

Kontrolni vprašalnik za preverjanje skladnosti s standardom ISO 17799

Ime revizorja: _____

Datum revizije: _____

| Kontrolni seznam za nadzor varnostne politike - standard BS 7799.2:2002 | | | | |
|---|--|--|------------|-----------|
| Povezava s standardom | | Revizijsko področje, namen in vprašanja | Rezultati | |
| Standard | Poglavje | Vprašanje za revizijo | Ugotovitve | Skladnost |
| Varnostna politika | | | | |
| 3.1 | Politika varovanja informacij | | | |
| 3.1.1 | <u>Dokument o politiki varovanja informacij</u> | Ali obstaja politika varovanja informacij, ki je potrjena s strani vodstva podjetja in ustrezno objavljena? Ali so vsi zaposleni seznanjeni s politiko varovanja informacij? Ali je vodstvo podjetja zavezano k uveljavljanju varnostne politike in je vzpostavljen način za nadzor nad izvajanjem varnostne politike? | | |
| 3.1.2 | <u>Pregled in ovrednotenje</u> | Ali ima varnostna politika lastnika, ki skrbi za nadzor in sprotno prilagajanje varnostne politike vsem spreminjajočim se procesom v podjetju? Ali obstajajo postopki za spreminjanje varnostne politike pri spremembah npr. varnostni incident, pojav novih ranljivosti sistema, spremembe v organizacijski ali tehnični infrastrukturi. Ali obstaja zapisan način za pregled in vzdrževanje dokumenta o politiki varovanja vključno z odgovornostmi in datumi pregledov? | | |
| Organiziranost varovanja | | | | |
| 4.1 | Temeljni ustroj varovanja informacij | | | |
| 4.1.1 | <u>Forum za upravljanje varovanja informacij</u> | Ali obstaja upravljalni forum, ki zagotavlja jasne usmeritve in vidno podporo posloводства za uvedbo in sprotno spreminjanje varovanja informacij? Varovanje informacije je poslovna odgovornost vseh članov posloводства. | | |
| 4.1.2 | <u>Usklajevanje varovanja informacij</u> | Ali obstaja forum, ki ga sestavljajo predstavniki vseh delov organizacije, za koordinacijo uveljavljanja varnostne politike in nadzorstev? | | |
| 4.1.3 | <u>Razporejanje odgovornosti za varovanje informacij</u> | Ali so odgovornosti za zaščito posameznih sredstev in izvajanje posebnih varnostnih postopkov jasno določene? | | |
| 4.1.4 | <u>Odobritveni proces za naprave informacijske tehnologije</u> | Ali obstaja postopek v katerem je potrebna odobritev posloводства za nove naprave informacijske tehnologije (poslovna in tehnična odobritev)? Odobritveni proces mora zajemati strojno in programsko opremo. | | |
| 4.1.5 | <u>Svetovanje strokovnjaka za varovanje informacij</u> | Ali obstaja praksa za pomoč z nasvetom strokovnjaka za varovanje informacij, ko je to potrebno? Določiti je potrebno osebo, za koordinacijo pridobljenih znanj in izkušenj, za zagotavljanje pomoči pri odločitvah glede varnostnih vprašanj. | | |
| 4.1.6 | <u>Sodelovanje med organizacijami</u> | Ali obstajajo ustrezne povezave in kontakti z organi, zadolženimi za izvajanje zakonov, s ponudniki računalniških storitev, telekomunikacijskimi ponudniki ... za izmenjavo informacij in hitro pomoč ob varnostnih incidentih? | | |
| 4.1.7 | <u>Neodvisni pregled varovanja informacij</u> | Ali se revizija varnostne politike opravlja neodvisno in v rednih časovnih intervalih? To zagotavlja skladnost varnostne politike z dejanskimi postopki v organizaciji. | | |

| Kontrolni seznam za nadzor varnostne politike - standard BS 7799.2:2002 | | | | |
|--|---|---|-------------------|------------------|
| Povezava s standardom | | Revizijsko področje, namen in vprašanja | Rezultati | |
| Standard | Poglavje | Vprašanje za revizijo | Ugotovitve | Skladnost |
| 4.2 | Varovanje dostopa tretjih strank | | | |
| 4.2.1 | <u>Prepoznavanje tveganja pri stikih s tretjimi strankami</u> | Ali se organizacija zaveda tveganja pri stikih s tretjimi strankami in so uvedeni ustrezni varnostni postopki? Ali so podani upravičeni razlogi za dostop/stik s tretjimi strankami? Ali so vsi dostopi/stiki s tretjimi strankami zabeleženi? | | |
| | | Prepoznavanje tveganja pri delu s pogodbenimi organizacijami ali osebami v organizaciji (on-site). Ali so tveganja predvidena? Ali obstajajo ustrezne kontrole za zmanjševanje tveganja? | | |
| 4.2.2 | <u>Varnostna določila v pogodbah s tretjimi strankami</u> | Ali obstaja formalna pogodba s sklici na vsa potrebna določila, ki zagotavljajo skladnost z varnostnimi usmeritvami in standardi v organizaciji? Pogodba mora biti podpisana preden se omogoči dostop do naprav informacijske tehnologije. | | |
| 4.3 | Zunanji izvajalci (outsourcing) | | | |
| 4.3.1 | <u>Varnostna določila v pogodbah z zunanjimi izvajalci</u> | Ali so v pogodbi s tretjo stranko vsebovana varnostna določila o skladnosti z veljavno zakonodajo, postopki za vzdrževanje in testiranje informacijskih virov, pravica do revizije, postopki fizičnega varovanja, zahtevana razpoložljivost, postopki v primeru katastrofe? | | |
| Razvrstitev in kontrola sredstev | | | | |
| 5.1 | Odgovornost za sredstva | | | |
| 5.1.1 | <u>Popis sredstev</u> | Ali se popis sredstev redno obnavlja z aktualnimi podatki? Ali ima vsako sredstvo svojega lastnika, točno določeno mesto ter določeno in potrjeno varnostno razvrstitev? | | |
| 5.2 | Razvrstitev informacij | | | |
| 5.2.1 | <u>Razvrstitvene smernice</u> | Ali obstajajo navodila in smernice za razvrščanje informacijskih sredstev, kot pomoč pri določanju nivoja zaščite in upravljanju z informacijskimi sredstvi? (Zaupnost, neporočenost, razpoložljivost) | | |
| 5.2.2 | <u>Označevanje in rokovanje z informacijami</u> | Ali so vzpostavljeni postopki za razvrščanje in delo z informacijami v skladu z razvrstitveno shemo v organizaciji? (tiskana poročila, izpisi na zaslonih, razni nosilci podatkov, elektronska sporočila, prenosi datotek, govorna sporočila ...) Ali se razvrstitev informacij redno preverja, da ne prihaja do nepotrebnih dodatnih poslovnih stroškov? Ali obstajajo postopki za uničevanje podatkov? | | |
| Varovanje v zvezi z osebjem | | | | |
| 6.1 | Varovanje pri opredelitvi dela in virov | | | |
| 6.1.1 | <u>Vključevanje varnosti v opisih dela in odgovornosti</u> | Ali so vloge in odgovornosti pri varovanju vključene v opise dela, tako kot so opisane v varnostni politiki organizacije? Opisane morajo biti splošne odgovornosti za izvedbo in vzdrževanje varnostne politike, kot tudi natančno določene odgovornosti ali dodatni varnostni postopki za posamezna sredstva (vire). | | |
| 6.1.2 | <u>Preverjanje osebja</u> | Ali se preverjajo podatki v prošnjah pri zaposlitvi za nedoločen čas, za delavce, ki imajo stik z občutljivimi informacijami? (priporočila, kvalifikacije, zanesljivost ...) | | |
| 6.1.3 | <u>Dogovor o zaupnosti</u> | Ali so vsi zaposleni podpisali ustrezno izjavo o zaupnosti kot del osnovnih pogojev zaposlitve? Ali izjava vsebuje varovanje informacij in premoženja organizacije? | | |

