ITAF™

2. izdaja

Okvir strokovnega ravnanja za dajanje zagotovil/ revidiranje IS

Slovenski prevod

ISACA
Zaupanje v informacijske sisteme in koristi od njih
Slovenski odsek

About ISACA®
With more than 110,000 constituents in 85 countries, ISACA *(www.isaca.org)* is a leading global provider of knowledge, certifications, community, advocacy and education on information systems (IS) assurance and security, enterprise governance and management of IT, and IT-related risk and compliance. Founded in 1969, the non-profit, independent ISACA hosts international conferences, publishes the *ISACA® Journal*, and develops international IS auditing and control standards, which help its constituents ensure trust in, and value from, information systems. It also advances and attests IT skills and knowledge through the globally respected Certified Information Systems Auditor® (CISA®), Certified Information Security Manager® (CISM®), Certified in the Governance of Enterprise IT® (CGEIT®) and Certified in Risk and Information Systems Control™ (CRISC™) designations.

ISACA continually updates and expands the practical guidance and product family based on the COBIT framework. COBIT helps IT professionals and enterprise leaders fulfil their IT governance and management responsibilities, particularly in the areas of assurance, security, risk and control, and deliver value to the business.

Disclaimer
ISACA has designed and created *ITAF™: A Professional Practices Framework for IS Audit/Assurance, 2nd Edition* (the 'Work') primarily as an educational resource for assurance professionals. ISACA makes no claim that use of any of the Work will assure a successful outcome. The Work should not be considered inclusive of all proper information, procedures and tests or exclusive of other information, procedures and tests that are reasonably directed to obtaining the same results. In determining the propriety of any specific information, procedure or test, assurance professionals should apply their own professional judgement to the specific circumstances presented by the particular systems or information technology environment.

Quality Statement
This Work is translated into Slovenian from the English language version of ISACA® ITAF™: A Professional Practices Framework for IS Audit/Assurance, 2nd Edition by the ISACA Slovenia Chapter with the permission of ISACA. The ISACA Slovenia Chapter assumes sole responsibility for the accuracy and faithfulness of the translation.

Reservation of Rights

ISACA
3701 Algonquin Road, Suite
1010 Rolling Meadows, IL 60008 USA
Phone: +1.847.253.1545
Fax: +1.847.253.1443
Email: *Info@isaca.org*
Web site: *www.isaca.org*

Provide Feedback: *www.isaca.org/ITAF*
Participate in the ISACA Knowledge Center: *www.isaca.org/knowledge-center*
Follow ISACA on Twitter: *https://twitter.com/ISACANews*
Join ISACA on LinkedIn: ISACA (Official), *http://linkd.in/ISACAOfficial*
Like ISACA on Facebook: *www.facebook.com/ISACAHQ*

O ISACA®

Z več kot 110.000 člani iz 85 držav je ISACA *(www.isaca.org)* vodilni globalni ponudnik znanja, nazivov, povezovanja strokovnjakov, zagovorništva in izobraževanja na področju dajanja zagotovil in varnosti informacijskih sistemov (IS), upravljanja in vodenja IT ter na področju tveganj in skladnosti IT. Neprofitno in neodvisno združenje ISACA, ustanovljeno leta 1969, prireja mednarodne konference, izdaja revijo *ISACA® Journal* in razvija mednarodne standarde za revizijo in nadzor IS, ki članom pomagajo zagotavljati zaupanje v in korist od informacijskih sistemov. Vzpodbuja tudi razvoj in potrjuje veščine in znanje o IT s podeljevanjem svetovno priznanih nazivov preizkušeni revizor informacijskih sistemov (Certified Information Systems Auditor® – CISA®), preizkušeni upravljavec varovanja informacij (Certified Information Security Manager ® – CISM®), preizkušen v vodenju IT v podjetju (Certified in the Governance of Enterprise IT® – CGEIT®) ter preizkušen v upravljanju tveganj in nadzoru informacijskih sistemov (Certified in Risk and Information Systems Control™ – CRISC™).

ISACA nenehno posodablja in širi praktične smernice in družino produktov na osnovi okvira COBIT. COBIT strokovnjakom IT in vodjem podjetij pomaga izpolnjevati njihove pristojnosti pri vodenju in upravljanju IT, zlasti na področjih dajanja zagotovil, varnosti, tveganj in nadzora ter zagotavljanja poslovnih koristi.

Izjava o omejitvi odgovornosti

ISACA je zasnovala in ustvarila ITAF™: Okvir strokovnega ravnanja za dajanje zagotovil/revizijo IS, 2. izdaja (v nadaljevanju: »delo«) predvsem kot izobraževalni vir za strokovnjake na področju dajanja zagotovil. ISACA ne trdi, da bo uporaba katerega koli dela tega dokumenta zagotovila uspešen izid. Tega dela ne smete razumeti kot delo, ki vključuje vse ustrezne informacije, postopke in preizkuse, ali kot delo, ki izključuje vse druge informacije, postopke in preizkuse, ki so razumno usmerjeni k pridobivanju istih rezultatov. Pri ugotavljanju ustreznosti določene informacije, postopka ali preizkusa mora strokovnjak za dajanje zagotovil uporabiti lastno strokovno presojo posameznih okoliščin, ki jih predstavljajo določeni sistemi ali okolje informacijske tehnologije.

Izjava o kakovosti

Delo je iz angleške različice ISACA® ITAF™: Okvir strokovnega ravnanja za dajanje zagotovil/revizijo IS, 2. izdaja, s soglasjem ISACA v slovenščino prevedel Slovenski odsek ISACA. Slovenski odsek ISACA prevzema vso odgovornost za pravilnost in skladnost prevoda z izvirnikom.

Pridržek pravic

ISACA
3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008, ZDA
Telefon: +1 847 253 1545
Telefaks: +1 847 253 1443
E-naslov: *Info@isaca.org*
Spletna stran: *www.isaca.org*

Posredujte povratne informacije: *www.isaca.org/ITAF*
Sodelujte v ISACA Knowledge Center: *www.isaca.org/knowledge-center*
Spremljajte ISACA na Twitterju: *https://twitter.com/ISACANews*
Pridružite se ISACA na LinkedInu: ISACA (uradni profil), *http://linkd.in/ISACAOfficial*
Všečkajte ISACA na Facebooku: *www.facebook.com/ISACAHQ*

Slovenski odsek ISACA
Dunajska cesta 106
SI-1000 Ljubljana, Slovenija
Telefon: +386 1 568 55 54
Telefaks: +386 1 568 63 32
E-naslov: *info@isaca.si*
Spletna stran: *www.isaca.si*

Povratne informacije, komentarje in predloge sprememb v zvezi s prevodom posredujte Slovenskemu odseku: *tajnik@isaca.si*
Pridružite se Slovenskemu odseku na LinkedInu: *http://www.linkedin.com/groups/ISACA-Slovenia-Chapter-4157929?trk=myg_ugrp_ovr*
Všečkajte Slovenski odsek na Facebooku: *https://www.facebook.com/IsacaSloveniaChapter*

ITAF™: Okvir strokovnega ravnanja za dajanje zagotovil/revizijo IS, 2. izdaja – slovenski prevod; december 2013

Zahvale

ISACA želi izraziti hvaležnost

Upravnemu odboru ISACA
Gregory T. Grocholski, CISA, The Dow Chemical Co., ZDA, mednarodni predsednik
Allan Boardman, CISA, CISM, CGEIT, CRISC, ACA, CA (SA), CISSP, Morgan Stanley, ZK, podpredsednik
Juan Luis Carselle, CISA, CGEIT, CRISC, Wal-Mart, Mehika, podpredsednik
Christos K. Dimitriadis, Ph.D., CISA, CISM, CRISC, INTRALOT S.A., Grčija, podpredsednik
Ramses Gallego, CISM, CGEIT, CCSK, CISSP, SCPM, 6 Sigma, Quest Software, Španija, podpredsednik
Tony Hayes, CGEIT, AFCHSE, CHE, FACS, FCPA, FIIA, vlada zvezne države Queensland, Avstralija, podpredsednik
Jeff Spivey, CRISC, CPP, PSP, Security Risk Management Inc., ZDA, podpredsednik
Marc Vael, Ph.D., CISA, CISM, CGEIT, CRISC, CISSP, Valuendo, Belgija, podpredsednik
Kenneth L. Vander Wal, CISA, CPA, Ernst & Young LLP (upokojen), ZDA, prejšnji mednarodni predsednik
Emil D'Angelo, CISA, CISM, Bank of Tokyo-Mitsubishi UFJ Ltd. (upokojen), ZDA, prejšnji mednarodni predsednik
John Ho Chi, CISA, CISM, CRISC, CBCP, CFE, Ernst & Young LLP, Singapur, direktor
Krysten McCabe, CISA, The Home Depot, ZDA, direktor
Jo Stewart-Rattray, CISA, CISM, CGEIT, CRISC, CSEPS, BRM Holdich, Avstralija, direktor

Odboru za nazive in upravljanje kariere
Allan Boardman, CISA, CISM, CGEIT, CRISC, ACA, CA (SA), CISSP, Morgan Stanley, ZK, predsednik
Garry James Barnes, CISA, CISM, CGEIT, CRISC, Stratsec, Avstralija
Christopher Whitman Bates, CISA, CGEIT, CRISC, Deloitte & Touche, ZDA
Terry Chrisman, CGEIT, CRISC, GE Money, ZDA
Timo Kai Heikkinen, CISA, CGEIT, Nordea Bank Finland Plc, Finska
Hitoshi Ota, CISA, CISM, CGEIT, CRISC, CIA, Mizuho Corporate Bank, Japonska
Ross E. Wescott, CISA, CIA, Portland General Electric, ZDA
David Yeung Yeok Wah, CISA, CFE, CIA, KPMG, Singapur

Odboru za strokovne standarde
Steven E. Sizemore, CISA, CIA, CGAP, Texas Health and Human Services Commission, ZDA, predsednik
Christopher Nigel Cooper, CISM, CITP, FBCS, HP Enterprises Security Services, ZK
Ronald E. Franke, CISA, CRISC, CFE, CIA, CICA, Myers and Stauffer LC, ZDA
Murari Kalyanaramani, CISA, CISM, CRISC, CISSP, CBCP, British American Tobacco IT Services, Malezija
Alisdair McKenzie, CISA, CISSP, ITCP, IS Assurance Services, Nova Zelandija
Katsumi Sakagawa, CISA, CRISC, PMP, JIEC Co. Ltd., Japonska
Ian Sanderson, CISA, CRISC, FCA, NATO, Belgija
Timothy Smith, CISA, CISSP, CPA, LPL Financial, ZDA
Rodolfo Szuster, CISA, CA, CBA, CIA, Tarshop S.A., Argentina

Zahvala strokovnjakom, ki so pregledali prevod

ITAF™: Okvir strokovnega ravnanja za dajanje zagotovil/revizijo IS, 2. izdaja, je v slovenščino za Slovenski odsek prevedel poklicni prevajalec, prevod pa so pregledali prostovoljci. V tej izdaji so bili prevedeni in pregledani prenovljeni standardi, smernice so prevzete iz prejšnjega prevoda. Vsi člani ISACA, ki so sodelovali pri tokratnem pregledu prevedenega okvirja, zaslužijo našo zahvalo in hvaležnost.

Strokovnjaki, ki so pregledali prevod
Peter Grasselli, CISA
mag. Marko Jagodic, CISA, CRISC
Boža Javornik, CISA, CISM
mag. Boštjan Kežmah, CISA
Tadej Kosmačin, CISA
mag. Jožica Kržič, CISA
dr. Nataša Žabkar, CISA
dr. Aleš Živkovič, CISA

Vsebina

Uvod

ITAF je celovit referenčni model vzpostavljanja dobre prakse, ki:
- vzpostavlja standarde, ki upoštevajo vloge in odgovornosti strokovnjakov dajanja zagotovil in revidiranja IS, strokovno znanje in izkušnje, skrbnost, ravnanje in zahteve glede poročanja;
- opredeljuje pojme in koncepte, specifične za dajanje zagotovil v zvezi z IS;
- predpisuje smernice in orodja ter tehnike za načrtovanje, oblikovanje, izvajanje in poročanje o nalogah dajanja zagotovil in revidiranja IS.

ITAF je osredotočen na gradivo ISACA in zagotavlja enoten vir, s pomočjo katerega lahko strokovnjaki dajanja zagotovil in revidiranja IS poiščejo usmeritve, raziskujejo politike in postopke, pridobijo programe revidiranja in dajanja zagotovil in sestavijo uspešna poročila.

Čeprav ITAF zajema obstoječe standarde in smernice dajanja zagotovil in revidiranja IS združenja ISACA, je zasnovan kot živ dokument. Novo razvite in izdane smernice bodo vključene v obstoječ okvir. Trenutne smernice ISACA so že bile preslikane v okvir.

Komisija ISACA za strokovne standarde in upravljanje kariere je zavezana k obširnemu posvetovanju pri pripravi standardov in smernic dajanja zagotovil in revidiranja IS. Pred izdajo kateregakoli dokumenta se na mednarodni ravni izda osnutek za splošno javno razpravo. Osnutek za razpravo spremlja spletni vprašalnik, ki bo na voljo na spletni strani *www.isaca.org/standardexposure*. Mnenja lahko direktorju razvoja strokovnih standardov pošljete tudi prek elektronske pošte na naslov *standards@isaca.org*.

Pogosto zastavljena vprašanja:
- **Za koga velja ITAF?** ITAF velja za posameznike, ki delujejo kot strokovnjaki dajanja zagotovil in revidiranja IS, in sodelujejo pri dajanju zagotovil za določene komponente aplikacij in infrastrukture IS. Ne glede na to pa je bilo poskrbljeno, da so ti standardi, smernice, orodja in tehnike sestavljeni tako, da so lahko uporabni in koristni tudi za širše občinstvo, vključno z uporabniki poročil dajanja zagotovil in revizije IS.
- **Kdaj je uporaba ITAF primerna?** Uporaba okvirja je predpogoj za dajanje zagotovil in revidiranje IS. Standardi so obvezni. Smernice, orodja in tehnike so zasnovani kot neobvezna pomoč pri izvajanju dajanja zagotovil.
- **Na katerem področju naj se uporabljajo ITAF standardi in z njimi povezane smernice dajanja zagotovil in revidiranja IS?** Zasnova ITAF upošteva, da se strokovnjaki dajanja zagotovil in revidiranja IS srečujejo z različnimi zahtevami in nalogami – od vodenja revizije osredotočene na IS, do sodelovanja pri finančni reviziji ali reviziji operativnega delovanja. ITAF je uporaben pri katerem koli formalnem poslu ocenjevanja in revidiranja IS.
- **Ali ITAF obravnava zahteve glede svetovalnega in posvetovalnega dela?** Poleg ocenjevalnega dela strokovnjaki dajanja zagotovil in revidiranja IS pogosto za delodajalca ali v imenu stranke opravljajo posle svetovanja in posvetovanja. Rezultat teh nalog je pogosto ocena določenega področja, prepoznavanje težav, negotovosti ali slabosti ter oblikovanje priporočil. Zaradi številnih razlogov, vključno z naravo dela, obsegom posla, neodvisnostjo in stopnjo preizkušanja, se takšno delo ne šteje kot revizija, zato strokovnjak za revizijo in dajanje zagotovil v zvezi z IS ne izda formalnega revizijskega poročila. ITAF ni zasnovan za obravnavanje specifičnih zahtev v zvezi s tovrstnim svetovalnim in posvetovalnim delom.

Organizacija

Standardi ITAF dajanja zagotovil in revidiranja IS so razdeljeni v tri kategorije:
- **Splošni standardi (serija 1000) –** so vodilna načela, po katerih se ravna strokovnjak dajanja zagotovil IS. Veljajo za izvajanje vseh nalog in obravnavajo etiko, neodvisnost, objektivnost in potrebno skrbnost, pa tudi strokovno znanje, usposobljenost in izkušenost strokovnjakov dajanja zagotovil in revidiranja IS.
- **Izvedbeni standardi (serija 1200) –** se nanašajo na izvajanje nalog, kot so načrtovanje in nadzor, opredeljevanje obsega, tveganj in pomembnosti, aktiviranje virov, upravljanje nadzora in zadolžitev, dokaze pri dajanju zagotovil in revidiranju ter na strokovno presojo in potrebno skrbnost.
- **Standardi poročanja (serija 1400) –** obravnavajo vrste poročil, način sporočanja in sporočene informacije.

Smernice ITAF dajanja zagotovil in revidiranja IS strokovnjaku za dajanje zagotovil in revidiranje IS zagotavljajo informacije in navodila na področju dajanja zagotovil in revidiranja IS. Skladno z zgoraj navedenimi tremi kategorijami standardov se smernice osredotočajo na različne revizijske pristope, metodologije in druga gradiva, ki zagotavljajo pomoč pri načrtovanju, izvedbi, ocenjevanju, preizkušanju in poročanju o procesih in kontrolah IS in povezanih pobudah dajanja zagotovil in revidiranja IS. Poleg tega smernice pomagajo razjasniti odnos med dejavnostmi in pobudami podjetja in podvzetimi aktivnostmi in pobudami IT.

Smernice ITAF za revizijo in dajanje zagotovil v zvezi z IS se prav tako delijo v tri kategorije:
- **splošne smernice (serija 2000),**
- **izvedbene smernice (serija 2200),**
- **smernice poročanja (serija 2400).**

Orodja in tehnike v razdelku 3000 zagotavljajo specifične informacije o različnih metodologijah, orodjih in predlogah; zagotavljajo navodila za njihovo uporabo in so namenjena operacionalizaciji informacij, podanih v smernicah. Upoštevajte, da so orodja in tehnike v različnih oblikah: dokumenti za razpravo, tehnične smernice, bele knjige, revizijski programi ali knjige, npr. objava ISACA o SAP, ki vsebuje smernice o sistemih za načrtovanja virov podjetja (ERP).

Skladno z zasnovo ITAF kot nenehno spreminjajočega se dokumenta so med številkami poglavij namerno vrzeli za prihodnje smernice.

Uporaba ITAF

Standardi so v vseh primerih obvezni. Pojem »mora« označuje obveznost. Vsakršna morebitna odstopanja se morajo obravnavati pred zaključkom posla dajanja zagotovil ali revidiranja IS.

Smernice niso obvezne, vendar njihovo upoštevanje močno priporočamo. Čeprav smernice strokovnjakom dajanja zagotovil in revidiranja IS dopuščajo določeno mero svobode pri uporabi, morajo biti strokovnjaki zmožni zagovarjati in upravičiti vsa pomembna odstopanja od smernic ali opustitev relevantnih poglavij smernice pri izvajanju poslov dajanja zagotovil in revidiranja IS. To velja zlasti, če je posel bolj na ravni revidiranja IS. Vse smernice ne bodo uporabne v vseh okoliščinah, vendar je potrebno njihovo uporabo vedno proučiti.

Orodja in tehnike predstavljajo dopolnilno gradivo in informacije za dodatno pomoč k smernicam. V nekaterih primerih tehnike predstavljajo alternativne možnosti ali celo vrsto tehnik, od katerih je številne mogoče uporabiti. Tehnike je dopustno izbrati samo, če so primerne in ustrezne, ter če strokovnjaku za dajanje zagotovil in revidiranje IS omogočajo pridobitev ustreznih, relevantnih, objektivnih in nepristranskih informacij.

Popolne informacije o standardih in smernicah ISACA za dajanje zagotovil in revidiranje IS so na voljo na spletni strani www.isaca.org/standards.

Postopek dajanja zagotovil ali revidiranja IS vključuje izvedbo določenih postopkov za zagotavljanje ustrezne ravni zagotovil glede obravnavane zadeve. Strokovnjaki dajanja zagotovil in revidiranja IS izvajajo naloge z namenom dajanja zagotovil na različnih ravneh, od pregleda do preverjanja ali preiskovanja.

Vsaka naloga dajanja zagotovil ali revidiranja IS mora biti izvedena v skladu s predpisanimi standardi v smislu usposobljenosti posameznikov za izvedbo naloge, načina izvedbe dela, vrste dela ter načina poročanja ugotovitev v povezavi z različnimi lastnostmi naloge in naravo pridobljenih rezultatov. Če bo posel izvajala ena oseba, mora ta oseba posedovati izkušnje in strokovno znanje potrebno za dokončanje posla. Če bo posel izvajalo več oseb, mora celotna skupina kolektivno posedovati potrebne izkušnje in strokovno znanje za izvedbo dela.

Vsaka naloga dajanja zagotovil ali revidiranja IS je neločljivo povezana z več ključnimi predpostavkami, vključno z naslednjim:
- obravnavano zadevo je mogoče opredeliti in je predmet revizije,
- obstaja visoka verjetnost uspešnega zaključka projekta,
- pristop in metodologija sta nepristranska,
- obseg projekta je zadostnega obsega za izpolnitev ciljev dajanja zagotovil in revidiranja IS,
- projekt bo pripeljal do objektivnega poročila, ki ne bo zavajalo bralca.

Standardi, ki jih izdajo drugi organi za standardizacijo

Čeprav standardi ITAF strokovnjakom za dajanje zagotovil in revidiranje IS zagotavljajo potrebne smernice in navodila, se lahko v določenih okoliščinah pojavi potreba po uporabi regulativnih standardov, ki jih izda druga organizacija.

Strokovnjak dajanja zagotovil in revidiranja IS lahko:
- uporablja standarde ITAF v povezavi s strokovnimi standardi, ki jih izdajo drugi pristojni organi,
- v poročilu navede uporabo drugih standardov ne glede na ITAF standarde.

Kadar strokovnjak za dajanje zagotovil in revidiranje IS uporablja druge standarde kot ITAF, mora paziti, da ne pride do nasprotujočih zahtev med standardi.

Kadar strokovnjak za dajanje zagotovil in revidiranje IS navede skladnost s standardi ITAF in obstajajo nasprotujoče zahteve med standardi ITAF in drugimi navedenimi standardi, mora strokovnjak dajanja zagotovil in revidiranja IS pri izvedbi pregleda in poročanju o rezultatih kot prevladujoče standarde uporabiti standarde ITAF, razen če druge standarde predstavljajo zakonske zahteve.

Pojmi in njihovi pomeni

V celotnem dokumentu se uporabljajo skupni izrazi, ki imajo določen pomen. Za zagotovitev razumljivosti in dosledne uporabe besed in njihovega pomena v kontekstu tega dokumenta je na spletni strani ISACA *www.isaca.org/glossary* na voljo celoten pojmovnik izrazov (slovenski prevod pojmovnika je na naslovu *http://www.isaca.si/dokumenti/ISACA_Pojmovnik_Prevod-Slo.pdf*).

Kodeks poklicne etike ISACA

ISACA je postavila ta Kodeks poklicne etike kot vodilo za strokovno in osebno ravnanje članov združenja in/ali imetnikov nazivov.

Člani in imetniki nazivov ISACA morajo:

1. Spodbujati skladnost z in podpirati vpeljavo ustreznih standardov in postopkov, namenjenih učinkovitemu vodenju in upravljanju informacijskih sistemov in tehnologij podjetja, vključno z: revidiranjem, nadzorovanjem, upravljanjem varnosti in tveganja.
2. Opravljati svoje naloge objektivno, z dolžno prizadevnostjo in strokovno skrbnostjo, ter skladno s strokovnimi standardi.
3. Delovati na zakonit način v interesu deležnikov, sočasno vzdrževati visoke standarde obnašanja in osebnostnih lastnosti, pri tem pa ne ogrožati ugleda stroke ali združenja.
4. Varovati zasebnost in zaupnost informacij, pridobljenih med opravljanjem svojih aktivnosti, razen če razkritje zahteva zakonodaja. Takšne informacije se ne smejo uporabljati za osebno korist in jih ni dovoljeno izdajati neprimernim strankam.
5. Ohranjati usposobljenost na svojem področju in sprejemati samo tiste aktivnosti, za katere lahko upravičeno pričakujejo, da jih bodo uspešno opravili s potrebnimi veščinami, znanjem in usposobljenostjo.
6. Primerne stranke obveščati o rezultatih opravljenega dela, vključno z razkritjem vseh pomembnih znanih dejstev, ki bi lahko ob nerazkritju izkrivila poročanje o rezultatih.
7. Podpirati strokovno izobraževanje deležnikov z namenom izboljšanja njihovega razumevanja vodenja in upravljanja informacijskih sistemov in tehnologij podjetja, vključno z: revidiranjem, nadzorovanjem, upravljanjem varnosti in tveganja.

