovnega mesta);
     2. evidenca vseh menjav organizacijskih enot zaposlenih v zadnjem letu;
     3. seznam vseh dostopov v SAPu (uporabnik, sistem/modul, vloge, datumi (od kdaj in do kdaj, če so kakšne omejitve);
     4. matrika vlog (katere transakcije so zajete v posamezni vlogi, z opisom vseh transakcij in pravilom, za katera delovna mesta se sme določeno vlogo dodeliti).
   - Test podatkov:
     - samo aktivni zaposleni podjetja ABC imajo dodeljen SAP dostop (preveri se, da nimajo dostopa do SAPa zaposleni, ki so že zapustili podjetje);
     - zaposlenim, ki so zamenjali delovno mesto, so bili odstranjeni vsi dostopi in bili ponovno dodeljeni skladno z zadolžitvami novega delovnega mesta;

[13] Datum izdaje končnega poročila je odvisen od zaključnega sestanka med izvajalcem in naročnikom ter morebitnih dodatnih dokaznih gradivih, ki bi jih naročnik predstavil naknadno.

- Upoštevanje principa »potrebe po vedenju«[14] (uporabniki imajo prvenstveno dostop le do sistema, ki ga za delo uporablja organizacijska enota, v kateri delajo, oz. ko za dodelitev dostopa do drugega modula/sistema obstaja primerna odobritev);
- Na vzorcu dostopov, ki so se dodelili v revizijskem obdobju, preveriti odobritve skrbnikov in pojasnilo, v kolikor je bil dodeljen dostop do drugega modula/sistema;
- Na vzorcu dostopov, ki so bili časovno omejeni, preveriti, če je bil dostop tudi pravočasno odstranjen.

c) Pregled principa nastavitve in vzdrževanja matrike vlog:
   - katere razmejitve odgovornosti so bile ohranjene od avtomatično vgrajenih v zasnovo SAP (kreiranje, spreminjanje, avtoriziranje (odobritev), pregled);
   - konflikti znotraj posameznih vlog (ena vloga ne vsebuje dveh od treh transakcij, ki omogočajo kreiranje, spreminjanje in avtoriziranje) – upoštevanje »need-to-know« principa znotraj matrike vlog;
   - na vzorcu zaposlenih preveriti, da zaposleni nima dodatno dodeljenih dostopov, kot je določeno v matriki vlog. Če ima, se preveri tudi odobritveni zahtevek.
d) Pregled smotrnosti dostopa za uporabnika:
   - z uporabnike se preveri datum zadnjega dostopa do SAPa (ali uporabnik dostop dejansko potrebuje).
e) Pregled razmejitve SAP uporabnikov:
   - razmejitev na skrbnike, ključne uporabnike, napredne uporabnike, končne uporabnike – obstoj različnih uporabnikov in merila;
   - Testni dostopi – dostop do testnega in razvojnega sistema, ki sta ločena od produkcijskega;
   - Uporabniki, ki imajo možnost spreminjanja nastavitev.
f) Izvedba morebitnih dodatnih postopkov, v kolikor se med pregledom izkaže potreba po tem.

11. Izdelki

- osnutek poročila (vsebina poročila predstavljena v Prilogi 1), poslano elektronsko v pdf formatu
- usklajevalni sestanek
- končno poročilo in povzetek poročila (vsebina poročila in povzetka predstavljena v Prilogi 1), poslano elektronsko v pdf formatu
- zaključni sestanek in predstavitev ugotovitev.

12. Prejemniki poročila oziroma povzetka poročila

- poslovodstvo podjetja ABC (poročilo in povzetek)
- vodja Sektorja za informatiko podjetja ABC (poročilo)
- vodja Informacijske varnosti podjetja ABC (poročilo)
- revizijska komisija nadzornega sveta podjetja ABC (povzetek)

Datum: 30.3.2021
Izvajalec: Simona Kotar

[14] Need-to-know razmejitve: 1. med službami/sektorji, 2. med oddelki znotraj ene službe/sektorja in 3. znotraj procesov (create, change, approve, display only).

6.3 Vprašalnik revidirancu

ORGANIZACIJA PODJETJA

1. Opišite dejavnost podjetja.
2. Predstavitev podatkov o številu zaposlenih, organizacijski strukturi in fluktuaciji
3. Kako je organizirano upravljanje z informacijsko tehnologijo? Ali ima podjetje svoj IT oddelek ali uporablja zunanjega izvajalca?