| Kontrolni seznam za nadzor varnostne politike - standard BS 7799.2:2002 | | | | |
|--|---|--|-------------------|------------------|
| Povezava s standardom | | Revizijsko področje, namen in vprašanja | Rezultati | |
| Standard | Poglavje | Vprašanje za revizijo | Ugotovitve | Skladnost |
| 6.1.4 | <u>Odnosi in pogoji zaposlitve</u> | Ali odnosi in pogoji zaposlitve vsebujejo odgovornost zaposlenih za informacijsko varnost? Za določena delovna mesta se preneha odgovornost šele po določenem času, po koncu zaposlitve v organizaciji. | | |
| 6.2 | Usposabljanje uporabnikov | | | |
| 6.2.1 | <u>Izobraževanje in usposabljanje za varovanje informacij</u> | Ali so vsi zaposleni in ostali uporabniki (tretja stranka) seznanjeni oz. poučeni o varovanju informacij in postopkih v organizaciji v rednih časovnih intervalih? | | |
| 6.3 | Ukrepanje ob incidentih in motnjah v delovanju | | | |
| 6.3.1 | <u>Poročanje o incidentih</u> | Ali obstaja točno določen postopek za hitro in učinkovito poročanje o varnostnih incidentih? | | |
| 6.3.2 | <u>Poročanje o pomanjkljivostih varovanja</u> | Ali obstaja točno določen postopek ali navodilo za poročanje o varnostnih pomanjkljivostih ali grožnjah v informacijskih sistemih ali servisih? | | |
| 6.3.3 | <u>Poročanje o motnjah v delovanju programske opreme</u> | Ali obstajajo postopki za poročanje o motnjah v delovanju programske opreme? | | |
| 6.3.4 | <u>Učenje iz preteklih dogodkov</u> | Ali obstajajo mehanizmi za nadzor nad tipom, količino, vrednostjo povzročene izgube posameznih napak ali motnjah v delovanju? Ali obstaja dnevnik napak? | | |
| 6.3.5 | <u>Disciplinski postopek</u> | Ali obstajajo disciplinski postopki za zaposlene, ki kršijo varnostno politiko in postopke predpisane v organizaciji? Ti postopki lahko delujejo preventivno. | | |
| Fizično in okolno varovanje | | | | |
| 7.1 | Varovano območje | | | |
| 7.1.1 | <u>Fizični varnostni pas</u> | Katere strateško postavljene fizične pregrade ščitijo informacijske procese? Primeri zaščite so avtomatska vrata ščitena z magnetno ali brezkontaktno kartico, vratar na vhodu, primerno zavarovane stene... | | |
| 7.1.2 | <u>Kontrole fizičnega vstopa</u> | Tip kontrol uporabljenih za nadzor prehoda avtoriziranega osebja med varovanimi območji v podjetju. | | |
| 7.1.3 | <u>Varovanje pisarn in računalniških prostorov</u> | Ali so pisarne in območja kjer je možen dostop do zaupnih informacij ali instalirana informacijska oprema za zagotavljanje storitev ali obdelavo podatkov ustrezno zaščitena (ključavnice, predali s ključavnicami, sefi)? | | |
| | | Ali je procesno informacijski servis ustrezno zavarovan proti naravnim in ostalim katastrofam? | | |
| | | Ali obstaja grožnja iz sosednjih prostorov? | | |
| 7.1.4 | <u>Delo v varovanih območjih</u> | Informacije morajo biti na voljo po principu potrebe (dostop do informacij, ki jih oseba potrebuje pri svojem delu). Ali obstajajo varnostne kontrole za tretje osebe in zaposlene v varnostnih območjih? | | |
| 7.1.5 | <u>Ločena območja za dostavo in odpremo podatkov</u> | Ali so dostavna območja ločena in ustrezno zaščitena, tako da se prepreči neavtoriziran dostop do podatkov? | | |
| | | Ali je opravljena analiza tveganja za vzpostavitev ustrezne varnosti na območjih dostave in odpreme informacij? | | |
| 7.2 | Varovanje opreme | | | |
| 7.2.1 | <u>Nameščanje zaščitene opreme</u> | Ali je postavitve opreme takšna, da lahko zmanjšamo nepotreben dostop do delovnega območja? | | |
| | | Ali so predmeti, viri ali sredstva, ki zahtevajo posebno varovanje ustrezno izolirani (osamljeni), da lahko zmanjšamo obseg potrebne splošne zaščite? | | |