V primeru, če se ne ravna po tem Kodeksu poklicne etike, se lahko proti članu ISACA ali imetniku naziva uvede preiskava o njegovem ravnanju in, končno, izreče disciplinski ukrep.

1. Standardi dajanja zagotovil in revidiranja IS

Kot je navedeno že v uvodu, je treba standarde ITAF (splošne, izvedbene in standarde poročanja) upoštevati v vseh okoliščinah. Poleg tega standardi vključujejo ključna pojasnila, ki so opredeljena kot pomoč strokovnjakom dajanja zagotovil in revidiranja IS, zato so informacije znotraj posameznega standarda, kjer se zahteva skladnost, poudarjene s **krepkim tiskom.** Standarde ITAF se redno pregleduje z namenom zagotavljanja nenehnih izboljšav in se jih po potrebi dopolnjuje, da sledijo nastajajočim izzivom na področju dajanja zagotovil in revidiranja IS.

Zahteve standardov

Za lažje razumevanje so na tem mestu vstavljene obvezne zahteve standardov.

Splošno

1001 Revizijska listina

1001.1 Pri dajanju zagotovil in revidiranju IS mora biti revidiranje ustrezno dokumentirano v revizijski listini, pri čemer morajo biti navedeni namen, zadolžitev, pristojnost in odgovornost.

1001.2 Pri dajanju zagotovil in revidiranju IS mora biti revizijska listina usklajena in potrjena na ustrezni ravni v podjetju.

1002 Organizacijska neodvisnost

1002.1 Dajanje zagotovil in revidiranje IS mora biti neodvisno od pregledovanega področja ali aktivnosti, da je omogočeno nepristransko dokončanje posla revidiranja in dajanja zagotovil.

1003 Strokovna neodvisnost

1003.1 Strokovnjaki dajanja zagotovil in revidiranja IS morajo biti tako dejansko kot po zaznavi neodvisni in objektivni v vseh zadevah, povezanih s posli revidiranja in dajanja zagotovil.

1004 Upravičeno pričakovanje

1004.1 Strokovnjaki dajanja zagotovil in revidiranja IS morajo imeti upravičeno pričakovanje, da je lahko posel izveden skladno s standardi dajanja zagotovil in revidiranja IS ter po potrebi skladno z drugimi ustreznimi strokovnimi in panožnimi standardi ali veljavnimi predpisi in da bo rezultat strokovno mnenje ali sklep.

1004.2 Strokovnjaki dajanja zagotovil in revidiranja IS morajo imeti upravičeno pričakovanje, da je glede na obseg posla možno sklepati o obravnavani zadevi in upoštevati kakršne koli omejitve.

1004.3 Strokovnjaki dajanja zagotovil in revidiranja IS morajo imeti razumno pričakovanje, da se organ vodenja zaveda svojih obveznosti in zadolžitev pri zagotavljanju ustreznih, relevantnih in pravočasnih informacij, ki so potrebne za izvedbo posla.

1005 Dolžna poklicna skrbnost

1005.1 Strokovnjaki dajanja zagotovil in revidiranja IS morajo pri načrtovanju in izvajanju poslov ter poročanju o njihovih izidih spoštovati dolžno poklicno skrbnost, vključno z upoštevanjem veljavnih strokovnih standardov za revizijo.

1006 Strokovna usposobljenost

1006.1 Strokovnjaki dajanja zagotovil in revidiranja IS morajo imeti skupaj z ostalimi sodelavci pri nalogi ustrezne veščine ter strokovno usposobljenost za izvedbo poslov dajanja zagotovil in revidiranja IS ter biti strokovno usposobljeni za opravljanje zahtevanega dela.

1006.2 Strokovnjaki dajanja zagotovil in revidiranja IS morajo skupaj s sodelavci pri nalogi posedovati ustrezno znanje o obravnavani zadevi.

1006.3 Strokovnjaki dajanja zagotovil in revidiranja IS morajo ohranjati strokovno usposobljenost z ustreznim nenehnim strokovnim izobraževanjem in usposabljanjem.

1007 Trditve

1007.1 Strokovnjaki dajanja zagotovil in revidiranja IS morajo pregledati trditve, na podlagi katerih bodo presojali obravnavano zadevo, z namenom, da bi ugotovili ali je mogoče takšne trditve revidirati in ali so te trditve zadostne, veljavne in relevantne.

1008 Merila

1008.1 Strokovnjaki dajanja zagotovil in revidiranja IS morajo izbrati merila, glede na katera se bo obravnavana zadeva presojala in ki so: nepristranska, celovita, relevantna, izmerljiva, razumljiva, splošno priznana, izdana s strani pristojnih organov in razumljiva ter na voljo vsem bralcem in uporabnikom poročila.

1008.2 Strokovnjaki dajanja zagotovil in revidiranja IS morajo upoštevati vire meril in se, preden sprejmejo manj znana merila, osredotočiti na tiste, ki jih objavijo relevantni pristojni organi.

Izvedba

1201 Načrtovanje posla

1201.1 Strokovnjaki dajanja zagotovil in revidiranja IS morajo načrtovati vsak posel dajanja zagotovil in revidiranja IS z namenom, da opredelijo:
- cilj/-e, obseg, časovni načrt in izdelke,
- skladnost z veljavnimi zakoni in strokovnimi revizijskimi standardi,
- uporabo na tveganjih temelječega pristopa, kjer je to primerno,
- vprašanja, ki so lastna poslu,
- zahteve glede dokumentacije in poročanja.

1201.2 Strokovnjaki dajanja zagotovil in revidiranja IS morajo razviti in dokumentirati projektni načrt posla dajanja zagotovil in revidiranja IS, ki opisuje:
- vrsto posla, cilje, časovni načrt in zahteve glede virov,
- časovno razporeditev in obseg revizijskih postopkov za izvedbo posla.

1202 Ocenjevanje tveganja pri načrtovanju

1202.1 Pri dajanju zagotovil in revidiranju IS morata biti za razvoj celotnega načrta revidiranja IS in določitev prioritet za učinkovito dodelitev virov za revizijo IS uporabljena ustrezen pristop in pripadajoča metodologijo za oceno tveganja.

1202.2 Strokovnjaki dajanja zagotovil in revidiranja IS morajo pri načrtovanju posameznih poslov prepoznati in oceniti tveganje, relevantno za področje pregleda.

1202.3 Strokovnjaki dajanja zagotovil in revidiranja IS morajo preučiti tveganja povezana z obravnavano zadevo, revizijsko tveganje in vpliv na izpostavljenost podjetja.

1203 Izvedba in nadzor

1203.1 Zato, da zajamejo prepoznana tveganja, morajo strokovnjaki dajanja zagotovil in revidiranja IS delo opraviti skladno z odobrenim načrtom revidiranja IS in v dogovorjenih rokih.

1203.2 Z namenom, da se dosežejo revizijski cilji in spoštujejo veljavni strokovni revizijski standardi, morajo strokovnjaki dajanja zagotovil in revidiranja IS nadzirati osebje, ki izvaja revizije IS in za katero so zadolženi.

1203.3 Strokovnjaki dajanja zagotovil in revidiranja IS lahko sprejmejo samo naloge, ki so v okviru njihovega strokovnega znanja in veščin ali naloge, za katere imajo upravičeno pričakovanje, da bodo veščine pridobili v teku posla ali da jih bodo opravili pod nadzorom.

1203.4 Za doseganje revizijskih ciljev morajo strokovnjaki dajanja zagotovil in revidiranja IS pridobiti zadostne in ustrezne dokaze. Ugotovitve in sklepi revizije morajo biti podprti z ustreznimi analizami in razlago teh dokazov.

1203.5 Strokovnjaki dajanja zagotovil in revidiranja IS morajo revizijski postopek dokumentirati z opisi revizijskega dela in revizijskimi dokazi, ki podpirajo ugotovitve in sklepe.

1203.6 Strokovnjaki dajanja zagotovil in revidiranja IS morajo prepoznavati in sklepati na podlagi ugotovitev.

1204 Pomembnost

1204.1 Strokovnjaki dajanja zagotovil in revidiranja IS morajo pri načrtovanju posla upoštevati morebitne slabosti ali pomanjkljivosti kontrol in pretehtati, ali bi te slabosti ali pomanjkljivosti kontrol lahko imele za posledico pomembno pomanjkljivost ali bistveno slabost.

1204.2 Strokovnjaki dajanja zagotovil in revidiranja IS morajo upoštevati revizijsko pomembnost in njeno povezanost z revizijskim tveganjem, ko določajo vrsto, časovno razporeditev in obseg revizijskih postopkov.

1204.3 Strokovnjaki dajanja zagotovil in revidiranja IS morajo upoštevati skupni učinek manjših pomanjkljivosti kontrol ali slabosti in možnost, da se pomanjkanje kontrol prevede v pomembno pomanjkljivost ali bistveno slabost.

1204.4 Strokovnjaki dajanja zagotovil in revidiranja IS morajo v svojem poročilu razkriti naslednje:
- pomanjkanje kontrol ali neučinkovite kontrole,
- pomembnost pomanjkljivosti kontrol,
- verjetnost, da bodo te slabosti povzročile pomembno pomanjkljivost ali bistveno slabost.

1205 Dokazi

1205.1 Strokovnjaki dajanja zagotovil in revidiranja IS morajo pridobiti zadostne in ustrezne dokaze, da lahko sprejmejo primerne sklepe, s katerimi utemeljijo izide posla.

1205.2 Strokovnjaki dajanja zagotovil in revidiranja IS morajo ovrednotiti zadostnost dokazov, pridobljenih za utemeljitev sklepov in doseganje ciljev posla.

1206 Uporaba dela drugih strokovnjakov

1206.1 Če je primerno, morajo strokovnjaki dajanja zagotovil in revidiranja IS preučiti možnost uporabe dela drugih strokovnjakov pri poslu.

1206.2 Strokovnjaki dajanja zagotovil in revidiranja IS morajo pred začetkom izvajanja posla oceniti in odobriti ustreznost strokovne usposobljenosti, sposobnosti, ustreznih izkušenj, virov, neodvisnosti in postopkov nadzora kakovosti drugih strokovnjakov.

1206.3 Strokovnjaki dajanja zagotovil in revidiranja IS morajo v okviru posla oceniti, pregledati in ovrednotiti delo drugih strokovnjakov ter dokumentirati odločitev, v kakšnem obsegu so uporabili in se zanašali na njihovo delo.

1206.4 Strokovnjaki dajanja zagotovil in revidiranja IS morajo odločiti, ali je delo drugih strokovnjakov izven revizijske skupine zadostno in popolno za sklepanje o trenutnih ciljih posla, ter sklep jasno dokumentirati.

1206.5 Strokovnjaki dajanja zagotovil in revidiranja IS morajo odločiti, ali se bodo zanašali na delo drugega strokovnjaka in delo neposredno vključili v poročilo, ali ga bodo v poročilu navedli ločeno.

1206.6 Strokovnjaki dajanja zagotovil in revidiranja IS morajo izvesti dodatne preizkusne postopke za pridobitev zadostnih in ustreznih dokazov v okoliščinah, kjer delo drugih strokovnjakov ne zagotavlja zadostnih ali ustreznih dokazov.

1206.7 Strokovnjaki dajanja zagotovil in revidiranja IS morajo zagotoviti ustrezno revizijsko mnenje ali sklep ter vključiti vsakršne omejitve obsega, v primeru da potrebni dokazi niso pridobljeni s pomočjo dodatnih preizkusov.

1207 Nepravilnosti in nezakonita dejanja

1207.1 Strokovnjaki dajanja zagotovil in revidiranja IS morajo med izvajanjem posla upoštevati tveganja nepravilnosti in nezakonitih dejanj.

1207.2 Strokovnjaki dajanja zagotovil in revidiranja IS morajo med izvajanjem posla ohranjati poklicno nezaupljivost.

1207.3 Strokovnjaki dajanja zagotovil in revidiranja IS morajo dokumentirati in primerni stranki pravočasno sporočiti vsako pomembno nepravilnost ali nezakonito dejanje.

Poročanje

1401 Poročanje

1401.1 Strokovnjaki dajanja zagotovil in revidiranja IS morajo o izvedbi posla pripraviti poročilo, v katerem sporočijo rezultate, vključno z:

- identifikacijo podjetja, predvidenimi prejemniki in kakršnimi koli omejitvami glede vsebine in posredovanja poročila;
- obsegom, cilji posla, obdobjem, ki ga zajema, ter vrsto, časovno razporeditvijo in obsegom opravljenega dela;
- ugotovitvami, sklepi in priporočili;
- vsakršnimi zadržki ali omejitvami obsega, ki jih ima strokovnjak dajanja zagotovil in revidiranja IS v zvezi s poslom;
- podpisom, datumom in prejemniki, skladno z določili revizijske listine ali listine o poslu.

1401.2 Strokovnjaki dajanja zagotovil in revidiranja IS morajo zagotoviti, da so ugotovitve v revizijskem poročilu podprte z zadostnimi in ustreznimi revizijskimi dokazi.

1402 Nadaljnja obravnava

1402.1 Strokovnjaki dajanja zagotovil in revidiranja IS morajo spremljati relevantne informacije, da lahko sklepajo, ali je poslovodstvo načrtovalo/sprejelo ustrezne in pravočasne ukrepe za obravnavanje poročanih revizijskih ugotovitev in priporočil.

Splošni standardi

Splošni standardi so vodilna načela, po katerih se ravna strokovnjak dajanja zagotovil in revidiranja IS. Veljajo za izvajanje vseh nalog in obravnavajo etiko, neodvisnost, objektivnost in dolžno skrbnost, kakor tudi strokovno znanje, usposobljenost in veščine strokovnjakov dajanja zagotovil in revidiranja IS.

Pri izvajanju naloge dajanja zagotovil ali revidiranja IS bo moral strokovnjak dajanja zagotovil in revidiranja IS pretehtati številne ključne odločitve v zvezi z obravnavano zadevo in merila za njeno ocenitev. Pri tem bo moral strokovnjak dajanja zagotovil in revizije IS upoštevati merila, po katerih bo izvajal nalogo (standardi) in v primerjavi s katerimi bo obravnavano zadevo ocenil (kriteriji).

Splošni standardi so:
1001 Revizijska listina
1002 Organizacijska neodvisnost
1003 Strokovna neodvisnost
1004 Upravičeno pričakovanje
1005 Dolžna poklicna skrbnost
1006 Strokovna usposobljenost
1007 Trditve
1008 Merila

Standardi so tukaj vključeni v celoti. Podčrtane besede so opredeljene v poglavju s pojmi. Za povezave do posameznih standardov obiščite spletno stran *www.isaca.org/standard*.

1001 Revizijska listina

Zahteve

1001.1 Pri dajanju zagotovil in revidiranju IS mora biti revidiranje ustrezno dokumentirano v revizijski listini, pri čemer morajo biti navedeni namen, zadolžitev, pristojnost in odgovornost.

1001.2 Pri dajanju zagotovil in revidiranju IS mora biti revizijska listina usklajena in potrjena na ustrezni ravni v podjetju.

Ključna pojasnila

Pri dajanju zagotovil in revidiranju IS naj bi:

- pripravili revizijsko listino za opredelitev aktivnosti notranjega dajanja zagotovil in revidiranja IS, ki dovolj podrobno sporoča naslednje informacije:
  - pristojnost, namen, zadolžitve in omejitve dajanja zagotovil in revidiranja IS,
  - neodvisnost in odgovornost dajanja zagotovil in revidiranja IS,
  - vloge in zadolžitve revidiranca med izvajanjem posla dajanja zagotovil ali posla revidiranja IS,
  - strokovne standarde, ki jih mora strokovnjak na področju dajanja zagotovil in revidiranja IS upoštevati pri izvajanju poslov dajanja zagotovil in revidiranja IS;
- revizijsko listino pregledali vsaj enkrat na leto oz. pogosteje, če se zadolžitve spremenijo,
- revizijsko listino po potrebi posodobili, da zagotovimo, da so namen in zadolžitve ves čas ustrezno dokumentirane,
- revizijsko listino uradno posredovali revidirancu pri vsakem poslu dajanja zagotovil ali revidiranja IS.

Pojmi

Pojem	Pomen
Posel dajanja zagotovil	Objektivno preiskovanje dokazov, da bi pridobili oceno postopkov upravljanja tveganja, kontroliranja ali upravljanja podjetja. Opomba: primeri lahko vključujejo posle pregledovanja računovodskih izkazov, smotrnosti poslovanja, skladnosti s pravili in posle povezane z varnostjo sistema.
Revizijska listina	Dokument, ki ga odobrijo pristojni za upravljanje in opredeljuje namen, pristojnost in zadolžitev aktivnosti notranjega revidiranja. Revizijska listina naj bi: • vzpostavila položaj notranjega revidiranja v podjetju, • odobrila dostop do zapisov, osebja in fizičnega premoženja, relevantnih za opravljanje poslov dajanja zagotovil in revidiranja IS, • opredelila obseg aktivnosti revidiranja.
Revizijski posel	Posebna revizijska naloga, opravilo ali pregled, npr. revizija, pregled samoocenitve kontrol, preiskava prevare ali svetovanje. Revizijski posel lahko obsega več nalog ali dejavnosti, ki so namenjene doseganju določenega niza povezanih ciljev.
Neodvisnost	Osvobojenost od okoliščin, ki ogrožajo objektivnost ali zaznano objektivnost. Grožnje za objektivnost je treba obvladovati na ravni posameznega revizorja, posla, funkcije ali organizacije. Neodvisnost vključuje neodvisnost mišljenja in zaznano neodvisnost.

Povezava s standardi in smernicami

Vrsta	Naslov
Smernica	2001 Revizijska listina

Datum uveljavitve

Ta standard ISACA velja za vse posle dajanja zagotovil in revidiranja IS, ki se začnejo 1. novembra 2013.

1002 Organizacijska neodvisnost

Zahteve

1002.1 Dajanje zagotovil in revidiranje IS mora biti neodvisno od pregledovanega področja ali aktivnosti, da je omogočeno nepristransko dokončanje posla revidiranja in dajanja zagotovil.

Ključna pojasnila

Dajanje zagotovil in revidiranje IS naj bi:

- v organizaciji revidiranca poročalo na takšni ravni, ki zagotavlja organizacijsko neodvisnost ter dajanju zagotovil in revidiranju IS omogoča izvajanje zadolžitev brez vmešavanja,
- podrobnosti o oslabitvi razkrilo primernim strankam, če je neodvisnost poslabšana dejansko ali po zaznavi,
- se izogibalo vlogam v pobudah v zvezi z IS, ki niso povezane z revidiranjem in zahtevajo prevzem upravljavskih odgovornosti, saj lahko takšne vloge ogrozijo prihodnjo neodvisnost,
- v revizijski listini ali listini o poslu obravnavalo neodvisnost in odgovornosti revidiranja.

Pojmi

Pojem	Pomen
Oslabitev	Stanje, ki povzroča slabost ali zmanjšano sposobnost za doseganje revizijskih ciljev. Oslabitev organizacijske neodvisnosti in objektivnosti posameznika lahko zajema osebna navzkrižja interesov, omejitve obsega delovanja, omejitve dostopa do zapisov, zaposlenih, opreme ali prostorov ter omejitve virov (npr. financiranja ali kadrovanja).
Neodvisnost	Osvobojenost od okoliščin, ki ogrožajo objektivnost ali zaznano objektivnost. Grožnje za objektivnost je treba obvladovati na ravni posameznega revizorja, posla, funkcije ali organizacije. Neodvisnost vključuje neodvisnost mišljenja in zaznano neodvisnost.
Zaznana neodvisnost	Izogibanje dejstvom in okoliščinam, ki so tako pomembni, da bi lahko razumna in obveščena tretja stranka, ki bi pretehtala vsa specifična dejstva in okoliščine, samostojno sklepala, da je ogrožena poštenost, objektivnost ali poklicna nezaupljivost podjetja, revidiranja ali člana revizijske skupine.
Neodvisnost mišljenja	Miselna naravnanost, ki omogoča sprejemanje sklepov neodvisno od vplivov, ki bi lahko ogrozili strokovno presojo, ter posledično posamezniku pri njegovem ravnanju omogoča poštenost, objektivnost in poklicno nezaupljivost.
Objektivnost	Zmožnost nepristranskega presojanja, izražanja mnenja in podajanja priporočil.

Povezava s standardi in smernicami

Vrsta	Naslov
Smernica	2002 Organizacijska neodvisnost

Datum uveljavitve

Ta standard ISACA velja za vse posle dajanja zagotovil in revidiranja IS, ki se začnejo 1. novembra 2013.

1003 Strokovna neodvisnost

Zahteve

1003.1 Strokovnjaki dajanja zagotovil in revidiranja IS morajo biti tako dejansko kot po zaznavi neodvisni in objektivni v vseh zadevah, povezanih s posli revidiranja in dajanja zagotovil.

Ključna pojasnila

Strokovnjaki dajanja zagotovil in revidiranja IS naj bi:

- izvajali posle dajanja zagotovil ali revidiranja IS nepristransko in brez predsodkov pri obravnavi zadev v zvezi z zagotovili in pri oblikovanju sklepov,
- bili dejansko neodvisni in bili hkrati ves čas zaznani kot neodvisnosti,
- podrobnosti o oslabitvi razkrili primernim strankam, če je neodvisnost poslabšana dejansko ali po zaznavi,
- s poslovodstvom in revizijsko komisijo, če je ta vzpostavljena, redno ocenjevali neodvisnost,
- se izogibali vlogam v pobudah v zvezi z IS, ki niso povezane z revidiranjem in zahtevajo prevzem upravljavskih odgovornosti, saj lahko takšne vloge ogrozijo prihodnjo neodvisnost.

Pojmi

Pojem	Pomen
Oslabitev	Stanje, ki povzroča slabost ali zmanjšano sposobnost za doseganje revizijskih ciljev. Oslabitev organizacijske neodvisnosti in objektivnosti posameznika lahko zajema osebna navzkrižja interesov, omejitve obsega delovanja, omejitve dostopa do zapisov, zaposlenih, opreme ali prostorov ter omejitve virov (npr. financiranja ali kadrovanja).
Neodvisnost	Osvobojenost od okoliščin, ki ogrožajo objektivnost ali videz nepristranskosti. Grožnje za objektivnost je treba obvladovati na ravni posameznega revizorja, posla, funkcije ali organizacije. Neodvisnost vključuje neodvisnost mišljenja in videz neodvisnosti.
Zaznana neodvisnosti	Izogibanje dejstvom in okoliščinam, ki so tako pomembni, da bi lahko razumna in obveščena tretja stranka, ki bi pretehtala vsa specifična dejstva in okoliščine, samostojno sklepala, da je ogrožena poštenost, objektivnost ali poklicna nezaupljivost podjetja, revidiranja ali člana revizijske skupine.
Neodvisnost mišljenja	Miselna naravnanost, ki omogoča sprejemanje sklepov neodvisno od vplivov, ki bi lahko ogrozili strokovno presojo, ter posledično posamezniku pri njegovem ravnanju omogoča poštenost, objektivnost in poklicno nezaupljivost.
Objektivnost	Zmožnost nepristranskega presojanja, izražanja mnenja in podajanja priporočil.

Povezava s standardi in smernicami

Vrsta	Naslov
Smernica	2003 Strokovna neodvisnost

Datum uveljavitve

Ta standard ISACA velja za vse posle dajanja zagotovil in revidiranja IS, ki se začnejo 1. novembra 2013.

1004 Upravičeno pričakovanje

Zahteve

1004.1 Strokovnjaki dajanja zagotovil in revidiranja IS morajo imeti razumno pričakovanje, da je lahko posel izveden skladno s standardi dajanja zagotovil in revidiranja IS ter po potrebi skladno z drugimi ustreznimi strokovnimi in panožnimi standardi ali veljavnimi predpisi in da bo rezultat strokovno mnenje ali sklep.

