1.04 Strokovni članek

Pomen izvedbenih politik pri uvajanju sistema upravljanja informacijske varnosti

UDK: 659.2:004.056(045)

Tomaž Kralj
Ministrstvo za finance, Davčna uprava Republike Slovenije
tomaz.kralj@gov.si

Simon Starček
Ministrstvo za finance, Davčna uprava Republike Slovenije
simon.starcek@gov.si

IZVLEČEK

Informacijska tehnologija v organizaciji nudi orodje za doseganje poslovnih ciljev. Skoraj nemogoče si je predstavljati organizacijo, ki bi uspešno poslovala brez ustrezne informacijske podpore poslovnim procesom. Enako velja za informacijsko varnost, saj organizacije, sploh v javnem sektorju, pri poslovanju ustvarjajo vse večje količine podatkov, katerih razkritje bi pomenilo razkritje poslovnih tajnosti ali kršitev zakonskih določb glede razkritja osebnih ali drugih podatkov. Informacijska tehnologija, kakor tudi informacijska varnost, sta danes vtkani v domala vse poslovne procese organizacije. Zaradi tega morajo organizacije uvesti organiziran pristop zagotavljanja ustrezne podpore informacijski varnosti, to je sistem upravljanja informacijske varnosti. Le-ta vključuje različne ravni varnostnih politik kakor tudi izvedbene politike, ki določajo ravnanje zaposlenih pri izvajanju poslovnega procesa tako, da bo zadoščeno zahtevam informacijske varnosti. V članku je opredeljen pomen informacijske varnosti in sistema za upravljanje informacijske varnosti. Na procesu dodeljevanja pravic dostopa do aplikacij v Davčni upravi Republike Slovenije je prikazan primer izvedbene politike, njen pomen v procesu vzpostavitve sistema upravljanja informacijske varnosti ter zagotavljanja varnosti podatkov. Opredeljen je tudi pomen izvedbene politike z vidika tveganj informacijske varnosti.

Ključne besede: informacijska varnost, sistem upravljanja informacijske varnosti, poslovni proces, Davčna uprava Republike Slovenije

JEL: D73, D81, K22

1 Uvod

Hitre družbene in ekonomske spremembe so težko predvidljive in segajo v temelje družbe. Zato spremembe in prilagoditve v organizacijah zahtevajo sprotno in takojšnje odzivanje na nove oblike tveganj. V sodobni družbi številnih varnostnih tveganj in groženj je treba ob sistematičnem pristopu na področju varnosti posvetiti posebno pozornost tudi obvladovanju informacij. Varnost je mogoče v teh primerih razumeti kot splet varnostnih ukrepov in postopkov, potrebnih za zaščito, sledljivost in preventivo zlorabe informacije (Tarman, 2012). Spremenjene ekonomske razmere v pogojih globalne konkurence so v zadnjih treh desetletjih sprožile potrebe po reformah tako v zasebnem kot v javnem sektorju. Družbenoekonomski razvoj je s svojim pritiskom na javne finance sprožil številna vprašanja o učinkovitem, preglednem in namenskem trošenju proračunskih sredstev (Stanimirovič & Vintar, 2012).

Organizacije posledično namenjajo vse večjo pozornost optimizaciji stroškov ter tehnološkim in drugim izboljšavam . Glede na tveganja in posledično s tem povezane mogoče stroške se vse pogosteje skrbi tudi za sistem varovanja informacij in komunikacij. Poslovni procesi so vsestransko povezani z informacijsko tehnologijo, saj informacijski sistemi obdelujejo in shranjujejo informacije, aplikacije, inovacije in zaupne podatke, ki so potrebni za opravljanje funkcij organizacije. Če se podatke pravilno uporablja, shranjuje in ščiti, se gradi zaupanje do partnerjev, zagotavlja poslovanje v skladu z zakonodajo in pravili ter zmanjšuje tveganja na vseh ravneh poslovanja.

Raziskava *Information Security Breaches Survey* o informacijski varnosti iz leta 2010, ki jo je izvedlo podjetje *Price Waterhouse Coopers* in je zajela preko 500 malih, srednjih in velikih podjetij, kaže, da je varnostna politika nujen element v podjetju. Podatki raziskave kažejo, da so človeški faktor, nepoštenost in zli nameni glavna varnostna težava v 62 % primerov, povzročitelji pa so v 82 % primerov zaposleni v organizaciji (Price Waterhouse Coopers, 2010). Raziskava, izvedena v letu 2012, kaže, da kar v kar 75 % velikih organizacijah in 61 % malih podjetjih lahko zaposleni uporabljajo pametne telefone in tablične računalnike za dostop do njihovih poslovnih sistemov. Ob tem 82 % velikih organizacij poroča o kršitvah varnosti, ki jih povzročajo zaposleni, vključno s 47 %, ki so izgubili ali razkrili zaupne informacije (Price Waterhouse Coopers, 2012). Zato je treba pri upravljanju varnosti informacij in komunikacij vzpostaviti organizacijske, tehnične, kadrovske in varnostne ukrepe tako, da bodo obvladovali notranje in zunanje vire tveganj ter varnostna tveganja.

Informacijska varnost se ukvarja z varovanjem informacij pred nepooblaščenim dostopom, razkritjem, uničenjem spremembo ali nerazpoložljivostjo. Informacijsko varnost lahko opredelimo tudi kot področje, ki se ukvarja z ohranjanjem zaupnosti, celovitosti in razpoložljivosti informacij. Poleg tega skrbi še za ohranjanje drugih lastnosti, kot so verodostojnost, odgovornost, neovrgljivost in zanesljivost (ISO/IEC 17799:2005, 2004). Po t. i. Parkerjevi

šesterici (angl. *Parkerian hexad*) je treba poleg zaupnosti, razpoložljivosti in celovitosti obravnavati še posest, istovetnost in uporabnost.

Informacijsko varnost označujemo kot varovanje (Ministrstvo za javno upravo, 2010):

- zaupnosti: varovanje podatkov in informacij pred razkritjem nepooblaščenim ter zagotavljanje odgovornosti za njihova dejanja;
- celovitosti: varovanje podatkov in informacij pred neavtoriziranimi spremembami, zagotavljanje verodostojnosti – točnosti, popolnosti in nespremenljivosti informacij ter postopkov procesiranja;
- razpoložljivosti: varovanje podatkov, informacij in servisov pred prekinitvami v delovanju ter zagotavljanje informacij pooblaščenim uporabnikom v času, ko jih potrebujejo, in na zahtevani način.