| Kontrolni seznam za nadzor varnostne politike - standard BS 7799.2:2002 | | | | |
|--|--|---|-------------------|------------------|
| Povezava s standardom | | Revizijsko področje, namen in vprašanja | Rezultati | |
| Standard | Poglavje | Vprašanje za revizijo | Ugotovitve | Skladnost |
| | | Ali obstajajo kontrole za zmanjšanje tveganj kot so kraja, požar, eksplozije, dim, poplava, prah, vibracije, kemični učinki, voda, prekinitvev preskrbe z električno energijo, elektromagnetna radiacija ...? | | |
| | | Ali obstaja politika o prepovedi kajenja, pitja in uživanja hrane v prostorih z računalniško opremo? | | |
| | | Ali obstaja okoliški nadzor za tveganja, ki lahko ogrozijo delovanje informacijskega sistema (membranske tipkovnice, sosednji prostori ...)? | | |
| 7.2.2 | <u>Preskrba z energijo</u> | Ali obstaja zaščita računalniške opreme pred prekinitvami električnega toka kot so dvojno napajanje, neprekinjevalni električni napajalnik (UPS), rezervni generator? Ali se sistem za neprekinjeno oskrbo z električno energijo testira v rednih časovnih intervalih? | | |
| 7.2.3 | <u>Varovanje kablskih vodov</u> | Ali so napajalni in telekomunikacijski kabli zaščiteni pred prestrežanjem informacij ali poškodbami? | | |
| | | Ali obstajajo dodatni varnostni mehanizmi za zaščito posebej občutljivih in pomembnih informacij? | | |
| 7.2.4 | <u>Vzdrževanje opreme</u> | Ali je oprema vzdrževana v skladu s proizvajalčevimi priporočili glede časov in načina vzdrževanja? Ali popravila in servisiranje opreme opravlja za to pooblaščen osebje? | | |
| | | Ali je vzpostavljeno beleženje vseh napak ali sumov o napakah in ustreznih postopkov za odpravo napak? | | |
| | | Ali obstajajo ustrezne kontrole za opremo, ki jo pošiljamo iz organizacije (popravilo, nadgradnja ...)? Ali je oprema zavarovana? Ali so zavarovalne zahteve izpolnjene? | | |
| 7.2.5 | <u>Varovanje opreme zunaj prostorov organizacije</u> | Ali obstajajo postopki za odobritev uporabe opreme zunaj prostorov organizacije (pooblastila vodstva)? Ali je stopnja varnostne zaščite za opremo, ki jo uporabljamo zunaj prostorov organizacije enaka ali večja kot v organizaciji? | | |
| 7.2.6 | <u>Zanesljivo izločanje ali ponovna uporaba opreme</u> | Ali so občutljivi podatki shranjeni na nosilcih podatkov fizično uničeni ali prepisani po prenehanju ali ponovni uporabi opreme za druge namene? | | |
| 7.3 | Splošne kontrole | | | |
| 7.3.1 | <u>Politika prazne mize in ekrana</u> | Ali je vključeno avtomatsko zaklepanje računalniškega zaslona? Ali obstajajo navodila zaposlenim o hranjenju zaupnih dokumentov (tiskani dokumenti, mediji) na varnem mestu? | | |
| 7.3.2 | <u>Iznos stvari, ki so last organizacije</u> | Ali je za iznos stvari (informacije, programska oprema), ki so last organizacije potrebno posebno dovoljenje? | | |
| | | Ali obstajajo redni revizijski postopki in kontrole za odkrivanje neavtoriziranega iznosa stvari? Ali so zaposleni seznanjeni o kontrolah in revizijskih postopkih omenjenih zgoraj? | | |
| Komunikacijsko in obratovalno upravljanje | | | | |
| 8.1 | Obratovalni postopki in odgovornosti | | | |
| 8.1.1 | <u>Dokumentirani obratovalni postopki</u> | Ali obstajajo jasni obratovalni postopki za vse računalniške sisteme v obratovanju (izdelava varnostnih kopij, vzdrževanje opreme ...)? Ali so ti postopki ustrezno dokumentirani in se uporabljajo v vsakodnevni opravilih? | | |

| Kontrolni seznam za nadzor varnostne politike - standard BS 7799.2:2002 | | | | |
|--|--|--|-------------------|------------------|
| Povezava s standardom | | Revizijsko področje, namen in vprašanja | Rezultati | |
| Standard | Poglavje | Vprašanje za revizijo | Ugotovitve | Skladnost |
| 8.1.2 | <u>Spreminjanje obratovalnih postopkov</u> | Ali se kakršnakoli sprememba obratovalnih postopkov ustrezno preveri in odobri? Vse spremembe v produkcijskem okolju mora potrditi pristojno vodstvo oz. lastnik sredstva. | | |
| | | Ali obstajajo revizijske sledi za vsako spremembo v produkcijskem okolju (programska oprema)? | | |
| 8.1.3 | <u>Postopki ravnanja ob incidentih</u> | Ali obstajajo postopki za ravnanje v slučaju varnostnih incidentov? | | |
| | | Ali postopki omogočajo hitro in učinkovito ukrepanje? | | |
| | | Ali postopki zajemajo različne vrste varnostnih incidentov (zastoj sistema, kršitev zaupnosti, ...)? | | |
| | | Ali se zabeleženi dogodki o varnostnih incidentih redno pregledujejo? Ali sledijo pregledom preventivni ukrepi za preprečevanje podobnih varnostnih incidentov? | | |
| 8.1.4 | <u>Ločevanje nalog</u> | Ali so naloge in področja dela ustrezno ločene, tako, da se zmanjša nevarnost zlorabe zaradi nepazljivosti ali zlonamernih dejanj? Če ločevanje nalog ni mogoče, je potrebno zagotoviti dodatne kontrole. | | |
| 8.1.5 | <u>Ločitev razvojnih in obratovalnih naprav</u> | Ali obstaja ločitev razvojnih in obratovalnih naprav? Razvojna programska oprema mora uporabljati drugo računalniško opremo kot programska oprema v obratovanju. | | |
| 8.1.6 | <u>Zunanje ravnanje z napravami</u> | Ali se za upravljanje z računalniškimi napravami ali omrežjem uporablja servis zunanjega pogodbenika – tretje stranke? | | |
| | | Ali so ugotovljena tveganja, ter sprejeti ustrezni ukrepi in kontrole za delo pogodbenih partnerjev (pogoji zapisani v pogodbi)? Ali je pridobljena odobritev lastnikov poslovnih in uporabniških rešitev? | | |
| 8.2 | Načrtovanje in prevzem sistema | | | |
| 8.2.1 | <u>Načrtovanje zmogljivosti</u> | Ali se spremljajo zmogljivostne zahteve? Ali se glede na trenutno obremenitev in projekcije zahtev planira nakup novih sredstev? Nadzor kapacitete diskovnega polja, spomina, procesorskega časa, tiskalnikov, komunikacijskih sistemov... | | |
| 8.2.2 | <u>Prevzem sistema</u> | Ali so določena merila za prevzem novega sistema, ali nadgradnje sistema? Ali so bili opravljeni ustrezni testi pred prevzemom sistema? | | |
| 8.3 | Zaščita pred zlonamerno programsko opremo | | | |
| 8.3.1 | <u>Kontrole proti zlonamerni programski opremi</u> | Ali obstajajo kontrole proti uporabi zlonamerne programske opreme? Ali varnostna politika vsebuje določilo o prepovedani uporabi neavtorizirane programske opreme? | | |
| | | Ali obstajajo postopki za preverjanje točnosti informacij o zlonamerni programski opremi pridobljenih preko različnih virov (internet, obvestila, protivirusni programi...)? | | |
| | | Ali je na računalnikih instalirana protivirusna zaščita? Ali se podatki o novi zlonamerni programski opremi obnavljajo v rednih časovnih intervalih? | | |
| | | Ali se preverja ves promet iz omrežij in virov, ki jim ne zaupamo? Preverjanje elektronske pošte in priponk, promet iz internet omrežja, diskete,... | | |