1004.2 Strokovnjaki dajanja zagotovil in revidiranja IS morajo imeti razumno pričakovanje, da je glede na obseg posla možno sklepati o obravnavani zadevi in upoštevati kakršne koli omejitve.

1004.3 Strokovnjaki dajanja zagotovil in revidiranja IS morajo imeti razumno pričakovanje, da se organ vodenja zaveda svojih obveznosti in zadolžitev pri zagotavljanju ustreznih, relevantnih in pravočasnih informacij, ki so potrebne za izvedbo posla.

Ključna pojasnila

Strokovnjaki dajanja zagotovil in revidiranja IS naj bi:

- sprejeli posle dajanja zagotovil in revidiranja IS samo, če je mogoče delo uspešno zaključiti skladno s strokovnimi standardi,
- sprejeli posel dajanja zagotovil in revidiranja IS samo, če je mogoče obravnavano zadevo oceniti na osnovi ustreznih meril,
- pregledali obseg posla dajanja zagotovil in revidiranja IS ter ugotovili, ali je jasno dokumentiran in strokovnjaku omogoča sklepanje o obravnavani zadevi,
- prepoznali in upoštevali vsakršne omejitve posla, ki ga je treba izvesti, vključno z dostopom do ustreznih, relevantnih in pravočasnih informacij,
- preučili ali obseg omogoča, da izrazijo mnenje revizorja o obravnavani zadevi.
  Omejitev obsega se lahko pojavi, ko informacije, potrebne za dokončanje posla niso na voljo, ko je časovni okvir dajanja zagotovil in revidiranja IS nezadosten ali ko organ vodenja poskuša omejiti obseg na izbrana področja. V takih primerih je mogoče razmisliti o drugih vrstah poslov, kot so podpora revidiranim finančnim poročilom, pregled kontrol, skladnost z zahtevanimi standardi in praksami ali skladnost s sporazumi, licencami, zakonodajo ali predpisi.

Pojmi

Pojem	Pomen
Mnenje revizorja	Uradna izjava strokovnjaka dajanja zagotovil in revidiranja IS, ki opisuje obseg revizije, uporabljene postopke za pripravo poročila ter ali ugotovitve podpirajo izpolnjevanje meril revizije ali ne. Vrste mnenj so: • **Pozitivno mnenje** – brez ugotovljenih izjem oziroma nobena od ugotovljenih izjem ne predstavlja pomembne pomanjkljivosti; • **Mnenje s pridržki** – ugotovljene izjeme, ki skupaj predstavljajo pomembno pomanjkljivost (vendar ne bistvene slabosti); • **Odklonilno mnenje** – ugotovljeno eno ali več pomembnih pomanjkljivosti, ki skupaj tvorijo bistveno slabost. Opomba: zavrnitev mnenja se izda, ko revizor ne more pridobiti dovolj ustreznih revizijskih dokazov, na podlagi katerih bi lahko oblikoval mnenje, ali ko mnenja ni mogoče oblikovati zaradi možnih interakcij več negotovosti in njihovega morebitnega skupnega vpliva.

Povezava s standardi in smernicami

Vrsta	Naslov
Smernica	2004 Upravičeno pričakovanje

Datum uveljavitve

Ta standard ISACA velja za vse posle dajanja zagotovil in revidiranja IS, ki se začnejo 1. novembra 2013.

1005 Dolžna poklicna skrbnost

Zahteve

1005.1 Strokovnjaki dajanja zagotovil in revidiranja IS morajo pri načrtovanju in izvajanju poslov ter poročanju o njihovih izidih spoštovati dolžno poklicno skrbnost, vključno z upoštevanjem veljavnih strokovnih standardov za revizijo.

Ključna pojasnila

Strokovnjaki dajanja zagotovil in revidiranja IS naj bi:
- posle opravljali ob upoštevanju poštenosti in skrbnosti,
- pokazali zadostno mero razumevanja in usposobljenosti za doseganje ciljev posla,
- ohranili poklicno nezaupljivost pri celotni izvedbi posla,
- ohranjali strokovno usposobljenost s pomočjo spremljanja strokovnih standardov in upoštevanjem njihovega razvoja,
- članom skupine sporočili njihove vloge in odgovornosti ter zagotavljali, da bo ekipa upoštevala ustrezne standarde pri izvajanju posla,
- upoštevali vse nejasnosti v zvezi z uporabo standardov med izvajanjem posla,
- ves čas opravljanja posla ohranjali učinkovito komunikacijo z relevantnimi deležniki,
- sprejeli primerne ukrepe za varovanje informacij, pridobljenih ali izpeljanih med izvajanjem posla, pred nenamernim razkritjem ali posredovanjem nepooblaščenim osebam,
- vse posle opravljali ob upoštevanju dajanja zadostnih zagotovil. Raven preizkušanja bo odvisna od vrste posla.

Opomba: dolžna poklicna skrbnost pomeni primerno skrb in usposobljenost, in ne nezmotljivosti ali izjemne uspešnosti.

Pojmi

Pojem	Pomen
Poklicna nezaupljivost	Pristop, ki vključuje dvom in kritično ocenjevanje revizijskih dokazov. Vir: Ameriški inštitut preizkušenih javnih računovodij (AICPA) AU 230.07

Povezava s standardi in smernicami

Vrsta	Naslov
Smernica	2005 Dolžna poklicna skrbnost

Datum uveljavitve

Ta standard ISACA velja za vse posle dajanja zagotovil in revidiranja IS, ki se začnejo 1. novembra 2013.

1006 Strokovna usposobljenost

Zahteve

1006.1 Strokovnjaki dajanja zagotovil in revidiranja IS morajo imeti skupaj z ostalimi sodelavci pri nalogi ustrezne veščine ter strokovno usposobljenost za izvedbo poslov dajanja zagotovil in revidiranja IS ter biti strokovno usposobljeni za opravljanje zahtevanega dela.

1006.2 Strokovnjaki dajanja zagotovil in revidiranja IS morajo skupaj s sodelavci pri nalogi posedovati ustrezno znanje o obravnavani zadevi.

1006.3 Strokovnjaki dajanja zagotovil in revidiranja IS morajo ohranjati strokovno usposobljenost z ustreznim nenehnim strokovnim izobraževanjem in usposabljanjem.

Ključna pojasnila

Strokovnjaki dajanja zagotovil in revidiranja IS naj bi:

- dokazali zadostno strokovno usposobljenost (spretnosti, znanje in izkušnje, ki so pomembne za načrtovani posel) pred začetkom dela,
- ocenili alternativne načine za pridobivanje spretnosti, vključno z najemom podizvajalcev, zunanjim izvajanjem dela nalog, preložitvijo začetka naloge, dokler ne pridobijo potrebnih spretnosti ali na drugačen način zagotovijo ustreznih spretnosti,
- zagotovili, da bodo člani skupine, ki nimajo niti naziva CISA niti drugega primernega strokovnega naziva ter sodelujejo pri poslu dajanja zagotovil in revidiranja IS, imeli zadostno formalno izobrazbo, usposobljenost in delovne izkušnje,
- pri vodenju skupine za izvedbo posla dajanja zagotovil in revidiranja IS v zadostni meri zagotavljali, da bodo vsi člani skupine ustrezno usposobljeni za opravljanje dodeljenega dela,
- dovolj dobro poznali ključna področja z namenom uspešne in učinkovite izvedbe posla dajanja zagotovil in revidiranja IS skupaj z morebitnimi specialisti in drugimi člani skupine,
- ves čas izpolnjevali zahteve glede strokovne izobrazbe ali razvoja, ki jih določa naziv CISA ali drugi primerni strokovni nazivi,
- redno izpopolnjevali strokovno znanje s pomočjo izobraževalnih tečajev, seminarjev, konferenc, spletnih oddaj in usposabljanja na delovnem mestu ter tako zagotavljali ustrezno raven strokovnih storitev, ki izpolnjujejo zahteve vloge dajanja zagotovil ali revidiranja IS.

Pojmi

Pojem	Pomen
Usposobljenost	Zmožnost za uspešno izvedbo določenega opravila, dejanja ali funkcije.
Strokovna usposobljenost	Spretnosti in izkušnje.

Povezava s standardi in smernicami

Vrsta	Naslov
Smernica	2006 Strokovna usposobljenost

Datum uveljavitve

Ta standard ISACA velja za vse posle dajanja zagotovil in revidiranja IS, ki se začnejo 1. novembra 2013.

1007 Trditve

Zahteve

1007.1 Strokovnjaki dajanja zagotovil in revidiranja IS morajo pregledati trditve, na podlagi katerih bodo presojali obravnavano zadevo, z namenom, da bi ugotovili ali je mogoče takšne trditve revidirati in ali so te trditve zadostne, veljavne in relevantne.

Ključna pojasnila

Strokovnjaki dajanja zagotovil in revidiranja IS naj bi:

- ovrednotili merila, na podlagi katerih bodo ocenili obravnavano zadevo, ter tako zagotovili, da podpirajo trditve,
- ugotovili, ali je trditve mogoče revidirati in ali jih informacije podpirajo,
- ugotovili, ali trditve temeljijo na merilih, ki so ustrezno opredeljena ter so predmet objektivne in merljive analize,
- zagotovili, da trditve ustrezajo pričakovanjem bralca ali uporabnika z zadostnim znanjem, kadar jih primerja z drugimi standardi formalnih določil, če je trditve oblikovalo poslovodstvo,
- zagotovili, da je trditve preverilo in potrdilo poslovodstvo, če so trditve navedle tretje stranke, ki upravljajo kontrole v imenu podjetja,
- poročali neposredno na podlagi obravnavane zadeve (neposredno poročilo) ali na podlagi trditve o obravnavani zadevi (posredno poročilo),
- sprejeli sklep o vsaki trditvi na podlagi niza izsledkov, ki temeljijo na merilih in strokovni presoji.

Pojmi

Pojem	Pomen
Trditev	Kakršna koli uradna izjava ali skupek izjav poslovodstva o obravnavani zadevi. Trditve naj bi bile pisne in naj bi načeloma vsebovale seznam posebnih lastnosti o obravnavani zadevi ali procesu, ki se nanaša na obravnavano zadevo.

Povezava s standardi in smernicami

Vrsta	Naslov
Smernica	2007 Trditve

Datum uveljavitve

Ta standard ISACA velja za vse posle dajanja zagotovil in revidiranja IS, ki se začnejo 1. novembra 2013.

1008 Merila

Zahteve

1008.1 Strokovnjaki dajanja zagotovil in revidiranja IS morajo izbrati merila, glede na katera se bo obravnavana zadeva presojala in ki so: nepristranska, celovita, relevantna, izmerljiva, razumljiva, splošno priznana, izdana s strani pristojnih organov in razumljiva ter na voljo vsem bralcem in uporabnikom poročila.

1008.2 Strokovnjaki dajanja zagotovil in revidiranja IS morajo upoštevati vire meril in se, preden sprejmejo manj znana merila, osredotočiti na tiste, ki jih objavijo relevantni pristojni organi.

Ključna pojasnila

Strokovnjaki dajanja zagotovil in revidiranja IS naj bi:

- temeljito razmislili o izbiri meril in bili sposobni utemeljiti svojo izbiro,
- se sklicevali na strokovno presojo pri zagotavljanju, da bodo merila, če veljajo, omogočala pripravo poštenega in objektivnega mnenja ali sklepa, ki ne bo zavajal bralca ali uporabnika. Znano je, da lahko poslovodstvo določi merila, ki ne izpolnjujejo vseh zahtev;
- preučili primernost in razpoložljivost meril, kot jih določa zahtevnost posla;
- če merila niso na voljo, so nepopolna ali predmet osebne razlage, bodo v poročilo dodatno vključili še kontekst, v katerem so merila uporabljena ter vključili opis in kakršne koli druge informacije, ki so potrebne za zagotovitev poštenosti, objektivnosti in razumljivosti poročila.

Primernost in ustreznost meril za presojo obravnavane zadeve je treba oceniti glede na naslednjih pet meril ustreznosti:

- **Objektivnost** – merila naj bi bila nepristranska, s čimer ne bi neugodno vplivala na ugotovitve in sklepe strokovnjakov ter skladno s tem ne bi zavajala uporabnikov, ki berejo poročilo;
- **Popolnost** – merila naj bi bila dovolj popolna, tako da so opredeljena vsa merila in kriteriji, ki bi ob upoštevanju pri izvedbi lahko vplivali na strokovno oceno pri izvajanju dajanja zagotovil in revidiranja z IS;
- **Relevantnost** – merila naj bi bila relevantna za obravnavano zadevo in naj bi prispevala k ugotovitvam in sklepom, ki izpolnjujejo cilje dajanja zagotovil in revidiranja IS;
- **Merljivost** – merila naj bi omogočala konsistentno merjenje obravnavane zadeve in pripravo konsistentnih sklepov, če jih različni strokovnjaki uporabijo v podobnih okoliščinah;
- **Razumljivost** – merila naj bi bila jasno sporočena in jih zadevni uporabniki naj ne bi razlagali preveč različno.

Na sprejemljivost meril vpliva njihova razpoložljivost uporabnikom strokovnega poročila, tako da lahko razumejo podlago za dajanje zagotovil ter relevantnost ugotovitev in sklepov. Viri lahko vključujejo merila, ki so:

- **priznana** – merila naj bi bila ustrezno priznana, tako da zadevni uporabniki ne bi podvomili o njihovi uporabi;
- **izdana s strani pristojnih organov** – poiskati bi bilo treba merila, ki izražajo veljavna formalna načela znotraj področja in ustrezajo zadevi. Formalna načela lahko npr. predpišejo strokovni organi, panožne skupine, vlada in upravni organi;
- **javno dostopna** – merila naj bi bila na voljo uporabnikom strokovnjakovega poročila. Primeri vključujejo standarde, ki so jih razvili strokovni računovodski in revizijski organi, kot so ISACA, Mednarodna zveza računovodskih strokovnjakov (IFAC) in drugi priznani vladni ali strokovnimi organi;
- **na voljo vsem uporabnikom** – če merila niso javno dostopna, bi bilo treba z njimi seznaniti vse uporabnike s pomočjo »trditev«, ki predstavljajo del strokovnega poročila. Trditve vključujejo izjave o obravnavani zadevi, ki izpolnjujejo zahteve »primernih meril«, tako da jih je mogoče revidirati.

1008 Merila *(nadaljevanje)*

Ključna pojasnila (nadaljevanje)

Poleg ustreznosti in razpoložljivost naj bi se pri izbiri meril za dajanje zagotovil IS upošteval tudi njihov vir v smislu njihove uporabe in potencialnih naslovnikov. Če se npr. spopadate s predpisi, je najprimerneje uporabiti merila, ki temeljijo na trditvah, pripravljenih na podlagi zakonodaje in predpisov, ki veljajo za obravnavano zadevo. Spet v drugih primerih pa so lahko relevantna merila panožnih ali trgovinskih združenj. Možni viri meril, ki so navedena v vrstnem redu njihovega upoštevanja, so:

- **Merila, ki jih določa ISACA** – to so javno dostopna merila in standardi, ki so jih pregledali in s potrebno poklicno skrbnostjo preverili mednarodno priznani strokovnjaki s področja vodenja, nadzora, varnosti IT in dajanja zagotovil;
- **Merila, ki jih določajo drugi strokovni organi** – ta merila podobno kot standardi in merila, ki jih je določila ISACA, veljajo za obravnavano zadevo ter so jih razvili strokovnjaki z najrazličnejših področij in so bila preverjena v procesu, ki zagotavlja ustrezno poklicno skrbnost;
- **Merila, ki jih določajo zakoni in predpisi** – čeprav lahko zakoni in predpisi predstavljajo podlago za merila, jih je treba uporabljati previdno. Njihovo besedilo je pogosto zapleteno in ima specifičen pravni pomen. Pogosto je treba pravna določila preoblikovati v trditve. Poleg tega lahko tolmačenje zakonodaje podajo samo člani pravne stroke.
- **Merila, ki jih določajo podjetja, ki ne sledijo predpisanim postopkom** – ta vključujejo relevantna merila, ki so jih pripravila druga podjetja, ki ne sledijo predpisanim postopkom skrbnega pregleda ter niso predmet javnega posvetovanja in razprave;
- **Merila, ki so bila razvita posebej za posel dajanja zagotovil ali revizije IS** – čeprav so lahko merila, pripravljena posebej za dajanje zagotovil in revidiranja IS, povsem ustrezna, je treba zlasti poskrbeti, da ta merila izpolnjujejo merila ustreznosti, zlasti popolnosti, merljivosti in objektivnosti. Merila, pripravljena posebej za dajanje zagotovil in revidiranja IS, so pripravljena v obliki trditev.

Izbrana merila je treba skrbno preučiti. Čeprav je upoštevanje lokalnih zakonov in predpisov pomembno in mora spadati med obvezne zahteve, je sprejeto dejstvo, da številni posli revidiranja in dajanja zagotovil IS vključujejo področja, kot so upravljanje sprememb, splošne kontrole IT in kontrole dostopa, ki jih ne pokrivajo zakoni ali predpisi. Poleg tega so nekatere panoge, kot na primer področje plačilnih kartic, vzpostavile obvezne zahteve, ki jih je treba upoštevati. Kadar zakonske zahteve temeljijo na načelih, naj bi strokovnjaki zagotovili, da izbrana merila izpolnjujejo cilje posla.

Pri izvajanju posla se lahko na podlagi dodatnih informacij ugotovi, da nekatera merila ne bodo potrebna za dosego ciljev. V teh okoliščinah nadaljnje delo v zvezi z merili ni potrebno.

Pojmi

Pojem	Pomen
Merila	Standardi in merila uspešnosti, ki se uporabljajo za merjenje in predstavitev obravnavane zadeve ter ki jih revizor IS uporablja za vrednotenje zadeve. Merila naj bi bila: • objektivna – nepristranska, • popolna – vključevala naj bi vse relevantne dejavnike, ki vodijo do sklepa, • relevantna – morajo se nanašati na obravnavano zadevo, • merljiva – zagotavljala naj bi dosledno merjenje, • razumljiva. Pri poslih potrjevanja so to merila uspešnosti, s katerim je moč preveriti pisne trditve poslovodstva glede obravnavane zadeve. Izvajalec pride do zaključka o obravnavani zadevi na podlagi primerjave z ustreznimi merili.

Povezava s standardi in smernicami

Vrsta	Naslov
Smernica	2008 Merila

Datum uveljavitve

Ta standard ISACA velja za vse posle dajanja zagotovil in revidiranja IS, ki se začnejo 1. novembra 2013.

Izvedbeni standardi

Izvedbeni standardi določajo osnovna pričakovanja pri dajanju zagotovil in revidiranju IS. Medtem ko ti standardi veljajo za strokovnjake dajanja zagotovil in revidiranja IS, ki opravljajo katero koli nalogo dajanja zagotovil in revidiranja IS, je skladnost pomembna zlasti pri opravljanju revizije. Posledično se izvedbeni standardi osredotočajo na pozornost strokovnjaka dajanja zagotovil in revidiranja IS na načrt in izvajanje dajanja zagotovil, zahtevane dokaze ter pripravo ugotovitev in sklepov pri dajanju zagotovil in revidiranju IS.

Izvedbeni standardi so naslednji:
1201 Načrtovanje posla
1202 Ocenjevanje tveganja pri načrtovanju
1203 Izvedba in nadzor
1204 Pomembnost
1205 Dokazi
1206 Uporaba dela drugih strokovnjakov
1207 Nepravilnosti in nezakonita dejanja

Standard so tukaj vključeni v celoti. Podčrtane besede so opredeljene v poglavju s pojmi. Za povezave do posameznih standardov obiščite spletno stran *www.isaca.org/standard.*

1201 Načrtovanje posla

Zahteve

1201.1 Strokovnjaki dajanja zagotovil in revidiranja IS morajo načrtovati vsak posel dajanja zagotovil in revidiranja IS z namenom, da opredelijo:
- **cilj/-e, obseg, časovni načrt in izdelke,**
- **skladnost z veljavnimi zakoni in strokovnimi revizijskimi standardi,**
- **uporabo na tveganjih temelječega pristopa, kjer je to primerno,**
- **vprašanja, ki so lastna poslu,**
- **zahteve glede dokumentacije in poročanja.**

1201.2 Strokovnjaki dajanja zagotovil in revidiranja IS morajo razviti in dokumentirati projektni načrt posla dajanja zagotovil in revidiranja IS, ki opisuje:
- **vrsto posla, cilje, časovni načrt in zahteve glede virov,**
- **časovno razporeditev in obseg revizijskih postopkov za izvedbo posla.**

Ključna pojasnila

Strokovnjaki dajanja zagotovil in revidiranja IS naj bi:
- razumeli dejavnost, ki je predmet revizije. Obseg potrebnega znanja je treba določiti glede na vrsto podjetja, njegovo okolje, področja tveganja in cilje posla;
- upoštevali smernice ali usmeritve o obravnavani zadevi, kot to dovoljujejo zakonodaja, predpisi, pravila ter direktive in smernice, ki jih izda vlada ali gospodarska panoga,
- izvedli oceno tveganj za zadostno zagotovilo, da se bodo pri poslu upoštevale vse ključne postavke. Na tej podlagi je mogoče pripraviti strategijo za izvedbo posla, ravni pomembnosti in zahteve glede virov;
- razvili projektni načrt posla z uporabo ustreznih metodologij projektnega vodenja za zagotovitev, da dejavnosti potekajo po načrtih in v okviru proračuna;
- v načrt vključili vprašanja, ki so lastna poslu, kot so:
  – razpoložljivost kadrov z ustreznim znanjem, spretnostmi in izkušnjami;
  – določitev potrebnih orodij za zbiranje dokazov, izvajanje preizkusov in pripravo/povzemanje informacij za poročanje;
  – ocenjevalna merila, ki jih je treba uporabiti;
  – zahteve glede poročil in njihovih prejemnikov;
- dokumentirali projektni načrt za izvedbo posla dajanja zagotovil in revidiranja IS z namenom jasno določiti naslednje:
  – cilj/-e, obseg in časovno razporeditev;
  – vire;
  – vloge in zadolžitve;
  – ugotovljena področja tveganj in njihov vpliv na načrt posla;
  – orodja in tehnike, ki jih je treba uporabiti;
  – predvidene razgovore za razjasnitev dejstev, ki jih je treba izvesti;
  – pridobitev relevantnih informacij;
  – postopke za preverjanje ali vrednotenje pridobljenih informacij in za njihovo uporabo v dokazilih;
  – predpostavke glede pristopa, metodologije, postopkov in pričakovanih rezultatov ter sklepov;
- načrtovali posel upoštevaje časovno razporeditev, razpoložljivost ter druge obveznosti in zadolžitve poslovodstva in revidiranca, če je le mogoče,
- prilagodili projektni načrt med izvajanjem posla dajanja zagotovil in revidiranja IS z namenom obravnave zadev, ki se odkrijejo med poslom, kot so nova tveganja, napačne predpostavke ali ugotovitve že izvedenih postopkov;
- za notranje posle:
  – revidiranca seznanili z revizijsko listino, po potrebi pa uporabili listino o poslu ali podoben dokument z namenom vnaprejšnje razjasnitve in potrditve sodelovanja pri specifičnih poslih;
  – revidiranca seznanili z načrtom, da bo ta v celoti seznanjen z obravnavano zadevo in bo lahko po potrebi zagotovil ustrezen dostop do posameznikov, dokumentacije in drugih virov;
- za zunanje posle:
  – pripravili ločene listine o poslu za vsak zunanji posel dajanja zagotovil in revidiranja IS;
  – pripravili projektni načrt za vsak zunanji posel dajanja zagotovil in revidiranja IS. Načrt naj bi dokumentiral vsaj cilj/-e in obseg posla.

Povezava s standardi in smernicami

Vrsta	Naslov
Smernica	2201 Načrtovanje posla

Datum uveljavitve

Ta standard ISACA velja za vse posle dajanja zagotovil in revidiranja IS, ki se začnejo 1. novembra 2013.