Varovanje zaupnosti informacij preprečuje nepooblaščene dostope in razkritje tistim osebam, ki do njih niso upravičene. Primer kršitve tega načela je razkritje zaupne informacije osebam, ki za to nimajo ustreznega pooblastila. Celovitost ali neoporečnost pomeni pravilnost informacij. To zagotavlja, da ne pride do nepooblaščenih ali nekontroliranih aktivnosti, kot so ustvarjanje, spreminjanje ali izbris informacijskih virov. Razpoložljivost informacij in informacijskih virov pomeni njihovo dosegljivost v trenutku, ko se pojavi poslovna potreba oziroma zahteva po njih. Primer kršitve tega načela je nerazpoložljivost elektronskega poštnega predala v delovnem času. Informacijska varnost se nanaša na vse sisteme in procese, ki so neposredno povezani z njimi (informacijski sistemi, zaposleni, računalniška oprema, agregati, fizična varnost, povezava v svetovni splet in podobno). Zaradi tega se informacijska varnost dotika celo vprašanj, kot so varovanje zasebnosti, upoštevanje zakonskih in drugih določil, neprekinjeno poslovanje, okrevanje po nesrečah, fizično varovanje, upravljanje z incidenti, varovanje človeških virov in podobno. Da lahko dosežemo ustrezno raven informacijske varnosti, moramo najprej poiskati optimalno razmerje med varnostjo, povezano z zaposlenimi, varnostjo, povezano s fizičnim varovanjem in varnostjo, povezano z organizacijo.

Informacijska tehnologija danes pokriva vse poslovne procese in je zaradi tega zagotavljanje varnega poslovanja organizacije postalo predvsem vprašanje oziroma problem zagotavljanja učinkovite informacijske varnosti. Dostop pooblaščenim osebam do ustreznih in kakovostnih informacij ob pravem času omogoča kakovostno delovanje, odločanje in prilagajanje. Zaradi tega naj bo vzpostavitev kakovostnega sistema varovanja informacij eden od strateških ciljev vsake sodobne organizacije. Le na tak način lahko organizacija doseže neprekinjeno poslovanje, zmanjša poslovna in druga tveganja, zmanjša stroške, povezane z informacijsko varnostjo, obvaruje dobro ime ter si zagotovi skladnost delovanja z veljavno področno zakonodajo.

Varovanje informacij in informacijskih sistemov je stalen proces, ki z dopolnjevanjem organizacijskih in tehničnih ukrepov varuje podatke oziroma

informacije pred razkritjem in nepooblaščenim dostopom (zaupnost), uničenjem in spremembami (celovitost) ter prekinitvami (razpoložljivost). Priprava celovite informacijske varnostne politike je tako prvi korak v smeri oblikovanja strategije varnega poslovanja. Varovanje informacij in informacijskih sistemov pomeni tudi usklajenost z zahtevami, opredeljenimi v zakonodaji.

V članku je na primeru izbranega poslovnega procesa v Davčni upravi Republike Slovenije prikazan primer izvedbene politike kot navodilo o dodeljevanju pravic dostopa do aplikacij. Proučen je njen pomen v procesu vzpostavitve sistema upravljanja informacijske varnosti ter zagotavljanju varnosti podatkov. Analiziran je tudi pomen izvedbene politike ob tveganjih informacijske varnosti. Pomen in vlogo izbranega primera izvedbene politike je na podlagi ugotovitev mogoče analizirati tudi v drugih poslovnih okoljih v javni upravi ali realnem sektorju.

2 Sistem upravljanja informacijske varnosti

Naloga sistema upravljanja informacijske varnosti (SUIV) je obvladovanje sodobnega poslovnega informacijskega sistema, nadzor nad delovanjem informacijskih virov in zmanjševanje učinkov entropije (težnje k nenehnemu propadu) poslovnega sistema. Zato uvajanje sistema varovanja informacij posega na vse odločitvene ravni procesa upravljanja. Certifikacija skladnosti sistema z zahtevami in določili ustreznega standarda ima pomembno vlogo tako pri delovanju organizacije kakor v sodelovanju z okoljem, saj zagotavlja vsem partnerjem, da organizacija obvladuje ustrezno raven varovanja informacij.

Koristi uvedbe sistema upravljanja informacijske varnosti:

- celosten pristop k informacijski varnosti v organizaciji;
- pravočasno odkrivanje in poročanje o varnostnih incidentih ter posledično zmanjšanje stroškov, ki jih taki dogodki povzročajo;
- kakovostnejše načrtovanje in vlaganje v tista področja, kjer je to res potrebno;
- učinkovito upravljanje in odprava varnostnih groženj;
- strukturiran in skladen pristop;
- dvig zaupanja v upravljanje informacijskih virov.

Sistem za upravljanje varovanja informacij naj torej zajema naslednja področja: organiziranost varovanja, razvrstitev in nadzor sredstev, človeške vire, fizično in okoljsko varovanje, upravljanje komunikacij in produkcije, nadzor dostopa, razvijanje in vzdrževanje sistemov, neprekinjeno poslovanje ter usklajenosti.

Prednosti, ki jih prinaša sistem upravljanja informacijske varnosti:

- okrepitev obstoječega okolja nadzora informacijske varnosti s ponovnim poudarkom na nadzoru nad varnostjo poslovnih informacij ter z nadgradnjo obstoječih politik in kontrol informacijske varnosti;
- spodbuda za pregled in posodabljanje nadzora informacijske varnosti – zmanjševanje tveganja;
- strokoven, standardiziran in racionalen pristop za obvladovanje tveganj, ki zagotavlja skladnost med več sistemi v daljšem časovnem obdobju in dosledno usmerja tveganja informacijske varnosti; pristop, upoštevajoč tveganje, se osredotoča na področja največjih tveganj in omogoča zmanjševanje tveganja;
- vodstvo in zaposleni so bolje seznanjeni s pogoji in nadzorom informacijske varnosti – kar omogoča zmanjševanje tveganja.