| Kontrolni seznam za nadzor varnostne politike - standard BS 7799.2:2002 | | | | |
|--|--|--|-------------------|------------------|
| Povezava s standardom | | Revizijsko področje, namen in vprašanja | Rezultati | |
| Standard | Poglavje | Vprašanje za revizijo | Ugotovitve | Skladnost |
| 8.4 | Skrbnišтво | | | |
| 8.4.1 | <u>Rezervna kopija podatkov</u> | Ali se redno izdeluje rezervna kopija pomembnih poslovnih podatkov, kritičnih strežnikov, konfiguracije komunikacijske opreme, ...? Inkrementalne kopije in popolna varnostna kopija. Ali so rezervne kopije podatkov shranjene varno in na ločenem kraju? Ali se rezervni podatki redno preskušajo, da zagotovimo njihovo zanesljivost za morebitno uporabo v sili? | | |
| 8.4.2 | <u>Dnevnik obratovanja</u> | Ali računalniški operaterji vodijo dnevnik vsega dela, ki se opravlja? (ime osebe, napake, ukrepi, ...) Ali se dnevnik obratovanja redno in neodvisno preverjajo glede na predpisane obratovalne postopke? | | |
| 8.4.3 | <u>Beleženje napak</u> | Ali so napake zabeležene in ustrezno obravnavane? Pregled zabeleženih napak in ukrepov za odpravo napak. | | |
| 8.5 | Ravnanje z omrežjem | | | |
| 8.5.1 | <u>Kontrole omrežja</u> | Ali so zagotovljene učinkovite kontrole kot so ločitev odgovornosti za obratovanje omrežja in obratovanje računalnikov? Ali je uvedena odgovornost in postopki za ravnanje z oddaljeno opremo in opremo v uporabnikovih prostorih? Ali obstajajo posebne kontrole za varovanje zaupnosti in neoporečnosti podatkov, ki se prenašajo po javnih omrežjih in za zaščito povezanih sistemov? (VPN, kriptiranje, ...) | | |
| 8.6 | Ravnanje z nosilci podatkov in varovanje | | | |
| 8.6.1 | <u>Ravnanje z zamenljivimi računalniškimi nosilci podatkov</u> | Ali obstajajo postopki za ravnanje z zamenljivimi računalniškimi nosilci podatkov (diskete, magnetni trakovi, spominske kartice, CD, ...) in tiskanimi poročili? | | |
| 8.6.2 | <u>Izločanje nosilcev podatkov</u> | Ali se računalniški nosilci podatkov izločajo zanesljivo in varno, ko niso več potrebni? Ali se izločanje občutljivih postavk beleži v dnevnik za kasnejše vpogled in revizijsko sled? | | |
| 8.6.3 | <u>Postopki rokovanja z informacijami</u> | Ali obstajajo postopki za rokovanje z informacijami? Ali je v postopkih opredeljena zaščita informacij pred nepooblaščenim razkritjem ali zlorabo? | | |
| 8.6.4 | <u>Varovanje dokumentacije sistema</u> | Ali je dokumentacija sistema ustrezno zaščiten pred nepooblaščenim dostopom? Ali je dostop do dokumentacije sistema omejen na najmanjšo možno mero po razdelilniku (seznamu), ki ga mora potrditi lastnik uporabniške rešitve? | | |
| 8.7 | Izmenjevanje informacij in programske opreme | | | |
| 8.7.1 | <u>Dogovori o izmenjevanju informacij in programske opreme</u> | Ali obstaja formalen dogovor za izmenjavo informacij in programske opreme med organizacijami? Ali dogovor opredeljuje varovanje poslovnih informacij glede na občutljivost in pomembnost informacij? | | |
| 8.7.2 | <u>Varovanje prenosnega medija</u> | Ali je pri prenosu podatkov upoštevana varnost prenosnega medija? Ali je medij zadostno zaščiten pred navtoriziranim dostopom, zlorabo ali spreminjanjem? | | |
| 8.7.3 | <u>Varovanje elektronskega poslovanja</u> | Ali je zaščita uporabljena pri elektronskem poslovanju zadostna? (Zaščita pred poneverbami, nezatajlivost, razkritje ali zloraba informacij, ...) | | |

| Kontrolni seznam za nadzor varnostne politike - standard BS 7799.2:2002 | | | | |
|---|--|--|------------|-----------|
| Povezava s standardom | | Revizijsko področje, namen in vprašanja | Rezultati | |
| Standard | Poglavje | Vprašanje za revizijo | Ugotovitve | Skladnost |
| | | Ali so varnostne kontrole, kot so autentikacija, avtorizacija, del elektronskega poslovanja? | | |
| | | Ali je med partnerji, ki poslujejo preko elektronskega poslovanja sklenjena ustrežna pogodba, ki zavezuje obe strani k zapisanim določilom vključno z varnostnimi zadevami? | | |
| 8.7.4 | <u>Varovanje elektronske pošte</u> | Ali obstaja varnostna politika o uporabi elektronske pošte? Potrebno je zmanjšati vse poslovne in fizične nevarnosti, ki se pojavijo z uporabo elektronske pošte. | | |
| | | Ali obstajajo kontrole in postopki za protivirusno pregledovanje, izločanje potencialno nevarnih priponk, ranljivost na napake kot so napačno naslavljanje ali usmerjanje, ...? | | |
| 8.7.5 | <u>Varovanje elektronskih pisarniških sistemov</u> | Ali obstajajo jasne usmeritve in določila za varovanje in uporabo elektronskih pisarniških sistemov? | | |
| | | Ali obstajajo navodila za učinkovito kontrolo in obvladovanje poslovnih in fizičnih nevarnosti, ki se pojavljajo v elektronskih pisarniških sistemih? | | |
| 8.7.6 | <u>Javno dostopni sistemi</u> | Ali obstaja formalen način avtorizacije za vse informacije, ki so javno dostopne? | | |
| | | Ali obstajajo kontrole za ohranjanje celosti informacij, ki so javno dostopne pred navtoriziranim dostopom? (Požarni zidovi, nastavitve operacijskega sistema, sistemi za odkrivanje vdorov – IDS, opazovanje delovanja sistemov, ...) | | |
| 8.7.7 | <u>Druge oblike izmenjave informacij</u> | Ali obstajajo postopki in kontrole za zaščito izmenjave informacij preko govornih, faksimilnih, slikovnih komunikacijskih poti? | | |
| | | Ali so vsi zaposleni seznanjeni s postopki ohranjanja zaupnosti občutljivih informacij pri izmenjevanju informacij? | | |
| Dostop do sistema | | | | |
| 9.1 | Poslovne zahteve za dostop do sistema | | | |
| 9.1.1 | <u>Politika obvladovanja dostopa</u> | Ali so poslovne zahteve za obvladovanje dostopa opredeljene in dokumentirane? Politika razpečevanja informacij naj upošteva načelo "kdo mora vedeti". | | |
| | | Ali politika obvladovanja dostopa določa pravice in pravila za uporabniške skupine in posamezne uporabnike? | | |
| | | Ali so uporabniki in ponudniki storitev seznanjeni s poslovnimi zahtevami glede obvladovanja dostopa? | | |
| 9.2 | Ravnanje z uporabniškim dostopom | | | |
| 9.2.1 | <u>Vpisovanje uporabnika</u> | Ali obstajajo formalni postopki za vpis in izbris ter dodeljevanje pravic uporabniku v večuporabniškem okolju informacijske tehnologije? | | |
| 9.2.2 | <u>Ravnanje s posebnimi pravicami</u> | Ali je dodelitev posebnih pravic v večuporabniškem okolju informacijske tehnologije omejena in ustrezno kontrolirana? Posebne pravice je potrebno dodeliti po principu "kdo potrebuje dostop" in po formalnem avtorizacijskem postopku. | | |
| 9.2.3 | <u>Ravnanje z uporabniškimi gesli</u> | Ali je dodeljevanje in spreminjanje gesel del formalnega upravljanja informacijskega sistema? | | |
| | | Ali so uporabniki podpisali dogovor, da bodo osebna gesla obravnavali zaupno in razkrivali gesla za delo skupine samo članom te skupine? | | |
| 9.2.4 | <u>Pregled uporabniških pravic dostopa</u> | Ali obstaja postopek za reden pregled uporabniških pravic dostopa? (pooblastila za posebne pravice vsake 3 mesece, ostalo vsakih 6 mesecev) | | |