1202 Ocenjevanje tveganja pri načrtovanju

Zahteve

1202.1 Pri dajanju zagotovil in revidiranju IS morata biti za razvoj celotnega načrta revidiranja IS in določitev prioritet za učinkovito dodelitev virov za revizijo IS uporabljena ustrezen pristop in pripadajoča metodologijo za oceno tveganja.

1202.2 Strokovnjaki dajanja zagotovil in revidiranja IS morajo pri načrtovanju posameznih poslov prepoznati in oceniti tveganje, relevantno za področje pregleda.

1202.3 Strokovnjaki dajanja zagotovil in revidiranja IS morajo preučiti tveganja povezana z obravnavano zadevo, revizijsko tveganje in vpliv na izpostavljenost podjetja.

Ključna pojasnila

Za dajanje zagotovil in revidiranje IS naj bi pri načrtovanju tekočih aktivnosti:

- vsaj enkrat na leto izvedli in dokumentirali oceno tveganja za lažjo pripravo revizijskega načrta za področje IS,
- vključili strateške načrte in cilje organizacije ter okvir in pobude za obvladovanje tveganj podjetja, kot del ocene tveganj,
- za vsak posel dajanja zagotovil in revidiranja IS ocenili in utemeljili količino virov revidiranja IS, ki so potrebni za izpolnitev zahtev posla,
- uporabili oceno tveganj pri izbiri področij in elementov, ki potrebujejo pozornost revizorja, ter odločitvi za načrtovanje in izvedbo določenih poslov dajanja zagotovil in revidiranja IS,
- pridobili potrditev ocene tveganj od deležnikov pri reviziji in drugih primernih strank,
- določili prednostne naloge in izdelali časovni načrt izvedbe revizije IS na podlagi ocene tveganj,
- na podlagi ocene tveganj pripravili načrt, ki:
  - služi kot okvir za aktivnosti dajanja zagotovil in revidiranja IS;
  - upošteva zahteve in aktivnosti dajanja zagotovil in revidiranja, ki niso povezane z IS;
  - bo posodobljen vsaj enkrat na leto in ga bodo odobrili pristojni za upravljanje;
  - obravnava zadolžitve, določene z revizijsko listino.

Strokovnjaki dajanja zagotovil in revidiranja IS naj bi pri načrtovanju posameznega posla:

- prepoznali in ocenili tveganje, ki se nanaša na področje pregleda;
- za vsak posel opravili predhodno oceno tveganja, ki se nanaša na področje pregleda. Cilji za vsak posamezni posel naj bi odražali rezultate predhodne ocene tveganj;
- pri določanju področij tveganj in načrtovanju posameznega posla upoštevali predhodne revizije, preglede in ugotovitve, vključno z že izvedenimi ukrepi. Upoštevali naj bi tudi splošni proces ocenjevanja tveganj, ki ga uporablja vodstvo;
- poskušali zmanjšati revizijsko tveganje na sprejemljivo raven ter izpolniti cilje revizije z ustrezno oceno z IS povezane obravnavane zadeve in povezanih kontrol z načrtovanjem in izvajanjem revizije IS;
- pri načrtovanju določenega postopka revidiranja IS upoštevali, da nižji ko je prag pomembnosti, natančnejša so revizijska pričakovanja in večje je revizijsko tveganje;
- za zmanjšanje tveganja večje pomembnosti lahko razširimo obseg preizkusa kontrol (zmanjšamo tveganje pri nadzoru) in/ali razširimo postopke preizkušanja podatkov (zmanjšamo tveganje pri odkrivanju), da bi pridobili dodatno zagotovila.

Pojmi

Pojem	Pomen
Revizijska listina	Dokument, ki ga odobrijo pristojni za upravljanje in opredeljuje namen, pristojnost in zadolžitve aktivnosti notranjega revidiranja. Revizijska listina naj bi: • vzpostavila položaj notranjega revidiranja v podjetju, • odobrila dostop do zapisov, osebja in fizičnega premoženja, relevantnih za opravljanje poslov dajanja zagotovil in revidiranja IS, • opredelila obseg aktivnosti revidiranja.
Revizijsko tveganje	Tveganje za sprejem nepravilnega sklepa na podlagi ugotovitev revizije. Tri komponente revizijskega tveganja so: • tveganje pri kontroliranju, • tveganje pri odkrivanju, • tveganje pri delovanju.

1202 Ocenjevanje tveganja pri načrtovanju *(nadaljevanje)*

Pojmi

Pojem	Pomen
Tveganje revizijskega področja	Tveganja, ki se nanašajo na revidirano področje: • poslovno tveganje (sposobnost kupca za plačilo, kreditna sposobnost, tržni dejavniki itd.), • pogodbeno tveganje (odgovornost, cena, vrsta, kazni itd.), • deželno tveganje (politika, okolje, varnost itd.), • projektno tveganje (viri, spretnosti, metodologija, stabilnost izdelka itd.), • tehnološko tveganje (rešitev, arhitektura, omrežje strojne in programske infrastrukture, distribucijski kanali itd.). Glejte tveganje pri delovanju.
Tveganje pri kontroliranju	Tveganje, da obstaja materialna napaka, ki je sistem notranjih kontrol ne more preprečiti ali pravočasno zaznati. Glejte tveganje pri delovanju.
Tveganje pri odkrivanju	Tveganje, da strokovnjak dajanja zagotovil ali revidiranja IS s postopki preizkušanja podatkov ne bo odkril napake, ki bi lahko bila pomembna, sama ali v kombinaciji z drugimi napakami. Glejte revizijsko tveganje.
Tveganje pri delovanju	Raven tveganja ali izpostavljenost, ne upoštevaje dejanja, ki jih je poslovodstvo izvedlo ali bi jih lahko izvedlo (npr. uvajanje kontrol). Glejte tveganje pri nadzoru.
Pomembnost (materialnost)	Revizijski koncept, ki zadeva pomembnost informacije glede na njen vpliv ali učinek na delovanje revidirane enote. Izraz relativne pomembnosti ali pomembnosti za neko določeno zadevo v kontekstu podjetja kot celote.
Ocena tveganja	Postopek, ki se uporablja za prepoznavanje in oceno tveganja in njegovih možnih vplivov. Ocene tveganj se uporabljajo za prepoznavanje elementov ali področij, ki predstavljajo največje tveganje, ranljivost ali izpostavljenost podjetja za uvrstitev v letni načrt revizije IS. Ocene tveganj se uporabljajo tudi za obvladovanje tveganja za uspešno dokončanje projekta in doseganje predvidenih prednosti.
Preizkušanje podatkov	Pridobivanje revizijskih dokazov o popolnosti, točnosti ali obstoju aktivnosti ali transakcij v obdobju revidiranja.

Povezava s standardi in smernicami

Vrsta	Naslov
Smernica	2202 Ocenjevanje tveganja pri načrtovanju

Datum uveljavitve

Ta standard ISACA velja za vse posle dajanja zagotovil in revidiranja IS, ki se začnejo 1. novembra 2013.

1203 Izvedba in nadzor

Zahteve

1203.1 Zato, da zajamejo prepoznana tveganja, morajo strokovnjaki dajanja zagotovil in revidiranja IS delo opraviti skladno z odobrenim načrtom revidiranja IS in v dogovorjenih rokih.

1203.2 Z namenom, da se dosežejo revizijski cilji in spoštujejo veljavni strokovni revizijski standardi, morajo strokovnjaki dajanja zagotovil in revidiranja IS nadzirati osebje, ki izvaja revizije IS in za katero so zadolženi.

1203.3 Strokovnjaki dajanja zagotovil in revidiranja IS lahko sprejmejo samo naloge, ki so v okviru njihovega strokovnega znanja in veščin ali naloge, za katere imajo upravičeno pričakovanje, da bodo veščine pridobili v teku posla ali da jih bodo opravili pod nadzorom.

1203.4 Za doseganje revizijskih ciljev morajo strokovnjaki dajanja zagotovil in revidiranja IS pridobiti zadostne in ustrezne dokaze. Ugotovitve in sklepi revizije morajo biti podprti z ustreznimi analizami in razlago teh dokazov.

1203.5 Strokovnjaki dajanja zagotovil in revidiranja IS morajo revizijski postopek dokumentirati z opisi revizijskega dela in revizijskimi dokazi, ki podpirajo ugotovitve in sklepe.

1203.6 Strokovnjaki dajanja zagotovil in revidiranja IS morajo prepoznavati in sklepati na podlagi ugotovitev.

Ključna pojasnila

Strokovnjaki dajanja zagotovil in revidiranja IS naj bi:

- dodelili člane skupine s spretnostmi in izkušnjami, ki ustrezajo zahtevam posla,
- v ekipo za revizijo IS vključili zunanje vire, kadar je to primerno, in zagotovili, da bo njihovo delo ustrezno nadzorovano,
- upravljali vloge in odgovornosti posameznih članov skupine za revizijo IS ves čas trajanja posla, pri čemer je treba obravnavati vsaj:
  - vloge za izvedbo in pregled,
  - zadolžitev za pripravo metodologije in pristopa,
  - pripravo revizijskih programov ali programov dajanja zagotovil,
  - izvedbo dela,
  - sprotno reševanje vprašanj, pomislekov in težav,
  - dokumentiranje in pojasnjevanje ugotovitev,
  - pisanje poročil;
- poskrbeli, da vsako nalogo revizijskega posla opravi en član ali več članov ekipe in nato pregleda drug usposobljen član ekipe,
- uporabili najboljše revizijske dokaze, ki jih je mogoče pridobiti, glede na pomembnost revizijskih ciljev, čas in trud potreben za pridobitev teh dokazov,
- pridobili dodatne dokaze, če se predhodno pridobljeni dokazi po strokovni presoji ne izkažejo za zadostne in ustrezne, da bi bilo mogoče na njihovi podlagi pripraviti mnenje ali z njimi podpreti ugotovitve in sklepe,
- organizirali in dokumentirali opravljeno delo med izvajanjem posla, pri čemer je treba upoštevati predhodno določene, dokumentirane in odobrene postopke,
- v dokumentacijo vključili:
  - cilje revizije in obseg dela, program revizije, izvedene korake revizije, zbrane dokaze, ugotovitve, sklepe in priporočila;
  - dovolj podrobnosti, ki bi skrbni in obveščeni osebi omogočale ponovno izvedbo postopkov, ki so bili že izvedeni v okviru posla, s čimer bi prišla do enakih ugotovitev;
  - opredelitev tega, kdo je opravil posamezno nalogo in kakšna je bila njegova vloga pri pripravi in pregledu dokumentacije;
  - datum priprave in pregleda dokumentacije;
- pridobili ustrezne pisne izjave revidiranca, ki podrobno navajajo kritična področja posla, vprašanja, ki so se pojavila, in odgovore nanje ter trditve revidiranca,
- ugotovili, ali so izjave revidiranca tudi ustrezno podpisane in datirane, s čimer revidiranec potrjuje svoje obveznosti v zvezi s poslom,
- dokumentirali in v delovnih dokumentih shranili vse navedbe, ki so jih prejeli med izvajanjem posla, bodisi pisne ali ustne.

1203 Izvedba in nadzor *(nadaljevanje)*

Povezava s standardi in smernicami

Vrsta	Naslov
Standard	1005 Dolžna poklicna skrbnost
Standard	1205 Dokazi
Standard	1401 Poročanje
Smernica	2202 Ocenjevanje tveganja pri načrtovanju

Datum uveljavitve

Ta standard ISACA velja za vse posle dajanja zagotovil in revidiranja IS, ki se začnejo 1. novembra 2013.

1204 Pomembnost

Zahteve

1204.1 Strokovnjaki dajanja zagotovil in revidiranja IS morajo pri načrtovanju posla upoštevati morebitne slabosti ali pomanjkljivosti kontrol in pretehtati, ali bi te slabosti ali pomanjkljivosti kontrol lahko imele za posledico pomembno pomanjkljivost ali bistveno slabost.

1204.2 Strokovnjaki dajanja zagotovil in revidiranja IS morajo upoštevati revizijsko pomembnost in njeno povezanost z revizijskim tveganjem, ko določajo vrsto, časovno razporeditev in obseg revizijskih postopkov.

1204.3 Strokovnjaki dajanja zagotovil in revidiranja IS morajo upoštevati skupni učinek manjših pomanjkljivosti kontrol ali slabosti in možnost, da se pomanjkanje kontrol prevede v pomembno pomanjkljivost ali bistveno slabost.

1204.4 Strokovnjaki dajanja zagotovil in revidiranja IS morajo v svojem poročilu razkriti naslednje:
- **pomanjkanje kontrol ali neučinkovite kontrole,**
- **pomembnost pomanjkljivosti kontrol,**
- **verjetnost, da bodo te slabosti povzročile pomembno pomanjkljivost ali bistveno slabost.**

Ključna pojasnila

Strokovnjaki dajanja zagotovil in revidiranja IS naj bi pri izvajanju posla:
- koncept pomembnosti uporabljali pri:
  – načrtovanju in izvajanju posla,
  – ocenjevanju vpliva določenih elementov, procesov, kontrol ali napak.

  Vsako pomanjkljivost, slabost ali pomanjkanje ustreznih politik, postopkov in kontrol bi bilo treba presojati v posebnih okoliščinah posla;
- upoštevali opredelitve pomembnosti, kjer jih določa zakonodaja ali regulatorni organi,
- upoštevali, da se lahko ocena pomembnosti in revizijskega tveganja občasno spremenita, kar je odvisno od okoliščin in spreminjajočega se okolja,
- poskušali zmanjšati revizijsko tveganje na sprejemljivo raven ter izpolniti cilje ob načrtovanju in izvajanju posla,
- upoštevali pomembnost ob določanju vrste, časa in obsega revizijskih postopkov,
- zmanjšali revizijsko tveganje za področja z višjo stopnjo pomembnosti z obsežnejšim preizkušanjem kontrol (zmanjšali tveganje pri kontroliranju) in/ali z obsežnejšim preizkušanjem podatkov (zmanjšali tveganje pri odkrivanju),
- ocenili učinek kompenzacijskih kontrol in ali so te učinkovite pri ugotavljanju, ali pomanjkljivost pri kontroli ali kombinacija pomanjkljivosti pri kontroli pomeni bistveno slabost,
- pri ugotavljanju pomembnosti upoštevali skupni učinek več napak ali nedelujočih kontrol,
- upoštevali ne samo velikost, ampak tudi vrsto pomanjkljivosti pri kontroliranju ter posebne okoliščine njihovega pojavljanja pri ocenjevanju njihovega skupnega učinka na revizijsko mnenje ali sklep.

Pojmi

Pojem	Pomen
Revizijsko tveganje	Tveganje za sprejem nepravilnega sklepa na podlagi ugotovitev revizije. Tri komponente revizijskega tveganja so: • tveganje pri kontroliranju, • tveganje pri odkrivanju, • tveganje pri delovanju.
Bistvena slabost	Pomanjkljivost ali kombinacija pomanjkljivosti pri notranjem kontroliranju, pri kateri obstaja razumna možnost, da bistveno napačne navedbe ne bo mogoče pravočasno preprečiti ali zaznati. Slabost pri kontroliranju se šteje za bistveno, če zaradi pomanjkanja kontrol ni mogoče podati zadostnega zagotovila o izpolnjevanju kontrolnih ciljev. Slabost, ki je opredeljena kot bistvena, pomeni, da: • kontrole niso vzpostavljene in/ali niso v uporabi in/ali so neustrezne, • je posredovanje zadeve nadrejenim neizbežno. Med pomembnostjo in ravnjo revizijskega tveganja, ki je sprejemljivo za strokovnjake dajanja zagotovil ali revidiranja IS, velja obratno sorazmerje, kar pomeni, da večja kot je stopnja pomembnosti, manjša je sprejemljivost revizijskega tveganja in obratno.

1204 Pomembnost *(nadaljevanje)*

Pojmi

Pojem	Pomen
Pomembnost	Revizijski koncept, ki zadeva pomembnost informacije glede na njen vpliv ali učinek na delovanje revidirane enote. Izraz relativne pomembnosti ali pomembnosti za neko določeno zadevo v kontekstu podjetja kot celote.

Povezava s standardi in smernicami

Vrsta	Naslov
Standard	1201 Načrtovanje posla
Standard	1202 Ocenjevanje tveganja pri načrtovanju
Standard	1207 Nepravilnosti in nezakonita dejanja
Standard	1401 Poročanje
Smernica	2202 Ocenjevanje tveganja pri načrtovanju
Smernica	2204 Pomembnost

Datum uveljavitve

Ta standard ISACA velja za vse posle dajanja zagotovil in revidiranja IS, ki se začnejo 1. novembra 2013.

1205 Dokazi

Zahteve

1205.1 Strokovnjaki dajanja zagotovil in revidiranja IS morajo pridobiti zadostne in ustrezne dokaze, da lahko sprejmejo primerne sklepe, s katerimi utemeljijo izide posla.

1205.2 Strokovnjaki dajanja zagotovil in revidiranja IS morajo ovrednotiti zadostnost dokazov, pridobljenih za utemeljitev sklepov in doseganje ciljev posla.

Ključna pojasnila

Strokovnjaki dajanja zagotovil in revidiranja IS naj bi pri opravljanju posla:

- pridobili zadostne in ustrezne dokaze, ki vključujejo:
  - postopke, kot so bili opravljeni,
  - izide opravljenih postopkov,
  - izvorne dokumente (v elektronski ali papirni obliki), zapise in dodatne informacije, uporabljene za podporo pri poslu,
  - ugotovitve in rezultate posla,
  - dokumentacijo, ki izkazuje, da je bilo delo izvedeno skladno z veljavno zakonodajo, predpisi in politikami;
- pripravili dokumentacijo, ki naj bo:
  - shranjena ter na voljo za obdobje in v obliki, ki sta skladna s politikami organizacije, odgovorne za revizijo ali dajanje zagotovil in strokovnimi standardi, zakoni in predpisi,
  - zaščitena pred nepooblaščenim razkritjem ali spreminjanjem za celotno obdobje priprave in hrambe,
  - pravilno uničena ob koncu obdobja hrambe;
- proučili zadostnost dokazov, da z njimi podprejo ocenjeno raven tveganja pri kontroliranju, če se dokazi pridobivajo iz preverjanja kontrol;
- ustrezno prepoznali, medsebojno povezali in popisali dokaze;
- upoštevali lastnosti, kot so izvor, vrsta (npr. pisni, ustni, vizualni, elektronski) in pristnost (npr. digitalni in ročni podpisi, žigi) dokazov pri ocenjevanju njihove zanesljivosti;
- upoštevali stroškovno najučinkovitejše in pravočasne načine za pridobitev potrebnih dokazov z namenom izpolnitve ciljev in tveganj v zvezi s poslom. Vendar težavnost ali stroški niso veljavna podlaga za opustitev potrebnega postopka;
- izbrali najprimernejši postopek za zbiranje dokazov glede na obravnavano zadevo (tj. glede na vrsto in časovno razporeditev revizije, strokovno presojo). Postopki, ki se uporabljajo za pridobitev dokazov, vključujejo:
  - poizvedovanje in potrjevanje,
  - ponovno izvajanje,
  - ponovno izračunavanje,
  - računanje,
  - analitične postopke,
  - preiskovanje,
  - opazovanje,
  - druge splošno sprejete metode;
- proučili vir in vrsto vsake pridobljene informacije da ovrednoti njeno zanesljivost in postavi zahteve za nadaljnje preverjanje. Na splošno velja, da je zanesljivost dokazov večja, kadar so ti:
  - v pisni obliki, in ne samo kot ustni izrazi mnenja,
  - pridobljeni iz neodvisnih virov,
  - pridobljeni s strani strokovnjaka samega, in ne s strani revidirane enote,
  - potrjeni s strani neodvisne stranke,
  - v hrambi pri neodvisni stranki,
  - rezultat preiskovanja,
  - rezultati opazovanja;
- pridobili nepristranske in zadostne dokaze, ki strokovno usposobljeni neodvisni stranki omogočajo ponovitev preizkusov ter pridobitev enakih izidov in ugotovitev;
- pridobili dokaze, ki so sorazmerni glede na pomembnost teme in ugotovljeno tveganje;
- dali ustrezen poudarek na točnost in popolnost informacij, če so te pridobljene od organizacije in so uporabljene za izvedbo revizijskih postopkov;
- razkrili vsak primer, ko zadostnih dokazov ni mogoče pridobiti, na način, ki je skladen z načinom sporočanja rezultatov posla dajanja zagotovil ali revidiranja IS;
- zaščitili dokaze pred nepooblaščenim dostopom in spremembami;
- shranili dokaze po končani reviziji ali dajanju zagotovil v zvezi z IS, dokler je to potrebno zaradi skladnosti z vsemi veljavnimi zakoni, predpisi in politikami.

1205 Dokazi (nadaljevanje)

Pojmi

Pojem	Pomen
Ustrezen dokaz	Merilo kakovosti dokazov.
Zadosten dokaz	Merilo količine dokazov; podpira vsa pomembna vprašanja glede ciljev in obsega revizije. Glejte dokaze.

Povezava s standardi in smernicami

Vrsta	Naslov
Smernica	2205 Dokazi

Datum uveljavitve

Ta standard ISACA velja za vse posle dajanja zagotovil in revidiranja IS, ki se začnejo 1. novembra 2013.

1206 Uporaba dela drugih strokovnjakov

Zahteve

1206.1 Če je primerno, morajo strokovnjaki dajanja zagotovil in revidiranja IS preučiti možnost uporabe dela drugih strokovnjakov pri poslu.

1206.2 Strokovnjaki dajanja zagotovil in revidiranja IS morajo pred začetkom izvajanja posla oceniti in odobriti ustreznost strokovne usposobljenosti, sposobnosti, ustreznih izkušenj, virov, neodvisnosti in postopkov nadzora kakovosti drugih strokovnjakov.

1206.3 Strokovnjaki dajanja zagotovil in revidiranja IS morajo v okviru posla oceniti, pregledati in ovrednotiti delo drugih strokovnjakov ter dokumentirati odločitev, v kakšnem obsegu so uporabili in se zanašali na njihovo delo.

1206.4 Strokovnjaki dajanja zagotovil in revidiranja IS morajo odločiti, ali je delo drugih strokovnjakov izven revizijske skupine zadostno in popolno za sklepanje o trenutnih ciljih posla, ter sklep jasno dokumentirati.

1206.5 Strokovnjaki dajanja zagotovil in revidiranja IS morajo odločiti, ali se bodo zanašali na delo drugega strokovnjaka in delo neposredno vključili v poročilo, ali ga bodo v poročilu navedli ločeno.

1206.6 Strokovnjaki dajanja zagotovil in revidiranja IS morajo izvesti dodatne preizkusne postopke za pridobitev zadostnih in ustreznih dokazov v okoliščinah, kjer delo drugih strokovnjakov ne zagotavlja zadostnih ali ustreznih dokazov.

1206.7 Strokovnjaki dajanja zagotovil in revidiranja IS morajo zagotoviti ustrezno revizijsko mnenje ali sklep ter vključiti vsakršne omejitve obsega, v primeru da potrebni dokazi niso pridobljeni s pomočjo dodatnih preizkusov.

Ključna pojasnila

Strokovnjaki dajanja zagotovil in revidiranja IS naj bi:

- proučili možnost uporabe dela drugih strokovnjakov pri izvajanju posla, kadar obstajajo omejitve (npr. tehnično znanje, ki ga zahteva narava naloge, ki jo je treba opraviti, omejena sredstva za revizijo, časovne omejitve), ki bi lahko oslabile revizijsko delo, ki ga je treba opraviti, ali kadar lahko s tem zboljša kakovost posla,
- dokumentirali vpliv na doseganje ciljev posla, če potrebni strokovnjaki niso na voljo, ter v načrt posla vključili posebna opravila za obvladovanje tveganj in upravljanje zahtev glede dokazov,
- proučili neodvisnost drugih strokovnjakov ob uporabi njihovega dela,
- imeli dostop do vseh delovnih dokumentov, spremljevalne dokumentacije in poročil drugih strokovnjakov, če takšen dostop ni vprašljiv s pravnega vidika,
- ugotovili in določili obseg uporabe dela drugega strokovnjaka in koliko se lahko zanesejo na njegovo delo, kadar strokovnjaku zaradi pravnih vprašanj ni odobren dostop do zapisov,
- uporabo dela drugih strokovnjakov dokumentirali v poročilu.