Zaznavanje in interpretacija varnosti sta v veliki meri odvisna od splošne varnostne kulture v organizaciji. Za ponazoritev – če zapisana pravila ali postopki v določeni organizaciji štejejo za neučinkovita in nepomembna, je takšen tudi odnos do varnostnih pravil. V organizaciji se vzpostavi negativen odnos do delovnih orodij, ki se najpogosteje kaže v obliki izgovorov, da določena naloga ni bila izvedena zaradi tega, ker je pravila ne narekujejo (Guldenmund, 2000). Aktiven odnos posameznika do zaščite in varovanja osebnih ter zaupnih podatkov, ki zajema celotno znanje o zaščiti in varovanju teh podatkov ter se kaže z zavestnim vedenjem v konkretni situaciji, lahko opredelimo kot izraz visoke stopnje varnostne kulture. Ta ne pomeni zgolj vedenja, ampak predvsem vsebino, globlje motive in vzroke, kjer je ogroženost vrednot glavni povod za njihovo zaščito (Košmrlj, 1982).

3 Standardi in sistem upravljanja informacijske varnosti

Področje upravljanja informacijske varnosti obravnava večje število mednarodno priznanih standardov in priporočil, kot so: SGP – *Standard of Good Practice*, ki ga izdaja *Information Security Forum* (ISF), BS 7799 (*British Standards Institute* – BSI), CIP-002-1, ki ga izdaja *North America Electric Reliability Council* (NERC), SP 800-53 A, ki ga izdaja *National Institute of Standards and Technology* (NIST), in ISO/IEC 27001 (*International Organization for Standardization* – ISO).

V prispevku se bomo osredotočili na družino standardov upravljanja informacijske varnosti 27000, ki so osnova za uvajanje sistema upravljanja informacijske varnosti. V to družino spadajo naslednji standardi:

- ISO/IEC 27000:2011 Informacijska tehnologija – Varnostne tehnike – Sistemi upravljanja informacijske varnosti – Pregled in izrazoslovje
- ISO/IEC 27001:2005 Informacijska tehnologija – Varnostne tehnike – Sistemi upravljanja informacijske varnosti – Zahteve
- ISO/IEC 27002:2008 Informacijska tehnologija – Varnostne tehnike – Pravila obnašanja pri upravljanju informacijske varnosti

- ISO/IEC 27003:2011 Informacijska tehnologija – Varnostne tehnike – Smernice za izvedbo sistema upravljanja informacijske varnosti
- ISO/IEC 27004:2011 Informacijska tehnologija – Varnostne tehnike – Upravljanje informacijske varnosti – Merjenje
- ISO/IEC 27005:2011 Informacijska tehnologija – Varnostne tehnike – Upravljanje tveganj informacijske varnosti.

Med navedenimi standardi je za certifikacijo priporočljiv standard ISO/IEC 27001:2005. Le-ta vsebuje formalni nabor specifikacij za model upravljanja informacijske varnosti. Splošna zahteva standarda je, da organizacija razvije, izvede, vzdržuje in stalno izboljšuje dokumentiran SUIV v skladu s poslovnimi aktivnostmi, ranljivostjo, ogroženostjo in tveganji. Naloga SUIV-a je, da zagotavlja ustrezne in sorazmerne varnostne kontrole, ki primerno ščitijo informacijska sredstva in omogočajo zaupanje strank ter drugih zainteresiranih.

Standarda ISO/IEC 27001:2005 in ISO/IEC 27002:2008 sta poslovodno in od posameznih tehnoloških rešitev neodvisni orodji, ki ponujata celovit pregled varovanja informacij pri poslovanju organizacije. Standarda sta glede informacijske varnosti celovita. To pomeni, da ne obravnavata le informacijske tehnologije in informacij v elektronski obliki, temveč informacije v vseh mogočih oblikah in medijih. Pri tem so mnoge opisane kontrole povsem organizacijske narave in niso povezane s tehnologijo, kot na primer razvrstitev informacij, politika čiste mize, fizično varovanje objektov, upravljanje človeških virov in podobno.

4 Uvedba sistema upravljanja informacijske varnosti v organizaciji

Uvedba sistema upravljanja informacijske varnosti je projekt, ki ga je treba izpeljati skrbno in v skladu z dobrimi praksami projektnega menedžmenta. To pomeni, da je treba opredeliti cilj, finančna sredstva, časovni okvir izvedbe projekta ter druge projektne vire, ki naj bodo na voljo pri uvedbi SUIV-a (npr. človeški viri, infrastruktura).

Pomemben vidik pri uvedbi sistema je ustrezna določitev cilja, ki mu bo SUIV zadostil. Uvedba sistema mora temeljiti na odločitvi in podpori najvišjega vodstva, ki mora spoznati ustrezen način vzpostavitve upravljanja informacijske varnosti kot pot pri doseganju rezultatov poslovanja na pregleden in kljub temu varen način.

Organizacije pri uvajanju SUIV-a pogosto ne sledijo projektnemu načinu uvajanja sistema. Tovrsten pristop je ustrezen, v kolikor organizacija razume pomen informacijske varnosti in uvede sistem skrbno ter v celoti. V kolikor pa se izpustijo določeni postopki ali celo izdelki, ki so prepoznani kot pomemben del končnega sistema, lahko sledi:

- varnostne politike in navodila niso usklajeni;

- varnostne politike in postopki niso podprti z ustreznimi navodili;
- sistem je nepregleden in ne omogoča doslednega izvajanja cikla PDCA[1] (načrtuj, izvajaj, nadzoruj, ukrepaj);
- sistem je le nabor delnih rešitev in nepovezana celota.

Če se SUIV ne uvede projektno ali se uvaja denimo kot posledica zahtev zunanjih dejavnikov po ureditvi področja, ki še ni del upravljanega dela informacijske varnosti v organizaciji, so v procesu uvajanja značilne medsebojno slabo ali celo nepovezane aktivnosti. Pogoste so tudi ponavljajoče aktivnosti, ki so časovno in finančno zahtevnejše, kot če bi bila uvedba sistema izvedena projektno.

Pri uvedbi SUIV-a je treba izvesti naslednje korake:

- vzpostavitev organizacijske strukture informacijske varnosti (odbor informacijske varnosti, vodja informacijske varnosti);
- analiza vrzeli, ki poda sliko trenutnega stanja v organizaciji glede na določila in zahteve ustreznega standarda in nakaže prihodnje korake projekta;
- ocena tveganja: ocena ogroženosti, posledic in ranljivosti informacij ter zmogljivosti za obdelavo informacij in verjetnost dogodka naštetih pojavov;
- določitev ciljev uvedbe sistema in opredelitev področij, ki jih bo uvedba sistema obsegala (postavitev meja);
- priprava krovne varnostne politike in drugih (področnih) varnostnih politik; krovna varnostna politika opredeljuje osnovna načela varovanja informacij v organizaciji in naslavlja druge varnostne politike, ki podrobno urejajo posamezna področja;
- opredelitev postopkov in navodil, ki bodo določali postopanje uslužbencev pri izvajanju poslovnih procesov na način, da bo zadoščeno zahtevam informacijske varnosti;
- predstavitev rezultatov projekta vodstvu;
- integracija sistema z drugimi sistemi vodenja, če so v organizaciji vzpostavljeni;
- usposabljanje zaposlenih.