| Kontrolni seznam za nadzor varnostne politike - standard BS 7799.2:2002 | | | | |
|---|--|---|------------|-----------|
| Povezava s standardom | | Revizijsko področje, namen in vprašanja | Rezultati | |
| Standard | Poglavje | Vprašanje za revizijo | Ugotovitve | Skladnost |
| 9.3 | Odgovornosti uporabnika | | | |
| 9.3.1 | <u>Uporaba gesel</u> | Ali obstajajo navodila za pomoč pri izbiri in upravljanju z gesli? | | |
| 9.3.2 | <u>Oprema brez prisotnosti uporabnika</u> | Ali so uporabniki in pogodbeniki seznanjeni z varnostnimi zahtevami in postopki za varovanje opreme brez prisotnosti uporabnika, kakor tudi s svojimi odgovornostmi za uvajanje takšne zaščite? Primer: odjava iz sistema takoj ko je delo opravljeno, povezava z osrednjim računalnikom se prekine takoj, ko je obdelava končana, ... | | |
| 9.4 | Obvladovanje mrežnega dostopa | | | |
| 9.4.1 | <u>Politika uporabe mrežnih storitev</u> | Ali obstaja politika uporabe mrežne infrastrukture in mrežnih storitev kot so: dostopna omrežja oz. deli omrežja, avtorizacijski postopki za ugotavljanje pravic, postopki za zaščito dostopa do mrežnih storitev, ...? | | |
| 9.4.2 | <u>Vsiljena pot</u> | Ali obstajajo kontrole, ki omejujejo pot med uporabniškim terminalom in računalniškimi storitvami, za katere ima uporabnik pooblastilo dostopa (vsiljena pot za zmanjšanje nevarnosti nepooblaščenega dostopa)? | | |
| 9.4.3 | <u>Overjanje uporabnikov</u> | Ali obstaja avtentikacijski mehanizem za overjanje uporabnikov, ki uporabljajo zunanje povezave? (tehnike šifriranja in tajnopisja, uporaba pametnih kartic, overjanja preko sistema izzivi/odgovor, ...) | | |
| 9.4.4 | <u>Overjanje vozlišča</u> | Ali se overjajo vse povezave z oddaljenimi računalniškimi sistemi? Overjanje vozlišča lahko služi kot druga, cenejša rešitev za overjanje skupin oddaljenih uporabnikov, ki so povezani z zavarovano, večuporabniško računalniško napravo. | | |
| 9.4.5 | <u>Zaščita oddaljenih diagnostičnih vrat</u> | Ali je dostop do diagnostičnih vrat (diagnostic ports) zavarovan z ustreznim varnostnim mehanizmom? | | |
| 9.4.6 | <u>Ločevanje v omrežjih</u> | Ali v omrežju obstaja več logičnih območij, ki so opredeljena z varnostnimi pasovi in povezana med sabo s požarnim zidom? | | |
| 9.4.7 | <u>Obvladovanje omrežnih povezav</u> | Ali obstajajo kontrole za omejevanje možnosti uporabnikov, za podporo poslovnih uporabniških rešitev, ki se izvajajo na skupnih omrežjih, zlasti tistih, ki segajo prek mej organizacije? (elektronska pošta, spletni promet, prenos datotek, ...) | | |
| 9.4.8 | <u>Obvladovanje omrežnega usmerjanja</u> | Ali so v skupnih omrežjih vključene kontrole usmerjanja, ki zagotavljajo, da računalniške povezave in informacijski tokovi ne kršijo politike dostopa do poslovnih uporabniških storitev? Pomembno predvsem za omrežja, ki so skupna z uporabniki tretjega partnerja (zunaj organizacijskega). | | |
| | | Ali kontrole usmerjanja temeljijo na prepoznavanju pošiljatelja in namembnega naslova? | | |
| 9.4.9 | <u>Varovanje omrežnih storitev</u> | Ali obstajajo jasni opisi varnostnih značilnosti vseh uporabljenih omrežnih storitev tako javnih kot zasebnih? | | |
| 9.5 | Obvladovanje dostopa do operacijskega sistema | | | |
| 9.5.1 | <u>Samodejno prepoznavanje terminalov</u> | Ali je uporabljeno samodejno prepoznavanje terminalov za overjanje povezav? Pomembno pri uporabniških rešitvah kjer se izvajanje lahko začne samo iz določenega mesta. | | |
| 9.5.2 | <u>Postopki prijavljanja na terminalu</u> | Ali je dostop do storitev informacijske tehnologije mogoč samo po opravljenem zanesljivem prijavnem postopku? | | |
| | | Ali postopek prijave v računalniški sistem zasnovan tako, da kar najbolj zmanjšuje možnost nepooblaščenega dostopa? | | |