Pojmi

Pojem	Pomen
Drugi strokovnjak	Drugi strokovnjak se lahko ne glede na to, ali gre za notranjega ali zunanjega sodelavca organizacije, nanaša na: • revizorja IS iz zunanje revizijske družbe, • svetovalca poslovodstva, • strokovnjaka na revizijskem področju, ki ga je imenovalo najvišje poslovodstvo ali skupina.

Povezava s standardi in smernicami

Vrsta	Naslov
Smernica	2206 Uporaba dela drugih strokovnjakov

Datum uveljavitve

Ta standard ISACA velja za vse posle dajanja zagotovil in revidiranja IS, ki se začnejo 1. novembra 2013.

1207 Nepravilnosti in nezakonita dejanja

Zahteve

1207.1 Strokovnjaki dajanja zagotovil in revidiranja IS morajo med izvajanjem posla upoštevati tveganja nepravilnosti in nezakonitih dejanj.

1207.2 Strokovnjaki dajanja zagotovil in revidiranja IS morajo med izvajanjem posla ohranjati poklicno nezaupljivost.

1207.3 Strokovnjaki dajanja zagotovil in revidiranja IS morajo dokumentirati in primerni stranki pravočasno sporočiti vsako pomembno nepravilnost ali nezakonito dejanje.

Ključna pojasnila

Strokovnjaki dajanja zagotovil in revidiranja IS naj bi:

- zmanjšali revizijsko tveganje na sprejemljivo raven pri načrtovanju in izvajanju posla, tako da:
  - se zavedajo, da bi zaradi nepravilnosti in nezakonitih dejanj lahko obstajale pomembne napake, pomanjkljivosti pri nadzoru ali napačne navedbe ne glede na oceno tveganja za nepravilnosti in nezakonita dejanja;
  - se seznanijo s podjetjem in njegovim okoljem, vključno z notranjimi kontrolami, namenjenimi preprečevanju ali odkrivanju nepravilnosti in nezakonitih dejanj, ki so relevantna za področje, obseg in cilje posla;
  - pridobijo zadostne in ustrezne dokaze da ugotovijo, ali so poslovodstvo ali drugi v podjetju seznanjeni z dejanskimi, možnimi ali domnevnimi nepravilnostmi in nezakonitimi dejanji;
- pri izvajanju revizijskih postopkov upoštevali nenavadne ali nepričakovane odnose, ki lahko nakazujejo tveganje za pomembne napake, pomanjkljivosti pri nadzoru ali napačne navedbe zaradi nepravilnosti in nezakonitih dejanj,
- načrtovali in izvajali postopke za preverjanje ustreznosti notranjih kontrol ter tveganja, da poslovodstvo zaobide kontrole, ki so namenjene preprečevanju ali odkrivanju nepravilnosti in nezakonitih dejanj,
- ocenili, ali lahko ugotovljene napake, pomanjkljivosti pri nadzoru ali napačne navedbe nakazujejo na nepravilnost ali nezakonito dejanje. Če takšen indic obstaja, naj bi upoštevali posledice v povezavi z drugimi pojasnili posla in še zlasti z navedbami poslovodstva;
- od poslovodstva pridobili pisno izjavo vsaj enkrat na leto ali odvisno od posla pogosteje, za:
  - potrditev zadolžitve poslovodstva za načrtovanje in izvajanje notranjih kontrol za preprečevanje ter odkrivanje nepravilnosti in nezakonitih dejanj;
  - razkritje zadevnih rezultatov vsakršne ocene tveganj, ki nakazuje, da se kot posledica nepravilnosti ali nezakonitega dejanja lahko pojavijo napake, pomanjkljivosti pri kontroliranju ali napačne navedbe;
  - razkritje seznanjenosti poslovodstva z nepravilnostmi in nezakonitimi dejanji, ki vplivajo na podjetje, v zvezi s poslovodstvom in zaposlenimi, ki imajo pomembne vloge pri notranjem kontroliranju;
  - razkritje seznanjenosti poslovodstva z domnevnimi ali morebitnimi nepravilnostmi in nezakonitimi dejanji, ki vplivajo na podjetje in so jih sporočili zaposleni, nekdanji zaposleni, regulatorji in drugi;
- pravočasno sporočali:
  - ustrezni ravni poslovodstva o vsaki ugotovljeni ali pridobljeni informaciji, da lahko obstaja pomembna nepravilnost ali nezakonito dejanje;
  - pristojnim za upravljanje o vsaki pomembni nepravilnosti in nezakonitih dejanjih, v katere so vključeni poslovodstvo ali zaposleni, ki imajo pomembno vlogo pri notranjem nadzoru;
- poročali osebam, pristojnim za upravljanje, o vseh bistvenih slabostih pri načrtovanju in izvajanju notranjih kontrol, namenjenih preprečevanju in odkrivanju nepravilnosti in nezakonitih dejanj, ugotovljenih med poslom, tudi če so zunaj njegovega obsega,
- upoštevali pravne in strokovne zahteve glede poročanja, ki veljajo v danih okoliščinah,
- razmislili o odstopu od posla, če pomembne napake, pomanjkljivosti pri nadzoru in napačne navedbe ali nezakonita dejanja vplivajo na nadaljevanje posla,
- dokumentirali vso komunikacijo, načrtovanje, rezultate, ocene in sklepe, ki se nanašajo na pomembne nepravilnosti in nezakonita dejanja, ki so bila poročana poslovodstvu, pristojnim za upravljanje, regulatorjem in drugim.

1207 Nepravilnosti in nezakonita dejanja *(nadaljevanje)*

Pojmi

Pojem	Pomen
Nepravilnost	Kršitev vzpostavljene politike upravljanja ali predpisane zahteve. To je lahko namerna napačna navedba ali zamolčanje informacij v zvezi s področjem revizije ali celotnim podjetjem, huda malomarnost ali nenamerno nezakonito dejanje.
Pomembna napačna navedba	Naključna ali namerna neresnična izjava, ki v izmerljivem obsegu vpliva na rezultate revizije.
Poklicna nezaupljivost	Pristop, ki vključuje dvom in kritično ocenjevanje revizijskih dokazov. Vir: Ameriški inštitut preizkušenih javnih računovodij (AICPA) AU 230.07

Povezava s standardi in smernicami

Vrsta	Naslov
Standard	1008 Merila
Standard	1202 Ocenjevanje tveganja pri načrtovanju
Standard	1205 Dokazi
Smernica	2206 Uporaba dela drugih strokovnjakov
Smernica	2207 Nepravilnosti in nezakonita dejanja

Datum uveljavitve

Ta standard ISACA velja za vse posle dajanja zagotovil in revidiranja IS, ki se začnejo 1. novembra 2013.

Standardi poročanja

Poročila, ki jih pripravijo strokovnjaki dajanja zagotovil in revidiranja IS, se bodo razlikovala glede na vrsto izvajanih nalog. Pri tem je treba upoštevati ravni zagotavljanja, ali so strokovnjaki dajanja zagotovil in revidiranja IS izvajali revizijo, ali zagotavljajo neposredna poročila o obravnavani zadevi ali pa poročajo o trditvah v zvezi z obravnavano zadevo in ali poročila temeljijo na delu, izvedenem na ravni pregleda ali preiskovanja.

Standarda poročanja sta:
1401 Poročanje
1402 Nadaljnja obravnava

Standard so tukaj vključeni v celoti. Podčrtane besede so opredeljene v poglavju s pojmi. Za povezave do posameznih standardov obiščite spletno stran *www.isaca.org/standard*.

1401 Poročanje

Zahteve

1401.1 Strokovnjaki dajanja zagotovil in revidiranja IS morajo o izvedbi posla pripraviti poročilo, v katerem sporočijo rezultate, vključno z:
- **identifikacijo podjetja, predvidenimi prejemniki in kakršnimi koli omejitvami glede vsebine in posredovanja poročila;**
- **obsegom, cilji posla, obdobjem, ki ga zajema, ter vrsto, časovno razporeditvijo in obsegom opravljenega dela;**
- **ugotovitvami, sklepi in priporočili;**
- **vsakršnimi zadržki ali omejitvami obsega, ki jih ima strokovnjak dajanja zagotovil in revidiranja IS v zvezi s poslom;**
- **podpisom, datumom in prejemniki, skladno z določili revizijske listine ali listine o poslu.**

1401.2 Strokovnjaki dajanja zagotovil in revidiranja IS morajo zagotoviti, da so ugotovitve v revizijskem poročilu podprte z zadostnimi in ustreznimi revizijskimi dokazi.

Ključna pojasnila

Strokovnjaki dajanja zagotovil in revidiranja IS naj bi:
- pridobili ustrezne pisne izjave revidiranca, ki podrobno navajajo kritična področja posla, vprašanja, ki so se pojavila in odgovore nanje ter njegove trditve;
- ugotovili, ali je revidiranec podpisal in datiral svoje izjave, s čimer je označil potrditev svojih obveznosti v zvezi s poslom;
- dokumentirali in obdržali v delovnem dokumentu vse pisne ali ustne izjave, ki so jih prejeli med izvajanjem posla. Izjave revidiranca naj bi za posle potrjevanja pridobili pisno, da se ne bi pojavili nesporazumi;
- prilagodili obliko in vsebino poročila za podporo vrsti izvedene naloge, kot so:
  – revizija (neposredna ali z namenom potrjevanja),
  – pregled (neposreden ali z namenom potrjevanja),
  – dogovorjeni postopki;
- v poročilu opisali bistvene ali pomembne slabosti in njihov vpliv na doseganje ciljev posla;
- obravnavali vsebino osnutka poročila s poslovodstvom obravnavanega področja pred zaključkom in izdajo poročila ter v končno poročilo vključili odziv poslovodstva na ugotovitve, sklepe in priporočila, kjer je to primerno;
- pristojnim za upravljanje in, kjer je to primerno, odgovornemu organu sporočili pomembne pomanjkljivosti in bistvene slabosti v kontrolnem okolju. V poročilu razkrili, da so jih sporočili;
- vsa ločena poročila navedli v končnem poročilu;
- poslovodstvu revidiranca sporočili pomanjkljivosti notranjega kontroliranja, ki so manj kot pomembne, vendar ne brez posledic. V takšnih primerih naj bi pristojne za upravljanje ali odgovorni organ obvestili, da so te pomanjkljivosti notranjega kontroliranja sporočili vodstvu revidiranca;
- navedli standarde, ki veljajo pri izvajanju naloge in poročali o vsakršni neskladnosti s temi standardi, če je to potrebno.

1401 Poročanje *(nadaljevanje)*

Pojmi

Pojem	Pomen
Relevantne informacije	Ocenjevalcu v zvezi s kontrolami povedo nekaj smiselnega o delovanju osnovnih kontrol ali sestavin kontrol. Najpomembnejša je informacija, ki neposredno potrjuje delovanje kontrol. Informacija, ki se posredno nanaša na delovanje kontrol, je lahko prav tako pomembna, vendar manj pomembna kot neposredna informacija. Oglejte si cilje glede kakovosti informacij v COBIT 5.
Zanesljive informacije	Informacija, ki je točna, preverljiva in iz objektivnega vira. Oglejte si cilje glede kakovosti informacij v COBIT 5.
Zadostne informacije	Informacije so zadostne, ko so jih ocenjevalci zbrali dovolj, da lahko oblikujejo utemeljen sklep. Vendar morajo biti informacije najprej primerne, da so lahko tudi zadostne. Oglejte si cilje glede kakovosti informacij v COBIT 5.
Ustrezne informacije	Relevantne (tj. primerne za predvideni namen), zanesljive (tj. točne, preverljive in iz objektivnega vira) ter pravočasne (tj. ustvarjene in uporabljene v ustreznem časovnem okviru) informacije. Oglejte si cilje glede kakovosti informacij v COBIT 5.
Pravočasne informacije	Te informacije so ustvarjene in uporabljene v časovnem okviru, ki omogoča preprečevanje ali odkrivanje pomanjkljivosti pri nadzoru, preden postanejo bistvene za podjetje. Oglejte si cilje glede kakovosti informacij v COBIT 5.

Povezava s standardi in smernicami

Vrsta	Naslov
Smernica	2401 Poročanje

Datum uveljavitve

Ta standard ISACA velja za vse posle dajanja zagotovil in revidiranja IS, ki se začnejo 1. novembra 2013.

1402 Nadaljnja obravnava

Zahteve

1402.1 Strokovnjaki dajanja zagotovil in revidiranja IS morajo spremljati relevantne informacije, da lahko sklepajo, ali je poslovodstvo načrtovalo/sprejelo ustrezne in pravočasne ukrepe za obravnavanje poročanih revizijskih ugotovitev in priporočil.

Ključna pojasnila

Notranje revidiranje IS naj bi vzpostavilo proces nadaljnje obravnave z namenom spremljanja in zagotavljanja, da so bili ukrepi poslovodstva učinkovito izvedeni ali da je višje poslovodstvo sprejelo tveganje neukrepanja.

Zunanji strokovnjaki dajanja zagotovil ali revidiranja IS se smejo zanašati na notranje revidiranje IS, da bo, odvisno od obsega in pogojev posla, nadaljevalo obravnavo njihovih usklajenih priporočil.

Povezava s standardi in smernicami

Vrsta	Naslov
Smernica	2402 Nadaljnja obravnava

Datum uveljavitve

Ta standard ISACA velja za vse posle dajanja zagotovil in revidiranja IS, ki se začnejo 1. novembra 2013.

2. Smernice dajanja zagotovil in revidiranja IS

Razdelek 2000 naslavlja smernice, ki podpirajo standarde:
2000 Splošne smernice
2200 Izvedbene smernice
2400 Smernice poročanja

Vsak razdelek znotraj smernic se osredotoča na eno od naslednjega:
- zadeve in procese v zvezi z IS, ki bi jih strokovnjak dajanja zagotovil in revidiranja IS moral razumeti in upoštevati pri odločanju o načrtovanju, določanju obsega, izvajanju in poročanju o aktivnostih dajanja zagotovil in revidiranja IS;
- procesi, postopki, metodologije in pristopi dajanja zagotovil in revidiranja IS, ki bi jih strokovnjak dajanja zagotovil in za revidiranja IS moral upoštevati pri izvajanju aktivnosti dajanja zagotovil in revidiranja IS.

Upoštevajte, da so te smernice v procesu posodabljanja zaradi novih standardov in COBIT 5. Spremljajte spletno stran ISACA, kjer so osnutki za javno obravnavo objavljeni predvidoma do konca 2013.

Splošne smernice

Splošne smernice so:
2001 Revizijska listina (G5)
2002 Organizacijska neodvisnost (G12)
2003 Strokovna neodvisnost (G17)
2004 Upravičeno pričakovanje (v razvoju)
2005 Dolžna poklicna skrbnost (G7)
2006 Strokovna usposobljenost (G30)
2007 Trditve (v razvoju)
2008 Merila (v razvoju)

Smernice so na tem mestu vključene v celoti. Za povezave na posamezne standarde obiščite *www.isaca.org/standard*.

2001 Revizijska listina (G5)

1. Izhodišča

1.1 Povezava s standardi

1.1.1 Standard S1 (1001) Revizijska listina določa: »Namen, zadolžitve, pristojnosti in odgovornost funkcije revidiranja informacijskih sistemov ali poslov revidiranja informacijskih sistemov morajo biti ustrezno dokumentirane v revizijski listini ali listini o poslu.«

1.2 Povezava s COBIT-om

1.2.1 ME 4.7 *Neodvisno jamstvo* navaja: »…Pridobite upravi pravočasno neodvisno zagotovilo o skladnosti IT z njihovimi usmeritvami, standardi in postopki ter s splošno sprejetimi praksami.«

1.2.2 ME 2.5 *Jamstvo notranje kontrole* navaja: »Po potrebi pridobite nadaljnje zagotovilo o popolnosti in uspešnosti notranjih kontrol z neodvisnimi zunanjimi pregledi.«

1.3 Potreba po smernici

1.3.1 Namen te smernice je pomagati revizorju IS, da pripravi revizijsko listino in v njej opredeli zadolžitev, pristojnost in odgovornost funkcije revidiranja IS. Namenjena je predvsem funkciji notranje revizije IS, vendar je njene posamezne vidike mogoče upoštevati tudi v drugih okoliščinah.

1.3.2 Ta smernica daje navodila za uporabo standardov revidiranja IS. Revizor IS jo mora upošteva pri odločanju o tem, kako bo uporabljal standarde revidiranja IS, uporabljati jo mora po strokovni presoji in mora biti pripravljen utemeljiti vsako odstopanje.

2. Revizijska listina

2.1 Pooblastilo

2.1.1 Revizor IS mora imeti jasno pooblastilo za izvajanje funkcije revidiranja IS. To pooblastilo je običajno dokumentirano v revizijski listini, ki mora biti uradno sprejeta. Kadar je revizijska listina sestavljena za revidiranje kot celoto, je vanjo vključeno pooblastilo za revidiranje IS.

2.2 Vsebina revizijske listine

2.2.1 V revizijski listini morajo biti jasno obravnavani štirje vidiki: namen, zadolžitev, pristojnost in odgovornost. Vidiki, ki jih je treba upoštevati, so navedeni v naslednjih točkah.

2.2.2 Namen:
- vloga,
- smotri/cilji,
- izjava o poslanstvu,
- predmet in obseg,
- cilji/naloge.

2.2.3 Zadolžitev:
- načela delovanja,
- neodvisnost,
- odnos do zunanje revizije,
- zahteve revidiranca,
- kritični dejavniki uspeha,
- ključni kazalniki delovanja,
- ocenjevanje tveganja,
- druga merila uspešnosti delovanja.

2.2.4 Pristojnost:
- pravica dostopa do informacij, zaposlenih, lokacij in sistemov, ki so pomembni za izvajanje revizij,
- predmet in obseg ali kakršne koli omejitve področja in obsega,
- funkcije, ki jih je treba revidirati,
- pričakovanja revidiranca,
- organizacijska struktura, vključno z linijami poročanja upravi in višjemu poslovodstvu,
- razvrščanje revizijskega osebja za IS.

2.2.5 Odgovornost:
- linije poročanja višjemu poslovodstvu,
- ocene izvajanja posla,
- ocene uspešnosti zaposlenih,
- kadrovanje/poklicni razvoj,
- pravice revidiranca,
- neodvisni pregledi kakovosti,
- ocenjevanje skladnosti s standardi,
- primerjalna analiza izvajanja in funkcij,
- ocenitev dokončanja načrta revizije,
- primerjava predračuna z dejanskimi stroški,
- dogovorjeni ukrepi, npr. pogodbene kazni, če ena ali druga stranka ne opravi svojih zadolžitev.

2.3 Komuniciranje z revidiranci

2.3.1 Uspešno komuniciranje z revidiranci vključuje:

- opis storitve, predmet in obseg storitve, njeno razpoložljivost in pravočasnost izvedbe,
- predložitev ocene stroškov ali predračunov, če so na voljo,
- opis težav in možne rešitve,
- zagotavljanje ustreznih in hitro dostopnih zmogljivosti za uspešno komuniciranje,
- opredelitev razmerja med ponujeno storitvijo in potrebami revidiranca.

2.3.2 Revizijska listina je trdna podlaga za komuniciranje z revidiranci in se mora med drugim sklicevati tudi na sporazume o ravni storitev glede zadev, kot so:

- razpoložljivost za nenačrtovano delo,
- dostava poročil,
- stroški,
- odgovor na pritožbe revidiranca,
- kakovost storitve,
- pregled izvajanja,
- komuniciranje z revidiranci,
- ocenjevanje potreb,
- samoocenjevanje tveganj in kontrol,
- dogovor o opisu nalog in pristojnosti za revizije,
- potek poročanja,
- dogovor o izsledkih.

2.4 Proces zagotavljanja kakovosti

2.4.1 Revizor IS naj prouči o smiselnosti vzpostavitve procesa zagotavljanja kakovosti (npr. pogovori, ankete o zadovoljstvu strank, pregledi izvajanja poslov) za boljše razumevanje potreb in pričakovanj revidirancev, pomembnih za funkcijo revidiranja IS. Po potrebi je treba te potrebe oceniti v primerjavi z revizijsko listino zaradi izboljšanja storitve ali spremembe njene izvedbe ali revizijske listine.

3. Listina o poslu

3.1 Namen

3.1.1 Listine o poslu se pogosto uporabljajo za posamezne posle ali za določitev predmeta in obsega ter ciljev razmerja med zunanjo revizijo IS in organizacijo.

3.2 Vsebina

3.2.1 V listini o poslu morajo biti jasno obravnavani štirje vidiki: namen, zadolžitev, pristojnost in odgovornost. Vidiki, ki jih je treba upoštevati, so navedeni v naslednjih odstavkih.

3.2.2 Zadolžitev:

- obseg,
- cilji,
- neodvisnost,
- ocena tveganja,
- posebne zahteve revidiranca,
- rezultati.

3.2.3 Pristojnost:

- pravica dostopa do informacij, zaposlenih, lokacij in sistemov, ki so pomembni za izvajanje naloge,
- obseg ali kakršne koli omejitve obsega dela,
- dokaz o dogovoru glede rokov in pogojev posla.

3.2.4 Odgovornost:

- predvideni prejemniki poročil,
- pravice revidiranca,
- pregledi kakovosti,
- dogovorjeni datumi dokončanja,
- dogovorjeni proračuni/honorarji, če so na voljo.

4. Datum uveljavitve

4.1 Ta smernica velja za vse revizije IS, ki se začnejo 1. septembra 1999 ali pozneje. Smernica je bila pregledana in posodobljena in velja od 1. februarja 2008.

2002 Organizacijska neodvisnost (G12)

1. Izhodišča

1.1 Povezava s standardi

1.1.1 Standard S2 (1002, 1003) Neodvisnost določa: »Revizor IS mora biti zaznan kot neodvisen in delovati neodvisno od revidiranca v vseh zadevah, povezanih z revizijo.«

1.1.2 Standard S2 (1002, 1003) Neodvisnost določa: »Funkcija revidiranja IS mora biti neodvisna od področja ali dejavnosti, ki se pregleduje, tako da je mogoče nepristransko dokončanje revizijske naloge.«

1.1.3 Standard S3 (1005) Poklicna etika in standardi določa: »Revizor IS mora dosledno upoštevati Kodeks poklicne etike ISACA.«

1.2 Povezava s COBIT-om

1.2.1 Izbira najustreznejšega gradiva v COBIT-u, ki je primerno glede na predmet in obseg določene revizije, temelji na izbiri posebnih COBIT-ovih procesov IT in upoštevanju COBIT-ovih kontrolnih ciljev ter z njimi povezanih praks upravljanja. Za uresničevanje zahteve po neodvisnosti revizorjev IS so procesi v COBIT-u, ki bodo najverjetneje ustrezni, izbrani in prilagojeni, razvrščeni na primarne in sekundarne.

1.2.2 PO4 *Opredelite procese, organizacijo in razmerja IT* izpolnjuje poslovno zahtevo za IT glede delovnega odziva na poslovno strategijo, pri čemer izpolnjuje zahteve upravljanja in zagotavljanja opredeljenih in pristojnih kontaktnih točk z usmerjanjem na vzpostavitev pregledne, prožne in odzivne organizacijske strukture IT ter opredelitev in vpeljavo procesov IT z lastniki, vlogami in zadolžitvami, vključenimi v poslovne procese in procese odločanja.

1.2.3 Sekundarni viri:

- ME2 *Spremljajte in vrednotite notranje kontrole*,
- ME4 *Zagotovite upravljanje IT*.

1.2.4 Najpomembnejša informacijska sodila so:

- primarna: uspešnost in učinkovitost,
- sekundarna: zaupnost, celovitost, razpoložljivost, skladnost in zanesljivost.

1.3 Potreba po smernici

1.3.1 Namen te smernice je dodatno pojasniti pomen pojma 'neodvisnost', kot je uporabljen v standardu S2 (1002, 1003), in obravnavati pristop revizorja IS in neodvisnost pri revidiranju IS.