Če je eden izmed ciljev projekta uvedbe SUIV-a tudi njegova certifikacija (npr. v skladu z mednarodnim standardom ISO/IEC 27001:2005), so potrebni iše dodatni postopki, in sicer:

- izvedba notranje presoje in odprava morebitnih neskladnosti glede na določila in zahteve standarda, po katerem bo izvedena certifikacija;
- izvedba certifikacijske presoje.

Vzpostavitev krovne politike informacijske varnosti in vzpostavitev področnih politik je izhodišče za vzpostavitev ustrezne ravni informacijske varnosti

1 Demingov krog PDCA (*Plan-Do-Check-Act*)

v organizaciji. Varnostna politika ni smernica ali standard, niti ni postopek, temveč je načrt za celovit program varnosti. Varnostna politika opredeljuje varnost tako, kot podrobnejši opis izdelka opredeljuje izdelek (Barman, 2002). Varnostna politika informacijskega sistema je definirana kot celovit pogled na varnost informacijskega sistema in zajema vse dejavnike, organizacijska pravila in postopke, ki kakorkoli vplivajo na varno in zanesljivo delovanje celotnega informacijskega sistema (Štrakl, 2003). Varnostna politika predstavlja osnovni temelj, na katerem se lahko razvije učinkovit in celovit program varnosti. Varnostna politika pomeni tudi uvajanje varnostnih pričakovanj vodstva v praksi, v obliki specifičnih, izmerljivih in preverljivih ciljev ter nalog. Varnostno politiko lahko opredelimo kot celovit načrt varovanja informacij in delovnih procesov v organizaciji, ki je zavezujoč za vse zaposlene, pred različnimi (neželenimi) zunanjimi in notranjimi vplivi, ki ogrožajo informacijsko varnost neke organizacije in varnost organizacije kot celote (Kralj, 2012).

Z vidika uslužbenca so krovne in področne politike pogosto vsebinsko in izvedbeno preveč splošne. Zato je treba izdelati natančnejša navodila, ki določajo ravnanje uslužbenca pri izvajanju poslovnih procesov. Takšna navodila kakovostneje določajo postopke ravnanja uslužbenca in opredeljujejo ustrezne obrazce ter evidence, ki se uporabljajo pri izvajanju procesa. V navodilih se opredelijo vloge posameznikov v obravnavanem procesu, njihove dolžnosti in odgovornosti ter tveganja in posledice v primeru opustitve dolžnega ravnanja.

5 Uvedba sistema upravljanja informacijske varnosti v davčni upravi – primer izvedbene politike

V Davčni upravi Republike Slovenije (v nadaljevanju davčna uprava) je skrb za varnost podatkov, celovitost in dostopnost podatkov naloga in dolžnost do vseh davčnih zavezancev v Republiki Sloveniji. V davčni upravi je več kot 2400 zaposlenih, v okviru Generalnega davčnega urada in 16 davčnih uradov ter 41 izpostav. Poslovanje je procesno zasnovano in deluje v skladu z zahtevami mednarodnega standarda kakovosti poslovanja ISO 9001:2008. Vzpostavitev ustreznega sistema informacijske varnosti v vsaki organizaciji, kakor tudi davčni upravi, omogoča varnost podatkov pred neavtoriziranim dostopom, uporabo, razkritjem ali spreminjanjem podatkov, k čemur davčno upravo zavezuje tudi zakonodaja (Zakon o tajnih podatkih, Uredba o varovanju tajnih podatkov itd.). Prepoznavanje pomena informacijske varnosti se kaže tudi v podpori najvišjega vodstva, saj so zahteve glede ustrezne vzpostavitve sistema SUIV del poslovne strategije davčne uprave.

Priprava celovitega SUIV-a obsega vse oblike varnostnih tveganj in je osnova za nemoteno in kakovostno poslovanje organizacije. »Politiko varovanja informacij« tvori več notranjih dokumentov, ki vodstvu ali oddelku, odgovornemu za varnost služijo kot krovna strategija varovanja oziroma vodilo pri kakovostnem in učinkovitem izvajanju varnostnih ukrepov in drugih aktivnosti v organizaciji (na primer aktivnost za zaščito informacij

pred razkritjem, izgubo ali krajo, aktivnost za neprekinjeno poslovanje in podobno). Politiko varovanja informacij sestavljajo krovna varnostna politika, ki ima podobno vlogo kot ustava za državo, in področne politike, ki predstavljajo smernice za oblikovanje izvedbenih varnostnih politik, kot je na primer navodilo o varni uporabi prenosnih naprav ali navodilo o dodeljevanju dostopa do aplikacij. Sistematično opredeljevanje postopkov, ki je v splošnem značilno za zagotavljanje informacijske varnosti, je pomembno z vidika preventive, saj prispeva k zmanjševanju, preprečevanju in izogibanju nevarnostim, ki so povezane s tako občutljivim področjem dela (Rančigaj et al., 2012).

Kot primer izvedbene politike je v članku predstavljeno navodilo o dodeljevanju pravic dostopa do aplikacij. Proces je mogoče opisati z naslednjimi primeri uporabe: dodelitev dostopa do aplikacije, omejitev oziroma dodajanje pravic obstoječemu dostopu in odvzem oziroma ukinitev pravice dostopa do aplikacije. V primeru organizacije z manjšim številom zaposlenih, ki za izvajanje poslovnih procesov praviloma uporablja tudi manjše število aplikacij, je zagotovitev ustrezne ravni varnosti pri izvajanju postopkov procesa upravljanja z dostopi do aplikacij načeloma enostavno opravilo. V primeru velikih organizacij, kot je davčna uprava, so ti postopki kompleksnejši. V davčni upravi je več kot 2000 uslužbencev, ki dostopajo in uporabljajo veliko število notranjih in zunanjih aplikacij. Zaradi velikosti organizacije je doseganje ustrezne ravni varnosti narekovalo potrebo po določitvi več oseb, t.i. skrbnikov, ki so odgovorni za upravljanje dostopov do aplikacij.