| Kontrolni seznam za nadzor varnostne politike - standard BS 7799.2:2002 | | | | |
|--|---|---|-------------------|------------------|
| Povezava s standardom | | Revizijsko področje, namen in vprašanja | Rezultati | |
| Standard | Poglavje | Vprašanje za revizijo | Ugotovitve | Skladnost |
| 9.5.3 | <u>Prepoznavanje in overjanje uporabnikov</u> | Ali ima vsak uporabnik vključno z operaterjem, sistemskim administratorjem, ... edinstven osebni identifikator izključno za osebno uporabo? Uporaba skupinskega uporabniškega imena se lahko uporablja samo v izjemnih okoliščinah, ko za to obstaja jasna poslovna korist. V tem primeru je potrebno uvesti dodatne kontrole. | | |
| | | Ali avtentikacijska metoda zagotavlja zanesljivo potrditev uporabljenega uporabniškega imena? (uporaba gesla, ki ga pozna samo uporabnik, biometrične metode, ...) | | |
| 9.5.4 | <u>Sistem ravnanja z geslom</u> | Ali obstaja učinkovit sistem ravnanja z gesli, ki zagotavlja kakovost gesel? (geslo za vsakega uporabnika, redno spreminjanje gesla, hranjenje gesel v šifrirani obliki, hranjenje že uporabljenih gesel, ni prikazovanja gesla na zaslonu, ...) | | |
| 9.5.5 | <u>Uporaba sistemskih podpornih programov</u> | Ali je uporaba sistemskih podpornih programov, ki so del operacijskega sistema, strogo nadzorovana? Sistemski podporni programi lahko obidejo varnostne kontrole. | | |
| 9.5.6 | <u>Alarm zaradi nasilja za varovanje uporabnikov</u> | Ali so uporabniki, ki bi lahko bili tarča nasilja opremljeni z alarmom zaradi nasilja? | | |
| 9.5.7 | <u>Izključevanje terminalov</u> | Ali se nedejavni terminali na javnih ali zunanjih mestih samodejno izključijo po določenem času nedejavnosti, da se prepreči dostop nepooblaščenih oseb? | | |
| 9.5.8 | <u>Omejevanje časa priključitve</u> | Ali obstaja omejevanje časa priključitve za uporabniške rešitve z velikim tveganjem? (omejevanje časovnih razdelkov za paketne prenose datotek, omejevanje časa povezave na normalni delovni čas, ...) | | |
| 9.6 | Obvladovanje dostopa do uporabniških rešitev | | | |
| 9.6.1 | <u>Omejevanje dostopa do informacij</u> | Ali je dostop do podatkov in opravil uporabniške rešitve omejen na skupine ali posamezne uporabnike skladno z organizacijsko politiko dostopa do informacij na temelju potreb posamezne poslovne uporabniške storitve? | | |
| 9.6.2 | <u>Osamitev občutljivih sistemov</u> | Ali imajo občutljivi sistemi namensko (osamljeno) računalniško okolje? Izvajanje uporabniške rešitve na namenskem računalniku, delitev opreme samo s sistemi, ki jim zaupamo, ... | | |
| 9.7 | Spremljanje dostopa do sistema in njegove uporabe | | | |
| 9.7.1 | <u>Beleženje dogodkov</u> | Ali se revizijske sledi z zapisom odmikov in drugih za varnost pomembnih dogodkov izdelujejo in hranijo za dogovorjeno obdobje zato, da so lahko v pomoč v kasnejših raziskavah in pri spremljanju kontrole dostopa? | | |
| 9.7.2 | <u>Spremljanje uporabe sistema</u> | Ali so uveljavljeni postopki za spremljanje uporabe informacijskega sistema? Postopki so potrebni za zagotavljanje, da uporabniki izvajajo samo to, za kar so bili izrecno pooblašteni. | | |
| | | Ali se rezultati spremljanja uporabe informacijskega sistema redno pregledujejo? | | |
| 9.7.3 | <u>Sinhronizacija ure</u> | Ali je računalniška ura naravnana na dogovorjeni standard npr. zahodnoevropski čas (GMT) ali na krajevni čas? Točna nastavitve ure je pomembna za zagotavljanje popolnosti dnevnikov za potrebe revizije. | | |
| 9.8 | Prenosne računalniške naprave in oddaljeno delo (Mobile computing and teleworking) | | | |
| 9.8.1 | <u>Prenosne računalniške naprave</u> | Ali obstaja formalna politika ki zajema nevarnosti pri delu s prenosnimi računalniki, osebnimi organizatorji, posebno v nezavarovanem okolju? | | |

| Kontrolni seznam za nadzor varnostne politike - standard BS 7799.2:2002 | | | | |
|--|---|--|-------------------|------------------|
| Povezava s standardom | | Revizijsko področje, namen in vprašanja | Rezultati | |
| Standard | Poglavje | Vprašanje za revizijo | Ugotovitve | Skladnost |
| | | Ali so uporabniki, ki uporabljajo prenosne računalniške naprave, dodatno izobraženi in opozorjeni na dodatne nevarnosti pri delu s temi napravami in postopki ter kontrolami za zmanjšanje teh nevarnosti? | | |
| 9.8.2 | <u>Oddaljeno delo</u> | Ali obstajajo postopki, politika in/ali standard za kontrolo oddaljenega dela? Politika mora biti skladna z obstoječo varnostno politiko organizacije. | | |
| | | Ali obstaja ustrezna zaščita oddaljenega delovnega mesta? Zaščita pred krajo opreme, navtorizirano razkritje podatkov, potrebno je določiti okolje za oddaljeno delo, ... | | |
| Razvijanje in vzdrževanje sistemov | | | | |
| 10.1 | Varnostne zahteve sistemov | | | |
| 10.1.1 | <u>Analiza in specifikacija varnostnih zahtev</u> | Ali ugotovitve poslovnih zahtev za nove rešitve ali razširitve obstoječih rešitev podrobno opredeljujejo zahteve za varnostne kontrole? Zahteve po varovanju in varnostne kontrole naj odsevajo poslovno vrednost ustreznih informacijskih sredstev in možno poslovno škodo. | | |
| | | Ali je ocenitev nevarnosti zaključena, pred pričetkom razvoja novega sistema? | | |
| 10.2 | Varovanje v uporabniških sistemih | | | |
| 10.2.1 | <u>Potrjevanje vhodnih podatkov</u> | Ali se vhodni podatki v uporabniških rešitvah potrjujejo, da zagotovimo njihovo pravilnost in ustreznost? Ali so upoštevane kontrole kot so preverjanje vhodnih podatkov, postopki za ravnanje pri napakah potrjevanja, opredelitev odgovornosti vsega osebja vključenega v vnašanje podatkov, ... | | |
| 10.2.2 | <u>Kontrola notranjih obdelav</u> | Ali so v obdelave vključene kontrole za ugotavljanje napak v obdelovanju ali namerno spreminjanje podatkov? Ali so ugotovljene možne nevarnosti za pojav napak pri obdelavah podatkov? | | |
| | | Ali obstajajo kontrole za zmanjšanje nevarnosti pri obdelavi podatkov? Uporabljene kontrole so odvisne od programske opreme in vpliva na poslovni proces pri popačenju podatkov. | | |
| 10.2.3 | <u>Overjanje sporočil</u> | Ali je overjanje sporočil uporabljeno pri rešitvah, kjer je ključnega pomena zaščita neoporečnosti vsebine? Oceniti je potrebno varnostno tveganje, da opredelimo ali je potrebno overjanje sporočil in kakšen je najprimernejši način izvedbe. Overjanje sporočil je metoda, ki se uporablja za ugotavljanje nepooblaščenih sprememb ali okvar v vsebini prenesenih sporočil. | | |
| 10.2.4 | <u>Potrjevanje izhodnih podatkov</u> | Ali so izhodni podatki potrjeni tako, da zagotavljajo pravilno obdelovanje podatkov? Ali so izhodni podatki smiselni, preverjanje obdelave vseh podatkov, opredelitev odgovornosti osebja vključenega v kontrolo izhodnih podatkov? | | |
| 10.3 | Kontrole šifriranja | | | |
| 10.3.1 | <u>Politika za uporabo šifrirnih kontrol</u> | Ali obstaja politika za uporabo šifrirnih kontrol za zaščito informacij? Ali nivo zaščite informacij temelji na osnovi klasifikacije občutljivosti podatkov? | | |
| 10.3.2 | <u>Šifriranje</u> | Ali so uporabljene tehnike šifriranja za zaščito podatkov? Ali nivo šifriranja podatkov temelji na oceni občutljivosti in zahtevani zaščiti podatkov? | | |