1.3.2 Ta smernica daje navodila za uporabo standardov revidiranja IS. Revizor IS jo mora upoštevati pri odločanju o tem, kako bo uporabljal standarde revidiranja IS, uporabljati jo mora po strokovni presoji in mora biti pripravljen utemeljiti vsako odstopanje.

2. Neodvisnost

2.1 Pristop

2.1.1 Revizorji IS si morajo pri vsem svojem delu prizadevati za spoštovanje veljavnih kodeksov poklicne etike in standardov revidiranja.

2.1.2 V skladu s COBIT-om mora revizijska listina zagotavljati, da pristojni člani vodstva organizacije ohranjajo in uveljavljajo neodvisnost, pristojnost in odgovornost revizijske funkcije.

3. Načrtovanje

3.1 Kadrovanje

3.1.1 Revizor IS vzpostavlja številna razmerja z ljudmi, ki so vključeni v revizijsko dejavnost in ima priložnost raziskovati najbolj skrite vidike področja, ki se revidira, pogosto pa tudi celo organizacijo. Odnos revizorja IS mora vedno ustrezati tej vlogi. Pri načrtovanju naj upošteva vsa znana razmerja.

3.1.2 Revizorji IS ne smeli sodelovati pri reviziji, če je njihova neodvisnost oslabljena. Neodvisnost je na primer oslabljena, če revizorji IS pričakujejo kakršen koli dobiček ali drugo osebno korist zaradi svojega vpliva na izide revizije. Vendar pa neodvisnost revizorjev IS ni nujno oslabljena zaradi revidiranja informacijskih sistemov, v katerih se v okviru rednega poslovanja pojavljajo tudi njihove osebne transakcije.

3.1.3 Na začetku revizije se od revizorjev IS lahko zahteva, da podpišejo izjavo o ne-navzkrižju interesov in s tem potrdijo svojo neodvisnost.

3.2 Prednostni revizijski načrt

3.2.1 COBIT-OV proces ME4 določa: »Poslovodstvo mora omogočiti neodvisno revizijo.« Za uresničitev tega cilja je treba določiti revizijski načrt. V načrtu mora biti preverjeno in potrjeno, da je pridobljeno pravilno in neodvisno zagotovilo glede učinkovitosti, uspešnosti in ekonomičnosti varnostnih postopkov in postopkov notranje kontrole. V okviru tega načrta mora poslovodstvo določiti prednostne naloge in cilje glede pridobivanja neodvisnih zagotovil.

4. Izvajanje revizijskega dela

4.1 Organizacija

4.1.1 Revizorji IS morajo biti organizacijsko neodvisni od področja, ki se revidira. Neodvisnost je oslabljena, če imajo revizorji IS neposreden nadzor nad področjem, ki se revidira. Neodvisnost revizorjev IS je lahko oslabljena tudi, če so revizorji IS odgovorni za neposredno poročanje tistim posameznikom, ki imajo neposreden nadzor nad področjem, ki se revidira. Neodvisnost revizorjev IS je lahko oslabljena tudi, če se od njih zahteva, da zaradi sledenja poročajo o času, ki so ga porabili za izvajanju revizije, ter o napredku, revizijskih zadevah itd. skupini za IT, ki je odgovorna za preizkušanje kontrol in ki o izidih poroča višjemu ali izvršilnemu poslovodstvu. To bi se lahko razumelo kot projekt skupine IT za vodenje revizorjev IS in kot slabitev neodvisnosti revizorjev IS. Poleg

tega naj revizorji IS tudi preverijo, če je bila neodvisnost oslabljena v primerih, kadar je bila podlaga za predmet in obseg opravljenega dela zahteva lastnikov kontrolnih procesov in bodo rezultati revizije uporabljeni za poslovne ali regulativne namene.

4.1.2 Neodvisnost naj redno ocenjujeta revizor IS in poslovodstvo. Pri oceni naj upoštevata dejavnike, kot so spremembe osebnih razmerij, finančni interesi ter prejšnji posli in zadolžitve. Revizorji IS naj pri tem neprekinjenem ocenjevanju pretehtajo možnost uporabe tehnik kontrolnega samoocenjevanja.

4.1.3 Odvisno od posla se revizorji IS lahko pogovorijo z ljudmi, analizirajo organizacijske procese, dobijo pomoč od osebja organizacije itd. Odnos revizorja IS in njegova zaznana neodvisnost morata biti v vseh okoliščinah ustrezna. Revizorji IS se morajo zavedati, da na njihovo podobo neodvisnosti lahko vplivajo njihova dejanja ali povezovanja. Vtis revizorjeve neodvisnosti pa lahko vpliva tudi na to, kako je sprejeto njegovo delo.

4.1.4 Če revizorji IS ugotovijo, da se določeno stanje ali odnos zaznava tako, da škoduje njihovi neodvisnosti, morajo vodstvo revizije čim prej obvestiti o takem zaznanem škodovanju.

4.2 Zbiranje informacij

4.2.1 Med različnimi stvarmi, ki jih je treba pridobiti za poznavanje organizacije, ki se revidira, morajo revizorji IS, za ohranitev svoje neodvisnosti pregledati:

- organizacijske usmeritve in postopke, ki se nanašajo na postopek neodvisnega dajanja zagotovil,
- revizijsko listino, izjavo o poslanstvu, usmeritve, postopke in standarde, prejšnja poročila in revizijske načrte,
- organigram.

4.3 Ocenjevanje kontrol

4.3.1 V revizijskih načrtih za IS naj bodo opredeljene dejavnosti, od katerih morajo biti revizorji IS neodvisni. Neodvisnost revizorjev IS od teh dejavnosti naj redno spremlja višje poslovodstvo ali oseba, ki določi in odobri načrte za revizijo IS. To spremljanje naj vključuje tudi ocenjevanje postopka za razporejanje posameznih revizorjev IS na specifične posle, tako da se preveri in potrdi, da ta postopek zagotavlja neodvisnost in zadostne veščine.

4.3.2 Vedno je treba preveriti in potrditi, da revizorji IS upoštevajo veljavne poklicne kodekse ravnanja. V mnogih okoliščinah to že zadošča za revizijski dokaz neodvisnosti. Če pa se pokaže kakšen znak, da je bila neodvisnost revizorja IS morda kompromitirana, je treba razmisliti o ponovnem pregledu in spremembi revizijskega načrta.

5. Poročanje

5.1 Učinek na poročanje

5.1.1 V okoliščinah, v katerih je neodvisnost revizorja IS oslabljena in revizor IS ostaja povezan z revizijo, je treba dejstva okrog vprašanja neodvisnosti revizorja IS razkriti ustrezni ravni poslovodstva in v poročilu.

6. Datum uveljavitve

6.1 Ta smernica velja za vse revizije IS, ki se začnejo 1. septembra 2000 ali pozneje. Smernica je bila pregledana in posodobljena ter velja od 1. avgusta 2008.

2003 Strokovna neodvisnost (G17)

1. Izhodišča

1.1 Povezava s standardi

1.1.1 Standard S2 (1002, 1003) Neodvisnost določa, da mora biti strokovnjak za revidiranje in dajanje zagotovil za IT »zaznan kot neodvisen in delovati neodvisno od revidiranca« v vseh zadevah, povezanih z revizijo.

1.1.2 Standard S2 (1002, 1003) Neodvisnost določa, da mora biti funkcija revidiranja in dajanja zagotovil za IT dovolj neodvisna od področja ali dejavnosti, ki se pregleduje, tako da je mogoče nepristransko dokončanje revizijske naloge.

1.1.3 Standard S3 (1005) Poklicna etika in standardi določa, da mora strokovnjak za revidiranje in dajanje zagotovil za IT pri izvajanju revizijskih nalog ravnati s potrebno poklicno skrbnostjo, vključno z upoštevanjem ustreznih strokovnih standardov.

1.2 Povezava s COBIT-om

1.2.1 Izbira najustreznejšega gradiva v COBIT-u, ki je primerno glede na področje in obseg določenega posla revidiranja in dajanja zagotovil, temelji na izbiri posebnih COBIT-ovih procesov IT in upoštevanju COBIT-ovih kontrolnih ciljev ter z njimi povezanih praks upravljanja. Za učinek nerevizijske vloge na neodvisnost strokovnjaka za revidiranje in dajanje zagotovil za IT so procesi v COBIT-u, ki bodo najverjetneje ustrezni, izbrani in prilagojeni, razvrščeni na primarne in sekundarne. Procesni in kontrolni cilji, ki jih je treba izbrati in prilagoditi, so lahko različni glede na določen obseg ter opis nalog in pristojnosti posla.

1.2.2 Primarni procesi IT so:
- PO6 *Sporočajte cilje in usmeritve vodstva*,
- PO9 *Ocenjujte in obvladujte tveganja IT*,
- PO10 *Upravljajte projekte*,
- DS2 *Upravljajte storitve tretje stranke*,
- DS7 *Izobrazite in usposobite uporabnike*,
- ME2 *Spremljajte in vrednotite notranje kontrole*,
- ME3 *Zagotovite skladnost z zunanjimi zahtevami*,
- ME4 *Zagotovite upravljanje IT*.

1.2.3 Sekundarni procesi IT so:
- PO7 *Upravljajte človeške vire v sektorju IT*,
- DS10 *Upravljajte probleme*.

1.2.4 Najpomembnejša informacijska sodila so:
- primarna: zanesljivost, zaupnost, skladnost in učinkovitost,
- sekundarna: uspešnost, celovitost in razpoložljivost.

1.3 Potreba po smernici

1.3.1 V mnogih podjetjih poslovodstvo, osebje IT in notranji revizorji pričakujejo, da se strokovnjaki za revidiranje in dajanje zagotovil za IT lahko vključujejo v nerevizijske dejavnosti, kot so:
- določitev strategij IS v zvezi s področji, kot so tehnologija, aplikacije in viri,
- ocenjevanje, izbira in uvedba tehnologij,
- ocenjevanje, izbira, prilagoditev potrebam podjetja in uvajanje aplikacij in rešitev IS tretjih strank,
- zasnova, razvoj in uvedba po meri izdelanih aplikacij in rešitev IS,
- vzpostavitev dobrih praks, politik in postopkov v zvezi z različnimi funkcijami IT,
- zasnova, razvoj, preizkušanje in uvedba varnosti in nadzora,
- upravljanje projektov IT.

1.3.2 Nerevizijska vloga na splošno vključuje sodelovanje pri pobudah za IT in v projektnih skupinah za IT z delom in/ali svetovanjem s polnim ali krajšim delovnim časom. Strokovnjaki za revidiranje in dajanje zagotovil za IT lahko opravljajo nerevizijsko vlogo z vključevanjem v dejavnosti, kot so:
- začasno opravljanje naloge s polnim delovnim časom ali posojanje osebja za revidiranje in dajanje zagotovil za IT projektnim skupinam za IS;
- vključevanje člana osebja za revidiranje in dajanje zagotovil za IT za krajši delovni čas kot člana različnih projektnih struktur, kot so projektni svet, projektna delovna skupina, ocenjevalna skupina, skupina za pogajanja in sklenitev pogodbe, skupina za uvedbo, skupina za zagotavljanje kakovosti in skupina za odpravljanje težav;
- občasno delovanje kot neodvisni svetovalec ali pregledovalec za posamezne primere (*ad hoc*).

1.3.3 Take nerevizijske vloge so pomemben del prispevka strokovnjaka za revidiranje in dajanje zagotovil za IT k izobraževanju in usposabljanju drugih članov podjetja. Strokovnjakom za revidiranje in dajanje zagotovil za IT omogočajo, da uporabijo svoje izkušnje in poznavanje podjetja za enkraten in dragocen prispevek k učinkovitosti in uspešnosti naložb podjetja v IT. Ponujajo tudi priložnosti za dvig ugleda funkcije revidiranja in dajanja zagotovil za IT in za pridobivanje dragocenih praktičnih izkušenj osebja za revidiranje in dajanje zagotovil za IT.

1.3.4 Kadar je strokovnjak za revidiranje in dajanje zagotovil za IT vključen v nerevizijsko vlogo v pobudi za IS in se pozneje ali sočasno izvaja revizija te pobude ali z njo povezane funkcije IS, utegnejo prejemniki priporočil in ugotovitev te razumeti kot pristranske. V taki situaciji se lahko pojavi zaznava, da sta zaradi nerevizijskega vključevanja strokovnjaka za revidiranje in dajanje zagotovil za IT oslabljeni njegova neodvisnost in nepristranskost.

1.3.5 Strokovnjak za revidiranje in dajanje zagotovil za IT, ki je vključen v nerevizijsko vlogo, naj oceni, ali njegova vloga povzroča dejansko ali opazno oslabitev njegove neodvisnosti. Strokovnjak za revidiranje in dajanje zagotovil za IT naj svetuje in ozavešča tistega, ki odloča o IT, kaj naj upošteva pri ocenjevanju ustreznosti kontrole. Strokovnjak za revidiranje in dajanje zagotovil za IT, ki opravlja nerevizijsko vlogo, naj ne bi sam potrjeval, ali je posamezna kontrola učinkovito zasnovana.

1.3.6 Namen te smernice je predložiti okvir, v katerem strokovnjak za revidiranje in dajanje zagotovil za IT lahko:
- ugotovi, kdaj utegne biti ali se morda zdi zahtevana neodvisnost oslabljena,
- razmisli o morebitnih drugih možnih pristopih k revidiranju, kadar zahtevana neodvisnost dejansko je ali se zdi oslabljena,
- zmanjša ali izloči vpliv strokovnjakov za revidiranje in dajanje zagotovil za IT na nerevizijske vloge, funkcije in storitve,
- določi zahteve za razkritja.

2. Revizijska listina

2.1 Pogoji nerevizijskega vključevanja strokovnjakov za revidiranje in dajanje zagotovil za IT

2.1.1 V revizijski listini za IT naj se določijo naloge in pooblastila strokovnjaka za revidiranje in dajanje zagotovil za IT, ki bo vključen v nerevizijske vloge, ter splošno vrsto, čas in obseg njegovih vlog, tako da ne bo oslabljena neodvisnost v zvezi s sistemi, ki bi jih ta strokovnjak za revidiranje in dajanje zagotovil za IT lahko revidiral. Na ta način se je mogoče izogniti potrebi za pridobitev posebnih pooblastil za vsak primer posebej.

2.1.2 Strokovnjak za revidiranje in dajanje zagotovil za IT naj da sprejemljiva zagotovila, da so posebne nerevizijske vloge iz opisa nalog in pristojnosti (TOR – Terms of Reference) skladne z revizijsko listino. Kakršna koli odstopanja naj bodo v TOR-u posebej opredeljena.

2.1.3 Kadar v revizijski listini nerevizijske vloge niso posebej navedene ali kadar revizijske listine sploh ni, naj strokovnjaki za revidiranje in dajanje zagotovil za IT poročajo poslovodstvu in revizijski komisiji, če ta obstaja, o tem, da so vključeni v nerevizijske vloge. Časovni okvir ali obseg vključevanja strokovnjakov za revidiranje in dajanje zagotovil za IT v projekte IS naj bo določen v posameznem opisu nalog in pristojnosti (TOR), ki ga podpiše vodja službe in odobri revizijska komisija.

3. Vrste nerevizijskih storitev

3.1 Vključevanja, ki ne slabijo neodvisnosti

3.1.1 Strokovnjaki za revidiranje in dajanje zagotovil za IT, ki strokovno svetujejo na podlagi svojega strokovnega znanja in izkušenj, na primer s sodelovanjem v komisijah, odborih, delovnih skupinah ali svetih, opravljajo nerevizijske dejavnosti, ki ne slabijo neodvisnosti strokovnjakov za revidiranje in dajanje zagotovil za IT. Neodvisnost strokovnjakov za revidiranje in dajanje zagotovil pa bi bila oslabljena, če bi strokovnjaki za revidiranje in dajanje zagotovil za IT na podlagi obsega ali narave svojega svetovanja sprejemali poslovodne odločitve ali opravljali poslovodne funkcije.

3.1.2 Nerevizijska vključevanja, ki ne slabijo neodvisnosti, če se izvajajo dodatni protiukrepi, so med drugim svetovanje o informacijski tehnologiji, ki je omejeno na svetovanje o zasnovi sistemov, namestitvi sistemov in sistemski varnosti. Nadzorni svet in poslovodstvo podjetja naj se zaneseta na delo strokovnjakov za revidiranje in dajanje zagotovil za IT kot temeljno podlago za odločanje o vpeljavi novega sistema, ustreznosti zasnove novega sistema, ustreznosti večjih sprememb v zasnovi obstoječega sistema in o ustreznosti sistema glede skladnosti s predpisanimi ali drugimi zahtevami.

3.2 Vključevanja, ki slabijo neodvisnost

3.2.1 Nerevizijske vloge, ki slabijo neodvisnost in nepristranskost, so med drugim pomembno vključevanje strokovnjaka za revidiranje in dajanje zagotovil za IT v procese snovanja, razvijanja, testiranja, nameščanja, konfiguriranja ali delovanja informacijskih sistemov ter zasnove kontrol za informacijske sisteme, ki so pomembni ali bistveni za področje revizije.

3.2.2 Nerevizijska vloge vključujejo tudi delo v upravljavski vlogi, kjer je strokovnjak za revidiranje in dajanje zagotovil za IT zadolžen za samostojno ali skupno sprejemanje poslovodnih odločitev ali za potrjevanje politik in standardov.

3.2.3 Neodvisnost strokovnjaka za revidiranje in dajanje zagotovil za IT bi bila lahko oslabljena, če bi ocenjevanje informacijskih sistemov vključevalo tudi preizkušanje kontrol aplikacij/sistemov, ki jih je strokovnjak za revidiranje in dajanje zagotovil za IT izbral med izvajanjem nerevizijske vloge.

3.2.4 Neodvisnost strokovnjaka za revidiranje in dajanje zagotovil za IT bi bila oslabljena lahko, če bi strokovnjak za revidiranje in dajanje zagotovil za IT zaradi obsega ali vrste svetovanja sprejemal poslovodne odločitve ali opravljal poslovodne funkcije.

4. Neodvisnost

4.1 Pomembnost neodvisnosti pri nerevizijskih vlogah

4.1.1 Strokovnjaki za revidiranje in dajanje zagotovil za IT morajo biti neodvisni v vseh zadevah, povezanih z revizijo; nobene zahteve pa ni, da bi moral biti strokovnjak za revidiranje in dajanje zagotovil za IT neodvisen ali zaznan kot neodvisen, kadar se vključuje v pobudo za IS v okviru svoje nerevizijske vloge, razen če to prepovedujejo drugi zunanji standardi.

4.1.2 Čeprav ni treba, da bi bil strokovnjak za revidiranje in dajanje zagotovil za IT neodvisen, kadar izvaja dela v nerevizijski vlogi, je nepristranskost še vedno poklicna zahteva. Strokovnjak za revidiranje in dajanje zagotovil za IT naj bi tudi dela v svoji nerevizijski vlogi izvajal nepristransko in strokovno.

4.1.3 Kljub temu da se za strokovnjaka za revidiranje in dajanje zagotovil za IT ne zahteva, da je neodvisen, kadar izvaja nerevizijsko vlogo na pobudo za IS, naj strokovnjak za revidiranje in dajanje zagotovil za IT pretehta, ali bi se lahko štelo, da ta vloga slabi njegovo neodvisnost, če bi strokovnjak za revidiranje in dajanje zagotovil za IT dobil nalogo, da revidira to pobudo za IS in/ali povezano funkcijo. Kadar je tako nasprotje predvidljivo (npr. če bo pozneje zahtevana neodvisna revizija in je na voljo samo en strokovnjak za revidiranje in dajanje zagotovil za IT z ustreznimi sposobnostmi za izvajanje nerevizijske vloge in poznejše revizije), naj se strokovnjak za revidiranje in dajanje zagotovil za IT o zadevi pogovori z revizijsko komisijo ali enakovrednim organom upravljanja, preden sprejme nerevizijsko vlogo.

4.1.4 O sodelovanju strokovnjaka za revidiranje in dajanje zagotovil za IT v nerevizijski vlogi pri pobudi za IS in o neodvisni reviziji te pobude za IS ali povezane funkcije naj odloča revizijska komisija ali enakovreden organ upravljanja. Opravi naj se analiza tveganja. Vidiki, ki bodo verjetno vplivali na odločitev, so:
- morebitni drugi možni viri za eno ali drugo vlogo,
- zaznavanje relativne dodane vrednosti dejavnosti, ki sta si v nasprotju,

- možnost za izobraževanje skupine za IS, kar bi lahko koristilo pri naslednjih pobudah,
- priložnosti za strokovni razvoj in načrtovanje nasledstva za strokovnjaka za revidiranje in dajanje zagotovil za IT,
- raven tveganja, pripisanega nerevizijski vlogi,
- vpliv na vidnost, ugled, podobo itd. funkcije revidiranja in dajanja zagotovil za IT,
- morebitni učinek odločitve na zahteve zunanjih revizorjev ali regulatorjev,
- določbe revizijske listine za IT.

4.2 Učinek nerevizijske vloge na poznejše revizije

4.2.1 Kadar je pobuda za IS ali funkcija IS revidirana zaradi zakonskih in/ali zahtev poslovodstva, mora biti strokovnjak za revidiranje in dajanje zagotovil za IT dejansko neodvisen in zaznan kot neodvisen od skupine za IS in njenega vodstva.

4.2.2 Strokovnjaki za revidiranje in dajanje zagotovil za IT ne smejo revidirati svojega lastnega dela ali opravljati nerevizijskih storitev, kadar so nerevizijska opravila bistvena ali pomembna za področje revizij, v katere so vključeni. Nerevizijsko vključevanje strokovnjakov za revidiranje in dajanje zagotovil za IT v neko pobudo za IS bi lahko oslabilo njihovo neodvisnost za revizijo te pobude za IS in/ali povezane funkcije. Strokovnjaki za revidiranje in dajanje zagotovil za IT naj izjavijo, ali je po njihovem mnenju nerevizijska vloga, ki so jo imeli, oslabila njihovo neodvisnost pri izvajanju revizije ali ne. Od revizijske komisije ali enakovrednega organa upravljanja naj se zahteva pisno soglasje s tem mnenjem.

4.2.3 Kritični dejavniki, ki bi lahko pomagali ugotoviti, ali bi bila neodvisnost strokovnjakov za revidiranje in dajanje zagotovil za IT v zvezi z revizijo zaradi njihove nerevizijske vloge lahko oslabljena ali ne, vključujejo vidike, kot so:

- vrsta, čas in obseg nerevizijske vloge pri pobudi za IS, kadar se razmišlja o reviziji te pobude za IS in/ali z njo povezane funkcije. Večja kot je moč odločanja v nerevizijski vlogi, višja je raven oslabitve neodvisnosti;
- obstoj dejstev, za katere je mogoče verjeti, da spodkopavajo neodvisnost. To vključuje vidike, kot so pomembna nagrada ali kazen v zvezi z nerevizijsko vlogo;
- zmožnost, pa tudi zavzetost strokovnjaka za revidiranje in dajanje zagotovil za IT, da kljub svoji nerevizijski vlogi ostane objektiven in nepristranski pri izvajanju revizije in poročanju o slabostih ali napakah;
- svoboda strokovnjaka za revidiranje in dajanje zagotovil za IT, da kljub vključenosti v nerevizijsko vlogo določi obseg in način izvajanja revizije;
- razkritje nerevizijske vloge strokovnjaka za revidiranje in dajanje zagotovil za IT, ravni, na kateri je bil vanjo vključen, in z njo povezanih pomembnih dejstev;
- obstoj pomembnih (pozitivnih ali negativnih) osebnih odnosov v času nerevizijske vloge, zlasti z ljudmi na vodilnih mestih;
- vpliv in/ali prepričevanje strokovnjaka za revidiranje in dajanje zagotovil za IT v njegovi nerevizijski vlogi, ne glede na pooblastila za odločanje, ki jih je imel strokovnjak za revidiranje in dajanje zagotovil za IT;
- kritičnost (razvrščeno po oceni tveganosti) informacijskih virov, ki bodo vključeni v revizijo in so bili vključeni tudi v nerevizijsko vlogo, ki jo je izvajala ista oseba.