Pri procesu dodeljevanja pravic dostopa do aplikacij so zaznana naslednja tveganja s področja informacijske varnosti:

- razkritje uporabniškega imena in gesla;
- dodelitev dostopa do aplikacije uporabniku, ki teh pravic sicer nima;
- dodelitev preveč oz. prevelikega obsega pravic uporabniku za dostop do aplikacij;
- neukinitev dostopa do aplikacije, ko bi to moralo biti izvedeno.

Do razkritja uporabniškega imena in gesla lahko pride zaradi nevestnega ravnanja uslužbenca, ki mu je bil dostop dodeljen ali zaradi neupoštevanja varnostnih postopkov pri dodeljevanju dostopa do aplikacije (evidentiranje, obveščanje).

Merila opremljenosti delovnega mesta opredeljujejo, kaj uslužbenec potrebuje za opravljanje delovnih nalog. Treba mu je dodeliti ustrezno računalniško opremo (osebni ali prenosni računalnik, tiskalnik ali le dostop do mrežnega tiskalnika itd.), pisarniško opremo in dostope do aplikacij. V kolikor se ne upošteva meril, se lahko uslužbencu dodelijo dostopi do aplikacij, do katerih ni upravičen. Enako velja za dodelitev preveč pravic v okviru ene aplikacije.

Ko je uslužbenec razporejen na drugo delovno mesto, je treba ukiniti dostope do aplikacij, do katerih več ni upravičen, oziroma odvzeti ali dodati pravice

znotraj posamezne aplikacije glede na zahteve delovnega mesta. V kolikor uslužbenec zapusti organizacijo, je treba ukiniti vse dostope do aplikacij, ki so mu bili dodeljeni. Obe okoliščini zahtevata centraliziran sistem evidentiranja dostopov do aplikacij za posameznega uporabnika. V nasprotnem primeru se zaradi neustreznega obveščanja določeni dostopi ne ukinejo. V kolikor gre za notranje aplikacije, lahko le-te izkoristi uslužbenec, ki pozna uporabniško ime in geslo bivšega uslužbenca ter neupravičeno dostopi do aplikacije oziroma izvede neavtoriziran dostop do podatkov. V kolikor gre za zunanjo aplikacijo, lahko do podatkov dostopi tudi bivši uslužbenec, čeprav mu je že prenehalo delovno razmerje z organizacijo, kjer mu je bil dostop dodeljen.

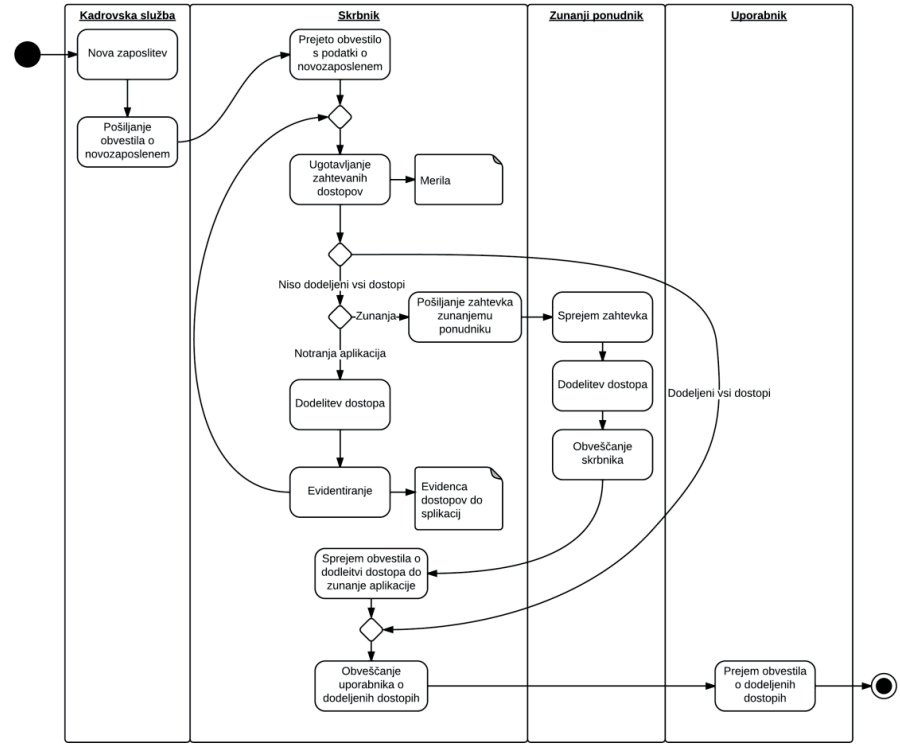
Proces prožijo naslednji dogodki:

- nova zaposlitev uslužbenca,
- premestitev uslužbenca,
- zahtevek za nov dostop oziroma za dodajanje ali odvzem pravic obstoječega dostopa in
- prekinitev delovnega razmerja uslužbenca.

Obveščanje skrbnikov o kadrovskih in drugih spremembah je pomemben del procesa, saj se na ta način doseže, da so uslužbencu pravočasno dodeljeni ustrezni dostopi, z ustreznimi pravicami, oziroma so mu pravočasno omejeni ali odvzeti tisti dostopi in pravice, ki mu v primeru prerazporeditve ali prekinitve delovnega razmerja ne pripadajo več.

Postopek dodelitve dostopov do aplikacij novozaposlenemu prikazuje diagram aktivnosti na sliki 1. Obvestilo o novozaposlenem posreduje kadrovska služba. Skrbniki dodeljevanja dostopov dodelijo dostope v skladu z merili, kjer je določeno, do katerih aplikacij in na kateri ravni ima uslužbenec pravico dostopa glede na njegovo delovno mesto. V primeru, da je treba dodeliti dostop do notranjih aplikacij, skrbnik oblikuje novo uporabniško ime in geslo ter posodobi podatek o dostopu do aplikacije za uporabnika v evidenco dostopov. V kolikor je treba dodeliti dostop do zunanje aplikacije, skrbnik izpolni zahtevek in ga pošlje zunanjemu ponudniku, ki je skrbnik aplikacije. Zunanji ponudnik izda uporabniško ime in geslo za dostop do aplikacije ter ju posreduje skrbniku na davčno upravo. Na koncu skrbnik pošlje uporabniku obvestilo s podatki o dostopih do posameznih aplikacij.