| Kontrolni seznam za nadzor varnostne politike - standard BS 7799.2:2002 | | | | |
|--|--|--|-------------------|------------------|
| Povezava s standardom | | Revizijsko področje, namen in vprašanja | Rezultati | |
| Standard | Poglavje | Vprašanje za revizijo | Ugotovitve | Skladnost |
| 10.3.3 | <u>Digitalni podpis</u> | Ali je z uporabo digitalnega podpisa zaščitena celovitost in verodostojnost elektronskih dokumentov? | | |
| 10.3.4 | <u>Nezatajlivost</u> | Ali je storitev nezatajivosti uporabljena v vseh primerih, kjer bi lahko prišlo do oporekanja določenega dogodka ali opravila npr. zanikanje opravljenega elektronskega plačila, oporekanje elektronsko podpisani pogodbi, ... ? | | |
| 10.3.5 | <u>Upravljanje s ključi</u> | Ali obstaja sistem upravljanja za podporo šifrirnih mehanizmov kot je šifriranje z skritim ključem in šifriranje z javnim ključem? | | |
| | | Ali se za upravljanje s ključi uporabljajo standardni postopki in uveljavljen sistem? (generiranje in pridobivanje javnih ključev, shranjevanje ključev, postopki ob razkritju ključev, varnostne kopije ključev, ...) | | |
| 10.4 | Varovanje datotek v računalniških sistemih | | | |
| 10.4.1 | <u>Obvladovanje programske opreme v obratovanju</u> | Ali obstajajo kontrole za uvedbo programske opreme v obratovanje? Kontrole so potrebne za zmanjšanje nevarnosti okvare sistemov v obratovanju. | | |
| 10.4.2 | <u>Zaščita preskusnih podatkov sistema</u> | Ali so preskusni podatki ustrezno zaščiteni? Pred uporabo dejanskih podatkov, ki vsebujejo osebne podatke je potrebno vse podatke spremeniti. | | |
| 10.4.3 | <u>Kontrola dostopa do knjižnic z izvorno kodo</u> | Ali obstajajo natančne kontrole za dostop do knjižnic z izvorno kodo? Te kontrole zmanjšujejo možnost neodobrenega spreminjanja računalniških programov. | | |
| 10.5 | Varovanje razvojnega in vzdrževalnega procesa | | | |
| 10.5.1 | <u>Postopki obvladovanja sprememb</u> | Ali obstajajo natančni kontrolni postopki za uvajanje sprememb v informacijskem sistemu? Obvladovanje uvajanja sprememb je potrebno za zmanjševanje okvar na informacijskih sistemih. | | |
| 10.5.2 | <u>Tehnični pregled sprememb v operacijskem sistemu</u> | Ali obstajajo postopki za pregled in testiranje uporabniških sistemov po spremembi operacijskega sistema (instalacija popravkov, nadgradnja sistema, ...)? | | |
| 10.5.3 | <u>Omejevanje sprememb pri paketih programske opreme</u> | Ali obstajajo priporočila, ki omejujejo spremembe pri paketih splošno uporabne programske opreme? Kolikor je mogoče in izvedljivo, bi morali pakete programske opreme uporabljati brez spreminjanja. Če so spremembe nujne, moramo originalno programsko opremo zadržati in opraviti spremembe na jasno označeni kopiji. Spremembe je potrebno preskusiti in dokumentirati. | | |
| 10.5.4 | <u>Skrite poti in trojanska koda</u> | Ali obstajajo kontrole, ki zagotavljajo, da pri razvoju/izvedbi novega informacijskega sistema ni skritih poti (dostop do sistema po nedokumentirani poti) ali trojanske kode? | | |
| 10.5.5 | <u>Razvoj programske opreme z zunanjimi izvajalci</u> | Ali obstajajo kontrole za nadzor razvoja programske opreme z zunanjimi izvajalci? Licenčne pogodbe, garancijska listina - escrow, pogodbeno obveznost za zagotavljanje kvalitete, testiranje pred instalacijo programske opreme za odkrivanje skrite kode - trojanske kode, ... | | |
| Načrtovanje neprekinjenega poslovanja | | | | |
| 11.1 | Vidiki načrtovanja neprekinjenega poslovanja | | | |
| 11.1.1 | <u>Proces načrtovanja neprekinjenega poslovanja</u> | Ali je vzpostavljen in upravljan proces razvijanja in vzdrževanja načrtov neprekinjenega poslovanja po vsej organizaciji? Ugotavljanje in zmanjševanje namernih ali slučajnih groženj ključnim storitvam, redno preizkušanje načrtov, izobraževanje osebja za izvajanje dogovorjenih izrednih ukrepov in postopkov... | | |