5. Načrtovanje

5.1 Učinek na neodvisnost

5.1.1 Pri načrtovanju kakršnih koli nerevizijskih vlog naj se oceni morebitni učinek nerevizijske vloge na neodvisnost za verjetno prihodnjo ali sočasno revizijo iste pobude za IS in/ali povezane funkcije.

5.1.2 Morebitni učinek katere koli prejšnje ali sedanje nerevizijske vloge strokovnjakov za revidiranje in dajanje zagotovil za IT pri kakršni koli pobudi za IS na njihovo neodvisnost naj se oceni že pri načrtovanju revizij za vse take pobude za IT in/ali povezane funkcije.

5.1.3 Revizijsko komisijo ali enakovreden organ upravljanja je treba obvestiti o morebitni oslabitvi neodvisnosti in o vseh morebitnih pojavih take oslabitve.

5.1.4 Strokovnjak za revidiranje in dajanje zagotovil za IT naj priporoči ukrepe ali kompenzacijske kontrole, ki jih vodstvo revizije ali revizijska komisija lahko izvede, da bo dano sprejemljivo zagotovilo o neodvisnosti in nepristranskosti. Med njimi so lahko:

- imenovanje dodatnih vodij in/ali oseb iz službe za revidiranje in dajanje zagotovil za IT, ki niso imeli nobene nerevizijske vloge na pregledovanem področju, da nadomestijo strokovnjaka za revidiranje in dajanje zagotovil za IT, ki ima ali je imel nerevizijsko vlogo;
- imenovanje vodij in/ali oseb, ki niso iz službe za revidiranje in dajanje zagotovil za IT, na primer izposoja osebja iz drugih poslovnih funkcij, oddelkov, zunanjih organizacij itd., da nadomestijo strokovnjaka za revidiranje in dajanje zagotovil za IT, ki ima ali je imel nerevizijsko vlogo;
- imenovanje neodvisnega strokovnjaka iz službe za revidiranje in dajanje zagotovil za IT ali iz drugih prej omenjenih virov, da opravi prijateljski pregled in deluje kot neodvisen razsodnik med načrtovanjem, delom na terenu in poročanjem.

5.1.5 Če je obseg vključevanja strokovnjakov za revidiranje in dajanje zagotovil za IT v nerevizijske vloge zelo velik, naj strokovnjaki za revidiranje in dajanje zagotovil za IT niti ne priporočajo ukrepov revizijski komisiji niti naj se neposredno ne vključujejo v preglede revizijskega področja, v katero so že bili polno vključeni oziroma so bili v njem udeleženi.

6. Izvajanje revizijskega dela

6.1 Spremljanje izvajanja revizije

6.1.1 Če obstaja pri reviziji možnost oslabljene neodvisnosti zaradi nerevizijskega vključevanja, naj vodstvo revidiranja in dajanja zagotovil za IT skrbno spremlja njeno izvajanje. Vse pomembne znake ogrožanja neodvisnosti zaradi nerevizijskega vključevanje naj vodstvo revidiranja in dajanja zagotovil za IT kritično ovrednoti in uvede potrebne popravljalne ukrepe. V takih primerih je treba obvestiti revizijsko komisijo ali enakovreden organ upravljanja.

6.1.2 Pri proučevanju, ali bi na revizije, ki jih izvajajo strokovnjaki za revidiranje in dajanje zagotovil za IT, lahko bistveno ali pomembno vplivala njihova nerevizijska vloga, naj revizijska komisija ali enakovreden organ upravljanja oceni tekoče revizije, načrtovane revizije,

zahteve in zaveze za revizije, kar vključuje zakone, predpise, pravila, pogodbe in druge dogovore, ter politike ali odločitve, s katerimi se strokovnjakom za revidiranje in dajanje zagotovil za IT nalagajo odgovornosti zaradi njihovega vključevanja v nerevizijsko vlogo.

6.1.3 Organi upravljanja naj vključijo dodeljevanje revizijskih virov na nerevizijske vloge, da se bodo lahko vnaprej zavedali morebitnih nasprotij in dobili od vodstva revizije zagotovilo, da bodo taka nasprotja čim manjša in ustrezno upravljana.

7. Poročanje

7.1 Zahteve po razkritju

7.1.1 Kadar bi neodvisnost vodstva in/ali osebja za revidiranje in dajanje zagotovil za IT v zvezi z revizijo neke pobude za IS in/ali povezane funkcije lahko bila ali bi se lahko zdelo, da je oslabljena zaradi nerevizijske vloge v tej pobudi za IS, naj strokovnjak za revidiranje in dajanje zagotovil za IT v revizijskem poročilu razkrije zadostne informacije o tej nerevizijski vlogi ter sprejete ukrepe, da lahko da sprejemljivo zagotovilo o neodvisnosti in nepristranskosti. To bo uporabnikom revizijskega poročila omogočilo, da bodo razumeli verjeten obseg oslabitve, če bo do nje prišlo, in sprejetih ukrepov za ublažitev njenega učinka. Informacije, katerih razkritje naj proučijo strokovnjaki za revidiranje in dajanje zagotovil za IT, vključujejo vidike, kot so:

- imena in položaj vodstva in osebja za revidiranje in dajanje zagotovil za IT, ki so bili vključeni v nerevizijske vloge pri pobudi za IT;
- vrsta, čas in obseg njihovega nerevizijskega vključevanja v pobudo za IS;
- razlogi za njihovo vključevanje v nerevizijsko vlogo pri pobudi za IS ter v revizijo te pobude za IS in povezane funkcije;
- sprejeti ukrepi za dajanje zagotovila, da neodvisnost in nepristranskost med potekom revizijskega dela in procesom poročanja nista bili pomembno oslabljeni;
- dejstvo, da je bila morebitna oslabitev neodvisnosti izpostavljena revizijski komisiji ali enakovrednemu organu upravljanja in njuno soglasje pridobljeno pred opravljanjem nerevizijske vloge;
- obstoj in obseg izvedenega pregleda, da se zagotovi sprejemljiva raven zanesljivosti opravljenega dela.

8. Datum uveljavitve

8.1 Ta smernica je bila pregledana in posodobljena ter velja od 1. maja 2010.

2004 Upravičeno pričakovanje (v razvoju)

2005 Dolžna poklicna skrbnost (G7)

1. Izhodišča

1.1 Povezava s standardi

1.1.1 Standard S3 (1005) Poklicna etika in standardi določa: »Revizor IS mora pri opravljanju revizijskih poslov dosledno upoštevati kodeks poklicne etike ISACA.«

1.1.2 Standard S3 (1005) Poklicna etika in standardi določa: »Revizor IS mora zagotavljati potrebno poklicno skrbnost, vključno z upoštevanjem ustreznih strokovnih revizijskih standardov.«

1.1.3 Standard S2 (1002, 1003) Neodvisnost določa: »Revizor IS mora biti zaznan kot neodvisen in delovati neodvisno od revidiranca v vseh zadevah, povezanih z revizijo.«

1.1.4 Standard S4 (1005) Strokovna usposobljenost določa: »Revizor IS mora biti strokovno usposobljen in imeti veščine in znanje za izvajanje revizijske naloge in vzdrževati mora svojo strokovno usposobljenost z ustreznim stalnim strokovnim izobraževanjem in usposabljanjem.«

1.1.5 Revizor IS lahko najde dodatna navodila v komentarjih navedenih standardov.

1.2 Povezava s COBIT-om

1.2.1 PO6 *Sporočajte cilje in usmeritve vodstva* izpolnjuje poslovno zahtevo za IT glede pravilnih in pravočasnih informacij o sedanjih in prihodnjih storitvah IT ter s tem povezanih tveganj in zadolžitev z usmerjanjem na zagotavljanje pravilnih, razumljivih in odobrenih politik, postopkov, smernic in druge dokumentacije udeležencem, ki sodelujejo v kontrolnem okviru IT.

1.2.2 PO7 *Upravljajte človeške vire v sektorju IT* izpolnjuje poslovno zahtevo za IT glede strokovno usposobljenih in motiviranih ljudi za ustvarjanje in izvajanje storitev IT z usmerjanjem na zaposlovanje in usposabljanje osebja, motiviranje osebja z jasnimi poklicnimi potmi, dodeljevanje vlog glede na sposobnosti, vzpostavitev opredeljenega procesa za pregledovanje, pripravo sistemizacije delovnih mest in zagotavljanje zavedanja glede odvisnosti od posameznikov.

1.2.3 PO9 *Ocenjujte in obvladujte tveganja IT* izpolnjuje poslovno zahtevo za IT glede analize in sporočanja tveganj IT ter njihovega morebitnega vpliva na poslovne procese in cilje z usmerjanjem na razvoj okvira za obvladovanje tveganj, ki je vključen v okvire za obvladovanje poslovnih in operativnih tveganj, ocenjevanje tveganj, zmanjševanje tveganj in sporočanje preostalega tveganja.

1.2.4 ME3 *Zagotovite skladnost z zunanjimi zahtevami* izpolnjuje poslovno zahtevo za IT glede zagotavljanja skladnosti z zakoni, predpisi in pogodbenimi zahtevami z usmerjanjem na prepoznavanje vseh veljavnih zakonov, predpisov in pogodb ter ustreznih ravni skladnosti IT in optimizacijo procesov IT za zmanjšanje tveganja neskladnosti.

1.2.5 ME4 *Zagotovite upravljanje IT* izpolnjuje poslovno zahtevo za IT glede združevanja upravljanja IT s cilji upravljanja podjetja in skladnosti z zakoni, predpisi in pogodbami z usmerjanjem na pripravo poročil za upravo o strategiji, delovanju in tveganjih IT ter odzivanju na zahteve upravljanja v skladu z usmeritvami uprave.

1.2.6 Sekundarni viri:

- PO1 *Opredelite strateški načrt za IT*,
- PO5 *Upravljajte investicije IT*,
- PO8 *Upravljajte kakovost*,
- PO10 *Upravljajte projekte*,
- AI1 *Določite avtomatizirane rešitve*,
- AI6 *Upravljajte spremembe*,
- DS3 *Upravljajte delovanje in zmogljivost*,
- DS7 *Izobrazite in usposobite uporabnike*,
- DS9 *Upravljajte konfiguracijo*,
- DS10 *Upravljajte probleme*.

1.2.7 Najpomembnejša informacijska sodila so:

- primarna: zanesljivost, zaupnost, celovitost, skladnost in uspešnost,
- sekundarna: učinkovitost in razpoložljivost.

1.3 Potreba po smernici

1.3.1 Namen te smernice je pojasniti izraz 'potrebna poklicna skrbnost', kot se uporablja za izvajanje revizije v skladu s standardom S3 (1005) revidiranja IS.

1.3.2 Pričakuje se, da člani in imetniki licence ISACA ravnajo v skladu s kodeksom poklicne etike ISACA; če ne, se proti članu ISACA ali imetniku njene licence lahko uvede preiskava in na koncu po potrebi izreče tudi disciplinski ukrep.

1.3.3 Smernica daje navodila za uporabo standardov revidiranja IS in ravnanje v skladu s kodeksom poklicne etike ISACA o izvajanju nalog s potrebno vestnostjo in poklicno skrbnostjo. Revizor IS jo mora upoštevati pri odločanju o tem, kako bo uporabljal standarde revidiranja IS, uporabljati jo mora po strokovni presoji in mora biti pripravljen utemeljiti vsako odstopanje.

2. Izvajanje revizijskega dela

2.1 Potrebna poklicna skrbnost

2.1.1 Standard potrebne skrbnosti je stopnja skrbnosti, s kakršno bi preudaren in usposobljen strokovnjak ravnal v danih okoliščinah. Potrebna poklicna skrbnost velja za posameznika, ki trdi, da izvaja posebno strokovno veščino, kot je revidiranje IS. Potrebna poklicna skrbnost zahteva od posameznika, da to strokovno veščino izvaja na ravni, ki jo imajo običajno strokovnjaki, ki delajo na tem posebnem področju.

2.1.2 Potrebna poklicna skrbnost velja za izvajanje strokovne presoje pri opravljanju prevzetega dela. Potrebna poklicna skrbnost pomeni tudi to, da se strokovnjak z ustrezno skrbnostjo loti zadev, ki zahtevajo strokovno presojo.

2.1.3 Potrebna poklicna skrbnost mora zajemati vse vidike revizije, kar med drugim vključuje ocenjevanje revizijskega tveganja, sprejetje revizijskih poslov, oblikovanje revizijskih ciljev, določitev obsega revizije, načrtovanje revizije, izvajanje revizije, dodeljevanje virov za revizijo, izbiro revizijskih preizkusov, ovrednotenje izidov preizkusov, revizijsko dokumentacijo, sklepne ugotovitve revizije, poročanje in izročitev izidov revizije. Pri tem mora revizor IS določiti ali oceniti:

- vrsto, raven, znanje in sposobnosti revizijskega osebja, potrebnega za uresničitev revizijskih ciljev,
- pomembnosti prepoznanih tveganj in njihov morebitni vpliv na revizijo,
- zbrane revizijske dokaze,
- strokovno usposobljenost, neoporečnost in ugotovitve drugih, na delo katerih se zanaša revizor IS.

2.1.4 Revizor IS mora ohraniti svojo neodvisnost in objektivnost duha v vseh zadevah, povezanih z izvajanjem posla revidiranja IT. Revizor mora biti pri obravnavanju revizijskih vprašanj in sprejemanju sklepov pošten, nepristranski in objektiven.

2.1.5 Revizor IS naj revizijo izvaja skrbno in pri tem upošteva strokovne standarde ter zakonske in druge predpisane zahteve. Revizor IS mora utemeljeno pričakovati, da je zadolžitve revizije IS mogoče izvesti v skladu z uveljavljenimi standardi revidiranja IS in drugimi ustreznimi predpisi, strokovnimi ali industrijskimi standardi, tako da bo po končani reviziji IS lahko izrazil strokovno mnenje. Revizor IS mora razkriti okoliščine kakršnih koli neskladnosti na način, ki je skladen z obveščanjem o izidih revizije.

2.1.6 Revizor IS mora imeti zadostno zagotovilo, da poslovodstvo razume svoje obveznosti in odgovornosti glede dajanja ustreznih, pomembnih in pravočasnih informacij, ki so potrebne za izvajanje revizijskega posla in zagotavljanja sodelovanja ustreznih zaposlenih med revizijo.

2.1.7 Revizor IS mora zakonito in pošteno delovati v interesu zainteresiranih, ob tem pa ohranjati visoke standarde ravnanja in značaja ter se ne sme vpletati v dejanja, ki bi škodovala ugledu poklica.

2.1.8 Revizor IS mora ohranjati zasebnost in zaupnost informacij, pridobljenih med opravljanjem svojih nalog, razen če razkritje zahtevajo z zakonom pooblaščeni organi. Take informacije se ne smejo uporabljati v zasebno korist ali razkrivati neustreznim strankam.

2.1.9 Revizor IS mora pri obveščanju ustreznih strank o izidih opravljenega dela ravnati z vso potrebno poklicno skrbnostjo.

2.1.10 Predvideni prejemniki revizijskih poročil upravičeno pričakujejo, da je revizor IS svoje delo ves čas revizije opravljal s potrebno poklicno skrbnostjo. Revizor IS ne sme sprejeti posla, če nima ustreznih sposobnosti, znanja in drugih virov za tako dokončanje dela, kot se od strokovnjaka pričakuje.

3. Datum uveljavitve

3.1 Ta smernica velja za vse revizije IS, ki se začnejo 1. septembra 1999 ali pozneje. Smernica je bila pregledana in posodobljena in velja od 1. marca 2008**.**

2006 Strokovna usposobljenost (G30)

1. Izhodišča

1.1 Povezava s standardi

1.1.1 Standard S4 (1006) Strokovna usposobljenost določa: »Revizor IS mora biti strokovno usposobljen in imeti veščine in znanje za izvajanje revizijske naloge. Revizor IS mora vzdrževati svojo strokovno usposobljenost z ustreznim stalnim strokovnim izobraževanjem in usposabljanjem.«

1.2 Povezava s COBIT-om

1.2.1 Kontrolni cilj na visoki ravni M3 (Pridobite neodvisno zagotovilo) navaja: »… pridobitev neodvisnega zagotovila, da se poveča zaupanje med organizacijami, strankami in tretjimi strankami kot izvajalci.«

1.2.2 Kontrolni cilj na visoki ravni M4 (Zagotovite neodvisno revizijo) navaja: »… zagotovitev neodvisne revizije, da se poveča stopnja zaupanja in izkoriščanja najboljših nasvetov iz prakse.«

1.2.3 Podrobni kontrolni cilj M3.7 (Strokovna usposobljenost neodvisne funkcije dajanja zagotovil) navaja: »Poslovodstvo mora zagotoviti, da ima neodvisna funkcija dajanja zagotovil strokovno usposobljenost, veščine in znanje, potrebne za uspešno, učinkovito in gospodarno izvajanje takih pregledov.«

1.2.4 Podroben kontrolni cilj M4.4 (Strokovna usposobljenost) navaja: »Poslovodstvo mora zagotoviti, da so revizorji, odgovorni za pregled dejavnosti IT organizacije, strokovno usposobljeni in da imajo kot skupina veščine, ki so potrebne za izvajanje takih revizij, in znanje (tj. domene CISA), potrebno za uspešno, učinkovito in gospodarno izvedbo takih pregledov. Poslovodstvo mora zagotoviti, da revizijsko osebje za revidiranje informacijskih sistemov vzdržuje svojo strokovno usposobljenost z ustreznim stalnim strokovnim izobraževanjem.«

1.3 Referenčno gradivo COBIT-a

1.3.1 COBIT-ovo referenčno gradivo ponujajo posebne COBIT-ove cilje ali procese, ki jih je treba upoštevati pri pregledovanju področja, ki ga obravnava ta smernica. Izbira najustreznejšega gradiva v COBIT-u, ki je primerno glede na predmet in obseg določene revizije, temelji na izbiri posebnih COBIT-ovih procesov IT in upoštevanju COBIT-ovih kontrolnih ciljev ter z njimi povezanih praks upravljanja. Za izpolnitev zahtev so izbrani in prilagojeni tisti COBIT-ovi procesi, ki bodo najverjetneje primerni. Razvrščeni so na primarne in sekundarne. Procesi in kontrolni cilji, ki jih je treba izbrati in prilagoditi, so lahko različni glede na določen obseg ter opis nalog in pristojnosti posla.

1.3.2 Primarni procesi so:

- PO7 *Upravljajte človeške vire*,
- M2 *Ocenite ustreznost notranjih kontrol*,
- M3 *Pridobite neodvisno zagotovilo*,
- M4 *Zagotovite neodvisno revizijo*.

1.3.3 Sekundarni procesi pa so:

- DS1 *Opredelite in upravljajte ravni storitev*,
- DS2 *Upravljajte storitve tretje stranke*,
- DS3 *Upravljajte delovanje in zmogljivost*,
- DS7 *Izobrazite in usposobite uporabnike*,
- M1 *Spremljajte proces*.

1.3.4 Najpomembnejša informacijska sodila za strokovno usposobljenost so:

- primarna: učinkovitost, uspešnost in razpoložljivost,
- sekundarna: zaupnost, celovitost, skladnost in zanesljivost.

1.4 Namen smernice

1.4.1 Od revizorjev IS se pričakuje, da so visoko strokovno usposobljeni. Da dosežejo ta cilj, morajo revizorji IS pridobiti potrebne veščine in zahtevano znanje za izvajanje nalog. Dodatni izziv pa je vzdrževanje strokovne usposobljenosti z nenehnim nadgrajevanjem svojega znanja in veščin.

1.4.2 S sprejemom izvajanja strokovnih storitev revizorji IS hkrati potrjujejo, da imajo želeno raven strokovne usposobljenosti, potrebno za izvedbo strokovnih storitev, in da bodo znanje in veščine revizorja IS skrbno in prizadevno uporabljene.

1.4.3 Glede na pričakovano visoko strokovno usposobljenost revizorji IS ne bi smeli prevzemati izvajanja nobenih storitev, za katere niso usposobljeni, razen če si pridobijo ustrezno svetovanje in pomoč, da lahko dajo sprejemljiva zagotovila za zadovoljivo opravljene storitve.

1.4.4 Revizor IS naj izvaja strokovne storitve z vso potrebno skrbnostjo, strokovnostjo in prizadevnostjo. Njegova stalna dolžnost je, da ohrani strokovno znanje in veščine na potrebni ravni, da lahko da sprejemljiva zagotovila, da bodo izpolnjene zahteve strokovnih revizijskih standardov in bo pregledovana organizacija deležna prednosti zanesljivih strokovnih storitev na podlagi najnovejših dosežkov razvoja v praksi, zakonodaji in tehniki.

1.4.5 ISACA uveljavlja vizijo, da je priznana svetovna vodilna organizacija za upravljanje IT, nadzor in dajanje zagotovil. V predgovoru k tej viziji je jasno poudarjeno, da bodo za prihodnji uspeh v strokah, ki jim je namenjena ISACA, potrebne veščine in sposobnosti, ki bodo dopolnjevale znanja, ki jih zagotavlja naziv CISA. ISACA je vodilna pri ugotavljanju, katere so te veščine in strokovne sposobnosti, in pri določanju načinov za njihovo ovrednotenje in presojo. Prav v zvezi s tem pa je potrebna smernica, ki daje navodila revizorjem IS, da si pridobijo potrebne veščine in znanje in ob izvajanju revizijskih poslov vzdržujejo svojo strokovno usposobljenost.

1.4.6 Ta smernica daje navodila za uporabo standarda revidiranja informacijskih sistemov S4 (1006) Strokovna usposobljenost. Revizor IS mora upoštevati to smernico pri ugotavljanju, kako doseči izvajanje omenjenega standarda, uporabiti strokovno presojo pri njegovi uporabi, in mora biti pripravljen utemeljiti vsako odstopanje.

1.5 Uporaba smernice

1.5.1 Pri uporabi te smernice mora revizor IS upoštevati njena navodila tudi glede na druge ustrezne standarde in smernice ISACA.

2. Odgovornost

2.1 Veščine in znanje

2.1.1 Revizor IS je predvsem odgovoren za pridobivanje potrebnega strokovnega znanja in tehničnih veščin za izvedbo vsakega posla, ki ga je sprejel.

2.1.2 Vodstvo revizije je sekundarno odgovorno za to, da je revizorju IS zaupalo izvedbo revizijskega posla, šele potem ko je zagotovilo, da ima revizor IS potrebno strokovno znanje in tehnične veščine, da lahko opravi svoje naloge.

2.1.3 Vodstvo revizije mora zagotoviti, da imajo člani skupine, ki izvajajo revizijo, potrebno znanje in veščine.

2.1.4 Veščine in znanje se razlikujejo glede na položaj in vlogo revizorja IS pri reviziji. Zahteva za upravljavske veščine in znanje naj bo sorazmerna s stopnjo revizorjeve odgovornosti.

2.1.5 Veščine in znanje vključujejo strokovnost pri prepoznavanju in obvladovanju tveganj in kontrolah ter poznavanje revizijskih orodij in tehnik. Revizor IS mora imeti analitično in tehnično znanje ter obvladati veščine vodenja razgovorov in medosebnih stikov ter predstavitvene veščine.

2.2 Strokovna usposobljenost

2.2.1 Strokovna usposobljenost pomeni imeti veščine ter strokovno znanje in izkušnje, pridobljene z ustrezno stopnjo izobrazbe in delovnimi izkušnjami.

2.2.2 Revizor IS mora dati sprejemljivo zagotovilo, da ima veščine in znanje, ki so potrebni za doseganje zahtevane ravni strokovne usposobljenosti.

2.2.3 Revizor IS naj izoblikuje želeno in/ali pričakovano raven strokovne usposobljenosti na podlagi ustreznih primerjalnih analiz. Te primerjalne analize se redno pregledujejo in posodabljajo.