PRAVILNIKI IN INTERNI AKTI

1. Ali ima podjetje varnostno politiko? Če da, kdaj je bila nazadnje posodobljena?
2. Katere interne politike, pravilniki in navodila opredeljujejo proces upravljanja dostopov?
3. Kako pogosto se pregledujejo in posodabljajo politike, pravilniki in navodila? Kdo je odgovoren za posodabljanje?
4. Na kakšen način so zaposleni seznanjeni s sprejetimi politikami, pravilniki in navodili? Ali so dokumenti zaposlenim splošno dostopni? Kako se zaposlene seznani s spremembami dokumentov?

VPELJAVA SAP SISTEMA

1. Opišite proces vpeljave SAP sistema.
2. Kakšne informacijske rešitve je podjetje uporabljalo pred uvedbo SAPa?
3. Kako se je izvedla vpeljava SAP sistema? Kdo je bil izvajalec? Kakšna je bila časovnica vpeljave?
4. Katere module SAP sistema je podjetje uvedlo?
5. Kako je bil vzpostavljen prenos podatkov in dostopov iz starih sistemov na SAP?
6. Kako so bili urejeni SAP uporabniški dostopi? Kdo je sestavil vloge s transakcijami? Kako se je določila dodelitev vlog uporabnikom?
7. Kako je bil organiziran prenos znanja uporabe?
8. Kako je dogovorjeno vzdrževanje, podpora in pomoč izvajalca po uvedbi sistema SAP?

UPRAVLJANJE Z DOSTOPI V SAP SISTEMU

1. Opišite proces dodeljevanja, odvzemanja in spreminjanja uporabniških dostopov v SAP sistem.
2. Kdo je odgovoren za kreiranje vlog?
3. Kdo je odgovoren za upravljanje uporabnikov in dostopov?
4. Na kakšen način se spremlja zahtevke in izvedbo upravljanja uporabniških dostopov?
5. Kako pogosto se izvaja pregled in čiščenje dodeljenih dostopov?

6.4 Načrt testiranj

1. Seznanitev z revizijskem okoljem: pregled uradne SAP dokumentacije – katalog vseh obstoječih transakcij po posameznem sistemu, katalog razmejitev odgovornosti, ki jih ima SAP v svoji zasnovi (SAP design), katalog vlog in pripadajočih transakcij znotraj vloge, pravilnik/mehanika/način dodeljevanja SAP dostopov uporabnikom.
2. Preizkus obstoja in delovanja notranjih kontrol z vidika upravičenosti dostopa uporabnika do SAPa:
   2.1. Potrebne evidence:
   - evidenca kadrovskih podatkov za vse zaposlene v podjetju ABC (ime, priimek, delovno mesto, sektor/služba, oddelek, datum zasedbe delovnega mesta);
   - evidenca vseh menjav zaposlenih med organizacijskimi enotami v zadnjem letu;
   - seznam vseh dostopov v SAPu (uporabnik, sistem/modul, vloge, datumi (od kdaj in do kdaj, če so kakšne omejitve);
   - matrika vlog (katere transakcije so zajete v posamezni vlogi, z opisom vseh transakcij in pravilom, za katera delovna mesta se sme določeno vlogo dodeliti).

   2.2. Test podatkov:
   - samo aktivni zaposleni podjetja ABC imajo dodeljen SAP dostop (preveri se, da nimajo dostopa do SAPa zaposleni, ki so že zapustili podjetje);
   - zaposlenim, ki so zamenjali delovno mesto, so bili odstranjeni vsi dostopi in bili ponovno dodeljeni skladno z zadolžitvami novega delovnega mesta;
   - upoštevanje principa »potrebe po vedenju«[15] (uporabniki imajo prvenstveno dostop le do sistema, ki ga za delo uporablja organizacijska enota, v kateri delajo, oz. ko za dodelitev dostopa do drugega modula/sistema obstaja primerna odobritev);
   - na vzorcu dostopov, ki so se dodelili v revizijskem obdobju, preveriti odobritve skrbnikov in pojasnilo, v kolikor je bil dodeljen dostop do drugega modula/sistema;
   - na vzorcu dostopov, ki so bili časovno omejeni, preveriti, če je bil dostop tudi pravočasno odstranjen;
   - Varnostne nastavitve za gesla.
3. Pregled principa nastavitve in vzdrževanja matrike vlog:
   - katere razmejitve odgovornosti so bile ohranjene od avtomatično vgrajenih v zasnovo SAP (kreiranje, spreminjanje, avtoriziranje (odobritev), pregled);
   - konflikti znotraj posameznih vlog (ena vloga ne vsebuje dveh od treh transakcij, ki omogočajo kreiranje, spreminjanje in avtoriziranje) – upoštevanje »need-to-know« principa znotraj matrike vlog;
   - na vzorcu zaposlenih preveriti, da zaposleni nima dodatno dodeljenih dostopov, kot je določeno v matriki vlog. Če ima, se preveri tudi odobritveni zahtevek.
4. Pregled smotrnosti dostopa za uporabnika:
   - za uporabnike se preveri datum zadnjega dostopa do SAPa (ali uporabnik dostop dejansko potrebuje).