Slika 1: Postopek dodelitve dostopov do aplikacij za novozaposlenega



6 Sklepne ugotovitve

Pomen informacijske varnosti je najlažje opredeliti takrat, ko je mogoče opredeliti vrednost informacije (npr. konkurenčna prednost) ali posledice v primeru okvare ali razkritja informacij. Pomembnost varovanja informacij zaradi kompleksnosti področja zahteva organiziran pristop v obliki upravljanja informacijske varnosti. Zato je vzpostavitev celostnega sistema upravljanja informacij postala potreba organizacije, ki se zaveda pomembnosti varnosti podatkov.

Nekatere organizacije so dolžne vzpostaviti sistem upravljanja informacijske varnosti in ga tudi potrditi oziroma certificirati po enem od veljavnih standardov na področju informacijske varnosti. Certifikacija je lahko zahteva trga, poslovnega partnerja, zakonodaje ali zahtev organizacije, ki opredeljuje predpise za delovanje organizacij s ciljnega področja.

Krovne in področne politike določajo okvir varnostne politike v organizaciji, vendar praviloma ne zadoščajo za celovito uvedbo SUIV-a. Pogosto so odsotna natančna navodila, ki določajo ravnanje uslužbenca in s tem zmanjšanje nastanka tveganj na področju informacijske varnosti. Takšna navodila vsebujejo izvedbene politike, ki določajo odgovornosti, dolžno ravnanje, postopke, opredelijo obrazce ali uslužbenca usmerijo na druge dokumente.

Namen izvedbenih politik je, da uslužbenec izvaja aktivnosti v določenem poslovnem procesu na način, ki je obvladovan, nadzorovan in v skladu z varnostno politiko.

V primeru, da pri uvedbi SUIV-a organizacija ne opredeli izvedbenih politik, ki so bile v analizi vrzeli ali pri oceni tveganja opredeljene kot potrebne, je takšna uvedba SUIV-a nepopolna. Posledično so povečana tudi tveganja na tem področju. Izkazuje se, da davčna uprava z izvedbenimi politikami pomembno dopolnjuje uvedni sistem upravljanja kakovosti, zmanjšuje informacijska in poslovna tveganja ter povečuje preglednost in sposobnost procesov.

V članku predstavljeni primer dodeljevanja dostopov do aplikacij v davčni upravi prikazuje proces, ki mora biti s stališča informacijske varnosti celostno in strokovno obravnavan. Gre za kompleksen proces, ki od vodstva, skrbnikov in zaposlenih zahteva odgovorno ravnanje, zavedanje in obvladovanje tveganj in posledic. Zaradi tega mora biti proces ustrezno dokumentiran. Pri izvajanju postopkov v skladu z vzpostavljenimi navodili, ki jih vsebujejo izvedbene politike informacijske varnosti, se zmanjšajo tveganja, zmanjša se verjetnost kršitve celovitosti, dostopnosti ali zaupnosti, ki so ključne značilnosti ustrezno vzpostavljenega sistema za upravljanje informacijske varnosti.

Menimo, da vzpostavitev izvedbenih politik brez krovne politike ne omogoča ustrezne osnove za učinkovit sistem SUIV v davčni upravi, kakor sicer v organizacijah. Izvedbene politike so pomemben del sistema, brez katerih sistem sicer obstaja, vendar ni pregleden in obvladljiv. Ob tem se tudi ne obravnava vseh tveganj, ki jih je mogoče obvladovati z vzpostavitvijo izvedbenih politik. S krovno politiko in poslovnikom kakovosti v davčni upravi ter z drugimi notranjimi dokumenti, ki opredeljujejo obvladovanje dokumentacije, obveščanja zaposlenih, informacijske varnosti idr., je vzpostavljen sistem stalnih izboljšav, preventivnih in korektivnih ukrepov, inovacij ter merjenja učinkov uvedenih ukrepov tudi za področja, ki jih obravnavajo izvedbene politike. Oblikovanje in uvedba izvedbenih politik v davčni upravi poteka v sodelovanju z vsemi ključnimi dejavniki: zaposlenimi, skrbniki, lastniki procesov ter vodstvom. Poseben poudarek na ravni izvedbenih politik je na medsebojni usklajenosti in skladnosti s krovno politiko ter morebitni medsebojni integraciji. Medsebojno neusklajene izvedbene politike pomenijo nov vir tveganj in neskladnosti v procesu poslovanja in ukrepanja. V davčni upravi nadaljnji razvoj na tem področju sledi cilju poenostavitve izvedbenih politik ter gradnji informacijske podpore njihovemu izvajanju, meritvam, analizam in nadzoru.

Vzpostavitev sistema SUIV pomeni pričetek dolgoročnega procesa v organizaciji. Pomembna je tudi njegova integracija z drugimi sistemi vodenja, v kolikor so uvedeni. Vzpostavitev krovnih in področni politik ter uvedba ustreznih izvedbenih politik je del procesa, ki zagotavlja ustreznejšo raven informacijske varnosti. Zaradi nenehnih sprememb v organizaciji mora tem spremembam slediti tudi SUIV. To pomeni, da se spremembe odrazijo tako v krovni politiki in področnih politikah kakor tudi na ravni izvedbenih politik.

Sistem stalnih izboljšav med drugim narekuje skladnost, aktivno prilagodljivost in posodobitev dokumentov, spremljanje, analiziranje ter merjenje učinkov uvedenih ukrepov, tudi izvedbenih politik. Izkušnja uvedbe izvedbenih politik v davčni upravi dokazuje višjo raven kakovosti in varnosti poslovanja, dvig razumevanja delovnih postopkov, zmanjšanje tveganj ter učinkovitejše obvladovanje in delovanje sistema.

Dr. Tomaž Kralj je diplomiral leta 1997 na Univerzi v Mariboru, Fakulteta za elektrotehniko, računalništvo in informatiko. Na tej fakulteti je dokončal magistrski in leta 2007 doktorski študij. Trenutno je zaposlen na Davčni upravi Republike Slovenije, kjer je zadolžen za področje informacijske varnosti. Je predavatelj na višjih strokovnih šolah in visokih šolah, na fakultetah pa sodeluje kot gostujoči predavatelj. Njegovo raziskovalno delo je povezano s programskimi metrikami, projektnim vodenjem, z informacijsko varnostjo ter doseganjem kakovosti.