| Kontrolni seznam za nadzor varnostne politike - standard BS 7799.2:2002 | | | | |
|--|---|--|-------------------|------------------|
| Povezava s standardom | | Revizijsko področje, namen in vprašanja | Rezultati | |
| Standard | Poglavje | Vprašanje za revizijo | Ugotovitve | Skladnost |
| 11.1.2 | <u>Neprekinjeno poslovanje in analiza posledic</u> | Ali so prepoznani dogodki, ki lahko povzročijo prekinitev poslovnega procesa? (odpoved strojne opreme, ogenj, ...) Ali je narejena analiza tveganj, ki opredeljuje posledice teh dogodkov? Ali strateški plan izhaja iz analize tveganj, tako da upošteva celovit pristop za neprekinjeno poslovanje? | | |
| 11.1.3 | <u>Pisanje in uveljavljanje načrta neprekinjenega poslovanja</u> | Ali načrti za neprekinjeno poslovanje upoštevajo časovni okvir v katerem mora poslovni proces ponovno delovati? Ali se načrt neprekinjenega poslovanja redno preskuša in dopolnjuje? | | |
| 11.1.4 | <u>Okvir načrtovanja neprekinjenega poslovanja</u> | Ali obstaja enoten okvir načrtov neprekinjenega poslovanja? Ali se okvir načrtov redno vzdržuje, da zagotovimo skladnost in istovetnost prioritet za preskušanje in vzdrževanje? Ali so pogoji za uveljavitev, kakor tudi imena posameznikov, odgovornih za izvedbo vsakega dela načrta jasno navedeni? | | |
| 11.1.5 | <u>Preskušanje, upravljanje, ponovno ocenjevanje načrtov za neprekinjeno poslovanje</u> | Ali se načrti za neprekinjeno poslovanje redno preskušajo za zagotavljanje učinkovitosti in trajne uspešnosti? Preskušanje je potrebno v primerih nabave nove opreme, nove tehnologije, spremembah v osebju ali organizaciji, spremembah poslovnih procesov, spremembah v zakonodaji, ... | | |
| | | Ali je zagotovljeno redno ažuriranje načrtov, da zaščitimo naložbo v razvoj prvotnega načrta in zagotovimo njegovo trajno uspešnost? Ali so v postopkih za nadzor sprememb v organizaciji upoštewane tudi potrebne spremembe načrta za neprekinjeno poslovanje? | | |
| Usklajenost | | | | |
| 12.1 | Usklajenost z zakonskimi zahtevami | | | |
| 12.1.1 | <u>Identifikacija potrebne zakonodaje</u> | Ali so ugotovljene in dokumentirane vse pomembne zakonske in pogodbene zahteve za informacijski sistem? Ali so jasno določene zahteve in osebne odgovornosti za izpolnjevanje zakonskih zahtev? | | |
| 12.1.2 | <u>Intelektualna lastnina</u> | Ali obstajajo postopki, ki zagotavljajo skladnost z zakonskimi omejitvami glede uporabe gradiv, programske opreme, ...? (avtorsko zaščitena programska oprema, licenčne pogodbe,) Ali se ti postopki redno izvajajo? (uporaba revizijskih orodij) | | |
| | | Ali se avtorsko zaščitena programska oprema dobavlja z licenčno pogodbo, ki omejuje njeno uporabo na določene računalnike in utegne omejevati kopiranje samo na izdelovanje rezervnih kopij? | | |
| 12.1.3 | <u>Varovanje evidenc v organizaciji</u> | Ali so pomembne evidence v organizaciji zaščitene pred izgubo, uničenjem ali ponarejanjem? Ali se evidence, ki so hranjene nad zakonsko potrebnim časom hrambe uničujejo? | | |
| 12.1.4 | <u>Zaščita osebnih in drugih podatkov</u> | Ali obstaja upravljavska struktura in kontrole za zaščito osebnih in drugih podatkov? (pridobivanje, namen uporabe, točnost, hranjenje podatkov) | | |
| 12.1.5 | <u>Preprečevanje zlorabe opreme informacijske tehnologije</u> | Ali se vsaka uporaba naprav za neposlovne ali nedovoljene namene, brez dovoljenja posloводства in ustreznega obračunavanja, obravnava kot nedovoljena uporaba opreme? Ali se pri prijavi v sistem prikaže opozorilo uporabniku? V opozorilu mora biti zapisano, da je sistem zaseben in da je neavtorizirana uporaba prepovedana. | | |

| Kontrolni seznam za nadzor varnostne politike - standard BS 7799.2:2002 | | | | |
|--|---|---|-------------------|------------------|
| Povezava s standardom | | Revizijsko področje, namen in vprašanja | Rezultati | |
| Standard | Poglavje | Vprašanje za revizijo | Ugotovitve | Skladnost |
| 12.1.6 | <u>Predpisi o uporabi šifriranja</u> | Ali so upoštevani vsi predpisi o šifriranju v vseh državah kjer deluje organizacija? Potrebno je upoštevati lokalne zakonske omejitve, ki obstajajo v nekaterih državah. | | |
| 12.1.7 | <u>Zbiranje dokazov</u> | Ali so postopki zbiranja dokazov v skladu z zakonodajo in splošno prakso v industriji? Za zagotovitev kvalitetnega dokaza je potrebno zagotoviti dobro revizijsko sled. | | |
| 12.2 | Pregledi varnostne politike in tehnične usklajenosti | | | |
| 12.2.1 | <u>Usklajenost z varnostno politiko</u> | Ali so vsa področja v organizaciji redno pregledujejo glede skladnosti z veljavno varnostno politiko, standardi in postopki? | | |
| 12.2.2 | <u>Preverjanje tehnične usklajenosti</u> | Ali so naprave informacijske tehnologije redno preverjene, če so usklajene z varnostnimi standardi? Ali se računalniški programi redno pregledujejo s pomočjo specialistične tehnične pomoči (izkušen sistemski inženir ali splošno uporabna programska oprema za samodejno izdelavo tehničnih poročil)? | | |
| 12.3 | Upoštevanje revidiranja sistema | | | |
| 12.3.1 | <u>Kontrole za revidiranje sistema</u> | Ali so revizijske zahteve in dejavnosti za preverjanje sistemov v obratovanju skrbno načrtovane in dogovorjene, tako da se karseda zmanjša nevarnost prekinjanja poslovnih procesov? | | |
| 12.3.2 | <u>Zaščita orodij za revidiranje</u> | Ali je dostop do orodij za revidiranje sistemov varovan, tako da preprečimo vsako možno zlorabo ali kršitev? | | |

Literatura

1. Information Security Management, Part2: Specification for Information security management systems AS/NZS 7799.2:2003 BS 7799.2:2002
2. Information Technology – Code of practice for Information Security Management AS/NZS ISO/IEC 17799:2001
3. Audit Check List for SANS, Val Thiagarajan