[15] Need-to-know razmejitve: 1. Med službami/sektorji, 2. Med oddelki znotraj ene službe/sektorja in 3. Znotraj procesov (create, change, approve, display only).

5. Pregled razmejitve SAP uporabnikov:
   - razmejitev na skrbnike, ključne uporabnike, napredne uporabnike, končne uporabnike – obstoj različnih uporabnikov in merila;
   - testni dostopi – dostop do testnega in razvojnega sistema, ki sta ločena od produkcijskega;
   - uporabniki, ki imajo možnost spreminjanja nastavitev.
6. Izvedba morebitnih dodatnih postopkov, v kolikor se med pregledom izkaže potreba po tem.

6.5 Povzetek podanih priporočil

- Vzpostavitev procesa upravljanja uporabniških dostopov in izdaja internega pravilnika, ki opredeljuje postopke dodeljevanja, odvzemanja in spreminjanja uporabniških dostopov.
- Uskladitev standardnih SAP procesov z obstoječimi poslovnimi procesi, prepoznati začetek in konec posameznega SAP procesa in oblikovanje vlog, ki ne omogočajo izvajanja aktivnosti, ki so odgovornost več kot enega poslovnega procesa.
- Uporaba izmišljenih podatkov v testnem sistemu, v kolikor ni možno zagotoviti razmejevanja odgovornosti oz. dodeliti dostop do podatkov, ki jih potrebuje uporabnik za izvajanje procesov, za katere je odgovoren.
- Vzpostavitev in testiranje enakih vlog v testnem okolju, kot jih podjetje uporablja v produkcijskem okolju. Tako se bo lahko pred vsako spremembo vlog omogočilo preverjanje delovanja in uporabnosti vlog in zagotovilo, da se proces lahko nemoteno izvaja že pred uvedbo sprememb v produkcijsko okolje.
- Takojšnji odvzem vloge SAP_ALL vsem uporabnikom in kreiranje posebnega uporabnika s profilom SAP_ALL, katerega geslo je skrito in zaklenjeno v sefu in se uporablja le v nujnih primerih in izključno za obdobje, ko je tak dostop potreben za odpravljanje kritičnih napak v delovanju sistema SAP.
- Vzpostavitev rednega (vsaj 2x letno) izvajanja podrobnega pregleda dodeljenih pravic zunanjim SAP uporabnikom. V primeru dodeljenih vlog, ki omogočajo širok obseg dostopa do podatkov in informacij priporočamo obvezno dokumentiranje upravičenosti dodelitve vloge in kratko časovno omejitev dostopov.
- Ukinitev vseh uporabnikov, za katere se ne more jasno določiti, kateremu zaposlenemu pripadajo, in kreiranje uporabnikov na način, da jih je mogoče enolično povezati s posameznim zaposlenim.
- Odstranitev kritičnih avtorizacij vsem uporabnikom, ki ne morejo podati ustrezne razlage, zakaj jih potrebujejo.
- Vzpostavitev politike upravljanja s SAP dostopi, ki bo določala način kreiranja uporabniških vlog ter postopek dodeljevanja, spreminjanja in odvzemanja SAP dostopov; vzpostavitev kataloga razpoložljivih vlog, ki odražajo potrebe poslovnih procesov; vzpostavitev procesa sistematičnega in dokumentiranega dodeljevanja in odstranjevanja vlog uporabnikom.
- Politika varovanja informacij, ki jo je podjetje ABC pripravilo za potrebe certifikacije ISO/IEC 27001:2013 naj jasno opredeljuje pravilno rokovanje z dostopi ter gesli do informacijskih sistemov in vključuje primere nedovoljenih praks.
- Takojšnja menjava gesel za uporabnike SAP*, SAPCPIC in TMSADM. Če standardni uporabniki niso v uporabi priporočamo tudi preklic vseh avtorizacij in zaklenitev (lock) uporabnikov v sistemu.
- Ponovna preveritev vseh nastavitev kontrolnih parametrov, ki se nanašajo na gesla v sistemu SAP, ter izdelava internega pravilnika, ki predpisuje politiko gesel, s katero naj se evidentno seznanijo vsi zaposleni, ki uporabljajo informacijske storitve podjetja ABC.
- Preveritev potrebe po dostopu do sistema SAP za vsakega zaposlenega in odstranitev podvojenih in nepotrebnih uporabnikov.
- Vzpostavitev postopka upravljanja z uporabniškimi dostopov, ki vključuje redno periodično pregledovanje dodeljenih uporabniških dostopov, in odstranjevanje dostopov, ki ne upoštevajo načel minimizacije in ločevanja vlog.