Mag. Simon Starček je leta 1999 diplomiral na Pedagoški fakulteti Maribor, na študijski smeri matematika. Na Univerzi v Ljubljani, Fakulteti za gradbeništvo in geodezijo je magistriral s področja geodezije. Zaposlen je na Davčni upravi Republike Slovenije, kjer je zadolžen za področje sistema kakovosti, poslovne odličnosti, projektnega vodenja, poslovnih in drugih tveganj, integritete ter sodeluje pri uvajanja sistema upravljanja informacijske varnosti. Ima dolgoletne izkušnje kot predavatelj, je tudi asistent za področje naravoslovja na Univerzi na Primorskem ter študent zaključnega letnika na doktorskem študijskem programu Univerze v Ljubljani, Fakulteti za gradbeništvo in geodezijo. Njegovo raziskovalno delo je povezano s področjem prostorske podatkovne infrastrukture, baz podatkov, upodobitve in kakovosti podatkov ter s področjem nepremičnin.

Viri in literatura

- Barman, S. (2001). *Writing information security policies*, 1st edition. New Riders Publishing.
- ISO (2005). *BS ISO/IEC 27001:2005: Informacijska tehnologija – Varnostne tehnike – Sistemi za upravljanje varovanja informacij – Zahteve*. Geneve: International Organization for Standardisation.
- ISO (2005). *BS ISO/IEC 27002:2005: Informacijska tehnologija – Varnostne tehnike – Kodeks za upravljanje varovanja informacij*. Geneve: International Organization for Standardisation.
- ISO (2008). *International standard ISO 9001: Sistemi vodenja kakovosti – Zahteve (ISO 9001:2008)*. Geneve: International Organization for Standardisation.
- Kralj, R. (2012). Varnostna politika informacijskega sistema. *Zbornik prispevkov konference: Informacijska varnost: odgovori na sodobne izzive*. Ljubljana: Fakulteta za varnostne vede.
- Ministrstvo za javno upravo (2010). *Priporočila informacijske varnostne politike javne uprave*. Ljubljana.
- Price Waterhouse Coopers. (2010). I*nformation Security Breaches Survey 2010: Technical Report*. London: Price Waterhouse Coopers. Pridobljeno 28. 9. 2012, s http://www.pwc.co.uk/audit-assurance/publications/isbs-survey-2010.jhtml
- Price Waterhouse Coopers. (2012). *Information Security Breaches Survey 2010: Technical Report*. London: Price Waterhouse Coopers. Pridobljeno 28. 9. 2012, s http://www.pwc.co.uk/en_UK/uk/assets/pdf/olpapp/uk-information-security-breaches-survey-technical-report.pdf
- Rančigaj, K., & Lobnikar, B. (2012). Vedenjski vidiki zagotavljanja informacijske varnosti: pomen upravljanja informacijske varnostne kulture. *Zbornik prispevkov konference: Informacijska varnost: odgovori na sodobne izzive* (1–12). Ljubljana: Fakulteta za varnostne vede. Pridobljeno 28. 9. 2012, s http://www.fvv.uni-mb.si/KonferencaIV/zbornik.html.
- Stanimirović, D., & Vintar, M. (2012). Menedžment zunanjega izvajanja IT-projektov v slovenskem javnem sektorju – vsebinski in postopkovni vidiki. *Uprava* X(1), 7–34.
- Štrakl, M. (2003). Varnostna politika informacijskega sistema. *14. delavnica o telekomunikacijah*, 19. in 20. maj 2003 (19–22). Brdo pri Kranju: VITEL. Pridobljeno 26. 9. 2012, s https://lms.uni-mb.si/vitel/14delavnica/clanki/marjan_strakl.pdf
- Tarman, M. (2012). Obvladovanje informacij – korelacija varovanja tajnih podatkov in poslovnih skrivnosti. *Korporativna varnost* 2012(1).
- Whitman, M. E., & Mattord, H. J. (2010). *Management Of Information Security*. Boston: Sourse Technology.

SUMMARY

IMPORTANCE OF OPERATION POLICIES IN IMPLEMENTING INFORMATION SECURITY MANAGEMENT SYSTEM

Key words: information security, information security management system, business process, Tax Administration of the Republic of Slovenia

Information Technology in an organization provides an essential tool for functioning and achieving business goals. The field of information security is becoming increasingly important as organizations, including those in the public sector, create more and more data in their business. Allowing data to be uncovered would reveal vital business information and/or constitute a violation of legislative provisions regarding the security of personal or other data.

Information security consists of:

- security confidentiality: securing data and information from being uncovered by a non-authorized person and ensuring the said person is held responsible for their actions;
- security integrity: securing data and information from unauthorized changes, ensuring reliability – the preciseness, completeness and invariability of information and processing procedures;
- security availability: securing data, information and services from operational interruptions and ensuring that information is provided to authorized users when it is needed and in the required way.

The security of information and information systems is a continual process for protecting data or information from being uncovered and from unauthorized access (confidentiality), destruction, alteration (integrity) and interruption (availability). Appropriate organizational and technical measures complement this process. Preparing a comprehensive information security policy is the first step towards creating a strategy for safe operations. The security of information and information systems also implies harmonisation with demands put forth in the relevant legislation.

The task of the information security management involves knowledge of the contemporary business information system, controlling the operation of information sources and reducing the effects of entropy (the tendency towards continuous destruction) of the business system. The information security management system thus intervenes on all crucial levels of the operation process. Certification that the system is in accordance with the demands and provisions of an adequate standard has an important role in operational organization and in cooperation with the surroundings because it ensures that all partners control the adequate level of information security.

Information Technology and information security are involved in almost all business processes of the organization. It is therefore necessary to introduce organized access to ensure adequate support for information security – the information security management system. This includes various levels of security policy as well as an operational policy which outlines how employees are to behave when carrying out their tasks in the operation process if they are to fulfil the requirements of information security. In the paper definitions are given for information security and the information security management system. Implementation policy is discussed using the example of the process for assigning access rights to applications at the Tax Administration of the Republic of Slovenia. The significance of implementation policy in the process of setting up the information security management system and ensuring data security is the focus of an in-depth investigation. Implementation policy is also defined in reference to information security risk.

The field of information security management includes a large number of internationally acknowledged standards and recommendations: SGP – Standard of Good Practice, published by Information Security Forum (ISF), BS 7799 (British Standards Institute – BSI), CIP-002-1, published by North America Electric Reliability Council (NERC), SP 800-53 A, published by National Institute of Standards and Technology (NIST), in ISO/IEC 27001 (International Organization for Standardization – ISO).

Of the standards listed, the ISO/IEC 27001:2005 standard is recommended for certification. This standard presents a formal set of specifications for a model of information security management. The common requirement of the standard is that organizations develop, carry out, maintain and continuously improve its documented information security management system taking into account their business activities, vulnerability, threats and risk. The task of the information security management system is to ensure adequate and comparable security controls that adequately protect the means of information and make customers and other interested parties confident.

Standards and other good practises for information security management systems in organizations highlight the following steps as crucial:

- setting up the information security organization structure (council of information security, leader of information security);
- analyzing the gap: assessment of the current situation in the organization in terms of the provisions and requirements of an adequate standard and outlining steps that must be taken in the future;
- risk assessment: assessment of threats and consequences, the vulnerability of information, the efficiency of information processing and the possibility that the events listed could occur;
- defining the goals of introducing the system and determining the fields the introduction of the system will encompass (setting up limits);

- preparing the main security policy and other (local) security policies: the main security policy defines the basic principle of information security in the organization and addresses the other security policies that manage particular fields in detail;
- defining processes and instructions that will determine how employees are to proceed when conducting business processes if they are to fulfil the requirements of information security;
- presenting the results of the project to the management;
- integration of the system with other management systems if such systems exist in the organization;
- training employees.

Main and local policies determine the range of security policy in the organization; however, this as a rule is not sufficient for the comprehensive introduction of information security. There is often a lack of detailed instructions, which outline the behaviour of employees and thus reduce risk in the field of information security. Instructions of this kind constitute an implementation policy that determines responsibility, required behaviour and processes and defines blank forms or directs the employee to other adequate documents. The purpose of implementation policy is to ensure that an employee carries out activities in a specific business process in a way that is controlled and in accordance with the security policy.

One example of implementation policy presented in the paper is the instructions on allocating rights for applications. The process can be described in terms of the following examples of usage: allocation of access to the application, limitation or addition of rights to the existing access and deprivation or abolition of rights to access the application. In the case of an organization with few employees, which accordingly uses fewer application for carrying out business processes, ensuring an adequate level of security when carrying out processes for managing access to applications is a simple task. In the case of large organizations like the Tax Administration, these processes are highly complex. At the Tax Administration over 2000 employees have access to and use a large number of internal and external applications. Because of the size of the organization it is necessary to achieve an adequate level of security and to appoint more so-called administrators, who are responsible for managing access to the applications.

The following risks in the field of information security can be identified in the process of allocating rights to applications:

- uncovering a username and password;
- allocating access to an application for a user who usually does not have this right;
- allocating too many access rights or too great an extent of access rights to a user;

- failing to abolish access to an application in a timely, appropriate manner.

It may happen that a username and password are uncovered because of the unintentional actions of an employee who was given access. This may be the result of a failure to consider security processes when giving access to the application (recording, information).

Standards for workplace equipment define outline what an employee needs to carry out everyday tasks. Adequate computer equipment (personal computer or laptop, printer or access to a network printer, and so forth), office equipment and access to applications must be defined. If these standards are not considered, it may happen that an employee is allocated access to applications for which he or she is not authorized; similarly, too many rights may be given in the framework of a single application.

When an employee transfers to a different job or position, access to those applications for which the person is no longer authorized must be cancelled and/or rights for a particular application must be added or abolished in line with the requirements of the new job or position. When an employee leaves the organization, any and all access to the application he or she had been given during his or her time at the organization must be cancelled. Both circumstances imply the need for a centralized system for recording an individual user's access to the application. Failing to do this could result in access not being cancelled simply due to inadequate information. In the case of internal applications, these can be used only by an employee who knows the username and password of the former employee and can thus obtain unauthorized access to the application or unauthorized access to data. In the case of external applications, the former employee himself or herself has access to data even though his or her employment relationship with the organization where he or she was given access no longer exists.

The process is triggered by the following events:

- hiring a new employee;
- transfer of an employee to another job or position;
- request for new access or for the adding or removal of rights to/from existing access and
- termination of an employee's employment relationship.

Informing administrators about personnel and other changes is an important part of the process, as this ensures that employees are given adequate, timely access with adequate rights or are limited or denied, in a timely manner, access and rights which no longer belong to them once their employment relationship has been changed or terminated.

In the event that implementation policy was not adequately defined when analysing the gap or assessing risk, the information security management

system may be considered incomplete. Risk is consequently higher in this field. It was found that through its implementation policy, the Tax Administration has provided an important counterpart to the system for quality management, and in doing so has lowered information and business risks and enhanced the transparency and capabilities of processes.

The paper presents the case of allocating access to applications at the Tax Administration. The discussion highlights how the process should be dealt with as a whole and professionally from the standpoint of information security. It is a complex process that demands of management, administrators and employees responsible behaviour and an awareness of and control over risks and consequences. It follows that the process must be adequately documented. When the process is carried out in accordance with the instructions contained in the implementation policy for information security, risks as well as the likelihood of breaching complexity, access or confidentiality – the main characteristics of a competently implemented system for information security management – are reduced.

We believe that setting up an implementation policy without a main policy would not provide an appropriate basis for an information security management system at the Tax Administration or in organizations in general. Implementation policy represents an important part of the system: without it the system may exist, but it will not be very transparent or manageable. Such systems also fail to address those risks that could be controlled by setting up an implementation policy. Through its main policy and quality guidelines, as well as other internal documents that define controls on documentation, employee information, information security, etc. the Tax Administration has established a system for constant improvement, preventive and corrective measures, innovations and measuring the effects of measures introduced in the fields covered by the implementation policy. The design and introduction of an implementation policy at the Tax Administration was conducted in cooperation with all key factors: employees, administrators, owner of processes and the management. On the level of implementation policy, special emphasis is placed on consistent interaction and compliance with the main policy and potential synergies. Potential non-synergy of the implementing policy presents a new source of risk, and measures will need to be taken accordingly in the process of operations. At the Tax Administration, a further development in this field is aimed at simplifying implementation policy and establishing information support for its performance, measurement, analysis and control.

Setting up an information security management system is the beginning of a long-term process at an organization. Its integration with other management systems is also very important, in so much as such systems have been or will be introduced. Establishing a main policy and local policies and the introduction of an adequate implementation policy are part of the process for ensuring a more adequate level of information security. Organizations also undergo

considerable changes, and the information security management system must keep pace with these changes. This means that changes are reflected in both the main policy and in local policies and on the level of implementation policy. The system of constant improvement dictates, among other things, accordance, active compliance and updating documents, monitoring, analysing and measuring the effects of the introduced measures, including the implementation policy. The experience of introducing an implementation policy at the Tax Administration has shown that in this way, a higher level of quality and operation security, greater understanding of working processes, reduced risk and more effective control over and functioning of the system can be achieved.