2.2.4 Revizor IS in/ali vodstvo revizije mora dati pred sprejetjem revizijskega posla sprejemljivo zagotovilo, da so na voljo strokovno usposobljeni kadri, potrebni za izvedbo katere koli revizijske naloge. Razpoložljivost takih strokovno usposobljenih kadrov je treba potrditi/zagotoviti pred začetkom revizije.

2.2.5 Vodstvo revizije je odgovorno za zagotavljanje, da so člani skupine strokovno usposobljeni izvesti revizijske naloge. Ugotavljanje temeljnih strokovnih sposobnosti članov skupine bo pomagalo učinkovito izrabiti razpoložljive vire.

2.2.6 Velja, da je primerno, če revizorji IS delijo svoje znanje in izkušnje, pridobljene najboljše prakse, z delom pridobljene izkušnje in znanje z drugimi člani skupine, da se doseže boljša strokovna usposobljenost vseh. Usposobljenost članov skupine se lahko izboljša tudi s sestanki za oblikovanje skupinskega duha, delavnicami, konferencami, seminarji, predavanji in drugimi načini medsebojnega vplivanja in delovanja.

2.3 Nenehno vzdrževanje

2.3.1 Revizorji IS morajo nenehno spremljati svoje veščine in znanje, da ohranjajo sprejemljivo raven strokovne usposobljenosti.

2.3.2 Vzdrževanje strokovne usposobljenosti s stalnim strokovnim izobraževanjem lahko med drugim vključuje usposabljanje, izobraževalne tečaje, programe za pridobitev licence, univerzitetne tečaje, konference, seminarje, delavnice, telekonference, internetne konference in sestanke študijskih krožkov.

2.3.3 Pridobivanje veščin in znanja in vzdrževanje ravni strokovne usposobljenosti je treba nenehno spremljati in veščine, znanje ter strokovno usposobljenost tudi redno ocenjevati.

2.4 Ocenjevanje

2.4.1 Ocenjevanje je treba izvesti na pošten, pregleden, lahko razumljiv, nedvoumen, nepristranski način, ki velja za splošno sprejemljivo prakso v danem zaposlitvenem okolju.

2.4.2 Ocenjevalna sodila in postopki morajo biti jasno opredeljeni, lahko pa so različni glede na okoliščine, kot so zemljepisni položaj, politično ozračje, narava posla, kultura in druge podobne okoliščine.

2.4.3 V revizijski družbi ali skupini revizorjev naj se izvede medfunkcijsko notranje ocenjevanje med skupinami ali posamezniki.

2.4.4 Za posameznega neodvisnega revizorja IS pa naj se ocenjevanje izvede na medkolegialni ravni, če je le mogoče. Če pregled med strokovnimi kolegi ni mogoč, naj revizor uporabi samoocenjevanje in ga dokumentira.

2.4.5 Delo notranjega revizorja IS naj ocenjuje ustrezna raven poslovodstva, ki lahko po potrebi ocenjuje tudi delo zunanjih revizorjev IS.

2.4.6 Vrzeli, ugotovljene med ocenjevanjem, je treba ustrezno odpraviti.

2.5 Analiza vrzeli in usposabljanje

2.5.1 Vrzeli, ugotovljene na podlagi razlik med dejansko in pričakovano ravnijo usposobljenosti, je treba zapisati in analizirati. Če je kateri koli vir pomanjkljiv, se ne sme uporabljati za opravljanje revizijskih nalog, če niso izvedeni ustrezni ukrepi za odpravo pomanjkljivosti. Če pa se pomanjkljivost opazi šele po začetku revizijskega posla, mora revizor IS oziroma vodstvo revizije pretehtati možnost, da pomanjkljivi vir umakne in ga zamenja z usposobljenim. Če pa je zaradi nujnosti predlagano, da se za nadaljevanje revizijskega posla še naprej uporablja isti vir, je treba revidiranca obvestiti o obstoju vrzeli. Tudi če revizor IS lahko da sprejemljivo zagotovilo o kakovosti revizije, je treba za nadaljnjo uporabo pomanjkljivega vira pridobiti soglasje revidiranca.

2.5.2 Pomembno je, da se analizirajo osnovni vzroki in ugotovi razlog za tako vrzel in da se čim prej izvedejo ustrezni popravljalni ukrepi, kot je na primer usposabljanje.

2.5.3 Usposabljanje, potrebno za revizijski posel, bi bilo treba dokončati v razumnem roku in pred začetkom revidiranja.

2.5.4 Učinkovitost usposabljanja je treba izmeriti po preteku primernega časa po končanem usposabljanju.

2.6 Razpoložljivost usposobljenih virov

2.6.1 Revizor IS oziroma vodstvo revizije mora poznati in analizirati zahtevane veščine in znanje za predlagane revizijske naloge, preden odgovori na zahtevo za predlog.

2.6.2 Revizor IS oziroma vodstvo revizije mora dati sprejemljiva zagotovila, da so na voljo potrebni viri z ustreznimi veščinami, znanjem in zahtevano stopnjo strokovne usposobljenosti, preden se začnejo izvajati revizijske naloge.

2.6.3 Revizorji IS ne smejo zatrjevati, da imajo strokovno znanje, sposobnosti ali izkušnje, ki jih v resnici nimajo.

2.7 Zunanje izvajanje

2.7.1 Kadar je del revizijskega posla oddan v izvajanje ali je pridobljena zunanja strokovna pomoč, je treba dati sprejemljivo zagotovilo, da je zunanji strokovnjak ali agencija, ki ji je delo oddano v izvajanje, ustrezno usposobljena. Ta smernica se uporablja tudi za izbiro zunanjega strokovnjaka.

2.7.2 Kadar je pritegnjena stalna strokovna pomoč, je treba usposobljenost zunanjih strokovnjakov redno meriti in spremljati oziroma pregledovati.

3. Stalno strokovno izobraževanje

3.1 Zahteve strokovnih organizacij

3.1.1 Stalno strokovno izobraževanje je metodologija, sprejeta za ohranjanje usposobljenosti in nadgrajevanje veščin in znanja.

3.1.2 Revizorji IS morajo upoštevati zahteve po stalnem strokovnem izobraževanju, ki jih postavljajo ustrezne strokovne organizacije, v katerih se združujejo.

3.2 Ustrezni programi

3.2.1 Programi za stalno strokovno izobraževanje morajo pomagati pri razširitvi veščin in znanja in se morajo nanašati na strokovne in tehnične zahteve dajanja zagotovil, varnosti in upravljanja IS.

3.2.2 Strokovne organizacije običajno predpisujejo ustrezne programe za priznavanje stalnega strokovnega izobraževanja. Revizorji IS se morajo ravnati po normativih, ki jih predpisujejo njihove strokovne organizacije.

3.3 Pridobivanje točk za stalno strokovno izobraževanje

3.3.1 Strokovne organizacije običajno predpišejo metodologijo pridobivanja točk za stalno strokovno izobraževanje in najmanjše število točk, ki jih morajo redno pridobivati njihovi člani. Revizorji IS se morajo ravnati po normativih, ki jih predpisujejo njihove strokovne organizacije.

3.3.2 Če je revizor IS vključen v več strokovnih organizacij, v katerih lahko pridobi najmanjše število točk, lahko revizor IS po svoji presoji pridobi točke za stalno strokovno izobraževanje skupaj iz ustreznih programov, če so ti usklajeni s pravili/smernicami, ki so jih oblikovale te strokovnih organizacije.

3.4 Politika ISACA za stalno strokovno izobraževanje

3.4.1 ISACA ima izdelano celovito politiko za stalno strokovno izobraževanje, ki velja za njene člane in imetnike naziva CISA. Revizorji IS z nazivom CISA morajo ravnati v skladu s politiko ISACA za stalno strokovno izobraževanje. Podrobnosti te politike so na voljo na spletni strani ISACA, www.isaca.org/CISAcpePolicy. Pojasnjena so sodila za:

- pridobitev naziva,
- obrazec za potrditev navzočnosti,
- kodeks poklicne etike,
- preglede ur stalnega strokovnega izobraževanja,
- preklic, ponovno obravnavo in pritožbo,
- status upokojenih in nedelujočih članov CISA,
- ustrezne izobraževalne dejavnosti,
- izračun ur stalnega strokovnega izobraževanja.

4. Evidenca

4.1 Matrika veščin in evidenca usposabljanja

4.1.1 Oblikovati je treba matriko veščine s prikazom potrebne veščine, znanja in strokovne usposobljenosti za različne ravni zahtevnosti dela. Ta matrika navzkrižno povezuje razpoložljive vire in njihove veščine in znanje. Taka matrika pomaga pri ugotavljanju vrzeli in potreb po usposabljanju.

4.1.2 Evidenco zagotovljenega usposabljanja skupaj s povratnimi informacijami o usposabljanju in njegovi učinkovitosti je treba vzdrževati, analizirati in se nanjo sklicevati ob prihodnjih potrebah.

4.2 Evidenca stalnega strokovnega izobraževanja

4.2.1 Kot to predpisujejo ustrezne strokovne organizacije in tudi ISACA, morajo revizorji IS voditi primerno evidenco programov za stalno strokovno izobraževanje, jo določen čas hraniti in po potrebi dati na voljo za pregled.

5. Datum uveljavitve

5.1 Ta smernica velja za vse revizije informacijskih sistemov, ki se začnejo 1. junija 2005. Celoten glosar izrazov lahko najdete na spletni strani ISACA na naslovu www.isaca.org/glossary (slovenski prevod je na naslovu http://www.isaca.si/dokumenti/naslovka/ISACA_Glossary_Translation-SI_1303.pdf).

2007 Trditve (v razvoju)

2008 Merila (v razvoju)

Izvedbene smernice

Izvedbene smernice so:
2201 Načrtovanje posla (G15)
2202 Ocenjevanje tveganja pri revizijskem načrtovanju (G13)
2203 Izvedba in nadzor (G8)
2204 Revizijska pomembnost (G6)
2205 Revizijski dokazi (G2)
2206 Uporaba dela drugih strokovnjakov (G1)
2207 Nepravilnosti in nezakonita dejanja (G9)
2208 Revizijsko vzorčenje (G10)

Smernice so na tem mestu vključene v celoti. Za povezave na posamezne standarde obiščite *www.isaca.org/standard*.

2201 Načrtovanje posla (G15)

1. Izhodišča

1.1 Povezava s standardi

1.1.1 Standard S5 (1201) Načrtovanje določa, da morajo strokovnjaki za revidiranje in dajanje zagotovil za IT načrtovati revizije informacijskih sistemov (IS), tako da upoštevajo cilje revizije in zagotovijo skladnost z ustreznimi zakoni in strokovnimi revizijskimi standardi. Izdelati in dokumentirati morajo:
- revizijski pristop, ki temelji na tveganjih,
- revizijski načrt s podrobnim opisom vrste in ciljev, časa in obsega, ciljev revizije in potrebnih virov,
- revizijski program in/ali načrt, ki podrobno navaja vrsto, čas in obseg revizijskih postopkov, potrebnih za dokončanje revizije.

1.1.2 Standard S11 (1202) Uporaba ocenjevanja tveganja pri revizijskem načrtovanju določa, da morajo strokovnjaki za revidiranje in dajanje zagotovil za IT:
- pri pripravi celovitega načrta revidiranja IS in pri določanju prednostnih nalog za učinkovito razporeditev virov za revidiranje IS uporabiti ustrezno tehniko oziroma pristop k ocenjevanju tveganja;
- pri načrtovanju posameznih pregledov prepoznati in oceniti tveganja, povezana s področjem pregleda, ter njegove povezave z drugimi področji revizije.

1.1.3 Standard S12 (1204) Revizijska pomembnost določa, da morajo strokovnjaki za revidiranje in dajanje zagotovil za IT upoštevati:
- revizijsko pomembnost in njeno povezanost z revizijskim tveganjem, ko se odloča o vrsti, času in obsegu revizijskih postopkov;
- morebitne slabosti ali odsotnost kontrol in pretehtati, ali bi take slabosti ali odsotnost kontrol lahko povzročile tudi bistveno pomanjkljivost ali pomembno slabost v informacijskem sistemu ter le-to upoštevati pri načrtovanju revizije;
- skupni učinek manjših pomanjkljivosti ali slabosti in odsotnosti kontrol, ki lahko povzročijo bistveno pomanjkljivost ali pomembno slabost v informacijskem sistemu.

1.2 Povezava s COBIT-om

1.2.1 Izbira najustreznejšega gradiva v COBIT-u, ki je ustrezno glede na področje določene revizije, temelji na izbiri posebnih COBIT-ovih procesov IT in upoštevanju COBIT-ovih kontrolnih ciljev ter z njimi povezanih praks upravljanja. Za izpolnitev zahtev strokovnjakov za revidiranje in dajanje zagotovil za IT v zvezi z načrtovanjem so postopki iz COBIT-a, ki bodo najverjetneje ustrezni, izbrani in prilagojeni, tu uvrščeni med primarne in sekundarne. Procesi in kontrolni cilji, ki jih je treba izbrati in prilagoditi, so lahko različni glede na posebno področje dela ter opis nalog in pristojnosti posla.

1.2.2 Primarni procesi IT so:
- ME1 *Spremljajte in vrednotite delovanje IT*,
- ME2 *Spremljajte in vrednotite notranje kontrole*,
- ME3 *Zagotovite skladnost z zunanjimi zahtevami*.

1.2.3 Sekundarni IT proces pa je:
- ME4 *Zagotovite upravljanje IT*.

1.2.4 Najpomembnejša informacijska sodila so:
- primarna: učinkovitost, uspešnost, razpoložljivost in skladnost,
- sekundarna: zaupnost, celovitost in zanesljivost.

1.3 Potreba po smernici

1.3.1 Namen te smernice je opredeliti sestavine v postopku načrtovanja, kot so navedene v standardu S5 (1201) v *ITAF: Okvir strokovnih praks za dajanje zagotovil za IT*.

1.3.2 Ta smernica tudi omogoča, da se z načrtovanjem revizijskega postopka dosežejo v COBIT-u zastavljeni cilji.

2. Dejavnosti pred izvedbo posla

2.1 Namen

2.1.1 Namen dejavnosti pred izvedbo posla je pomagati pri zagotavljanju, da so strokovnjaki za revidiranje in dajanje zagotovil za IT proučili vse dogodke ali okoliščine, ki bi lahko negativno vplivale na njihovo zmožnost, da načrtujejo in izvedejo revizijski posel ter zmanjšajo revizijsko tveganje na sprejemljivo nizko raven. Izvajanje teh predhodnih dejavnosti pomaga zagotoviti, da načrti za revizijski posel vključujejo naslednje:
- strokovnjaki za revidiranje in dajanje zagotovil za IT ohranjajo potrebno neodvisnost in zmožnost izvedbe posla,
- v zvezi z neoporečnostjo poslovodstva ni nobenih vprašanj, ki bi lahko vplivala na pripravljenost strokovnjaka za revidiranje in dajanje zagotovil za IT, da nadaljuje izvajanje posla,
- s strankami ni nobenega nesporazuma glede pogojev posla.

2.2 Dejavnosti

2.2.1 Strokovnjaki za revidiranje in dajanje zagotovil za IT naj izvedejo postopke v zvezi z ohranjanjem razmerja s stranko in določenega revizijskega posla. Pri stalnih revizijskih poslih se taki začetni postopki pogosto opravijo kmalu po zaključku prejšnje revizije.

2.2.2 Strokovnjaki za revidiranje in dajanje zagotovil za IT naj ocenijo skladnost z etičnimi zahtevami, vključno z neodvisnostjo. Začetni postopki strokovnjakov za revidiranje in dajanje zagotovil za IT tako glede nadaljevanja razmerja s stranko kot glede ocenjevanja etičnih zahtev (vključno z neodvisnostjo) se opravijo pred izvajanjem drugih, za tekoči revizijski posel pomembnih dejavnosti.

2.2.3 Strokovnjaki za revidiranje in dajanje zagotovil za IT naj se seznanijo s pogoji posla.

3. Načrtovanje

3.1 Revizijska strategija

3.1.1 Strokovnjaki za revidiranje in dajanje zagotovil za IT naj posel načrtujejo tako, da bo uspešno izveden, za revizijo pa naj določijo celovito revizijsko strategijo. Ustrezno načrtovanje pomaga zagotoviti, da bo pomembnim področjem revizije namenjena ustrezna pozornost, da bodo morebitne težave pravočasno prepoznane in rešene ter da bo revizijski posel primerno organiziran in voden, tako da bo izveden uspešno in učinkovito.

3.1.2 Jasna opredelitev projekta je kritičen dejavnik uspeha, ki zagotovi uspešnost in učinkovitost. Projekt revizije naj v opisu nalog in pristojnosti vsebuje zadeve, kot so:

- področja, ki naj se revidirajo,
- vrsto načrtovanega dela,
- visokonivojske cilje in obseg dela,
- teme, kot na primer proračun, dodelitev virov, razpored datumov, vrsta poročila, predvideni uporabniki/prejemniki,
- druge splošne vidike dela, kadar je to primerno.

3.1.3 Za funkcijo notranje revizije naj bo celovit revizijski načrt na podlagi tveganj za redne dejavnosti izdelan/posodobljen najmanj enkrat na leto. Tak načrt na visoki ravni naj služi kot okvir za revizijske dejavnosti in je namenjen reševanju nalog, določenih z revizijsko listino.

3.1.4 Običajno je načrt treba izdelati za vsako revizijsko nalogo. V načrtu morajo biti dokumentirani cilji revizije.

3.1.5 Vsak revizijski projekt se mora sklicevati na splošni revizijski načrt ali pa vsebovati posebna pooblastila, cilje in druge pomembne vidike dela, ki ga je treba opraviti.

3.1.6 Strokovnjaki za revidiranje in dajanje zagotovil za IT morajo pripraviti revizijski načrt, v katerem upoštevajo cilje revidiranca, ki se nanašajo na revizijsko področje in s tem povezano tehnološko infrastrukturo. Kadar je to primerno, naj upoštevajo tudi področje pregleda in njegovo pomembnost za podjetje (strateško, finančno in/ali operativno) ter pridobijo informacije o strateškem načrtu, vključno s strateškim načrtom za IT, in vso drugo ustrezno dokumentacijo v zvezi z revidirancem.

3.1.7 Strokovnjaki za revidiranje in dajanje zagotovil za IT naj spoznajo informacijsko arhitekturo in tehnološko usmeritev revidiranca, da lahko oblikujejo načrt, ki je primeren za sedanjo, in kjer je primerno, tudi za prihodnjo tehnologijo revidiranca.

3.2 Poznavanje podjetja

3.2.1 Razumevanje revidirančevega poslovanja in tveganj, s katerimi se sooča, je odločilen korak pri pripravi učinkovitega revizijskega načrta, osredotočenega na področja, ki so najobčutljivejša za prevare ali netočna ravnanja.

3.2.2 Pred začetkom revizijskega projekta naj bo delo strokovnjakov za revidiranje in dajanje zagotovil za IT načrtovano na način, ki je najprimernejši za dosego revizijskih ciljev. V okviru načrtovalnega postopka naj spoznajo podjetje in njegove procese. Poleg tega, da bodo strokovnjaki za revidiranje in dajanje zagotovil za IT spoznali delovanje podjetja in njegove zahteve za IT, jim bo to pomagalo pri določanju pomembnosti virov IT, ki jih pregledujejo, saj so ti povezani s cilji podjetja. Strokovnjaki za revidiranje in dajanje zagotovil za IT naj določijo obseg revizijskega dela ter izvedejo predhodno oceno notranjih kontrol nad funkcijo, ki jo pregledujejo.

3.2.3 Obseg poznavanja podjetja in njegovih procesov, ki se zahteva od strokovnjakov za revidiranje in dajanje zagotovil za IT, bo določen glede na vrsto podjetja in raven podrobnosti izvajanja revizijskega dela. Kadar strokovnjaki za revidiranje in dajanje zagotovil za IT obravnavajo neobičajne ali zapletene postopke, se od njih lahko zahteva tudi specializirano znanje. Obsežnejše poznavanje podjetja in njegovih procesov bo običajno prej zahtevano, kadar revizijski cilj zajema velik razpon funkcij IT, kot če se cilji nanašajo le na omejene funkcije. Za pregled s ciljem ovrednotenja nadzora nad plačnim sistemom podjetja bi bilo na primer običajno potrebno temeljitejše poznavanje podjetja kot za pregled s ciljem preizkusa kontrol v posebnem sistemu programskih knjižnic.

3.2.4 Strokovnjaki za revidiranje in dajanje zagotovil za IT naj spoznajo tipe osebja, dogodkov, transakcij in ravnanj, ki lahko bistveno vplivajo na določeno podjetje, funkcijo, proces ali podatke, ki so predmet revizijskega projekta. Poznavanje podjetja naj vključuje tudi poslovna, finančna in vgrajena tveganja, s katerimi se podjetje sooča, kakor tudi razmere na trgu podjetja in informacije o tem, v kolikšnem obsegu se podjetje pri doseganju svojih ciljev zanaša na zunanje storitve. Strokovnjaki za revidiranje in dajanje zagotovil za IT naj te informacije uporabijo pri prepoznavanju morebitnih težav, oblikovanju ciljev in področja dela, pri izvajanju dela in proučevanju ukrepov poslovodstva, na katera bi morali biti pozorni.

3.3 Pomembnost

3.3.1 V postopku načrtovanja naj strokovnjaki za revidiranje in dajanje zagotovil za IT praviloma določijo ravni pomembnosti načrtovanja, tako da bo revizijsko delo zadoščalo za uresničitev revizijskih ciljev in da bodo revizijski viri učinkovito uporabljeni. Na primer, pri pregledu obstoječega sistema bo strokovnjak za revidiranje in dajanje zagotovil za IT med načrtovanjem revizijskega programa za delo, ki ga je treba opraviti, ocenil pomembnost različnih sestavnih delov sistema. Pri določanju pomembnosti naj se upoštevajo tako kakovostni kot tudi količinski vidiki.

3.4 Ocenjevanje tveganja

3.4.1 Strokovnjaki za revidiranje in dajanje zagotovil za IT naj za revizijo izdelajo revizijski načrt, da zmanjšajo revizijsko tveganje na sprejemljivo raven.

3.4.2 Izvede naj se ocenjevanje tveganj, da se pridobi sprejemljivo zagotovilo, da bodo pomembne teme med revizijo ustrezno pokrite. S tem ocenjevanjem naj se ugotovijo področja, na katerih so pomembne težave zelo verjetne.

3.4.3 Ocena tveganj in razvrstitev prepoznanih tveganj glede na pomembnost za področje, ki se pregleduje, in za okolje IT v podjetju naj bosta izvedeni v potrebnem obsegu.

3.5 Ocenjevanje notranje kontrole

3.5.1 Projekti revidiranja in dajanja zagotovil naj vključujejo proučitev notranjih kontrol, in sicer neposredno v okviru ciljev projekta ali kot podlago za zanesljivost informacij, ki se zbirajo v okviru projekta. Kadar je cilj ocenjevanje notranjih kontrol, naj strokovnjaki za revidiranje in dajanje zagotovil za IT proučijo, v kolikšnem obsegu bo treba pregledati take kontrole. Kadar je cilj ocena učinkovitosti kontrol v določenem obdobju, naj revizijski načrt vključuje ustrezne postopke za dosego revizijskih ciljev, in med temi postopki naj bo

tudi preizkušanje skladnosti kontrol. Kadar pa ni cilj ocena učinkovitosti kontrol v določenem obdobju, ampak le ugotavljanje kontrolnih postopkov v določenem trenutku, se preizkušanje skladnosti kontrol lahko izključi.

3.5.2 Kadar strokovnjaki za revidiranje in dajanje zagotovil za IT ocenjujejo notranje kontrole z namenom, da se lahko zanesejo na kontrolne postopke v podporo informacij, zbranih kot del revizije, naj praviloma predhodno ocenijo kontrole in izdelajo revizijski načrt na podlagi tega ocenjevanja. Med pregledom naj strokovnjaki za revidiranje in dajanje zagotovil za IT pretehtajo primernost tega ocenjevanja, ko določajo, v kolikšnem obsegu se med preizkušanjem lahko zanesejo na te kontrole. Na primer, pri uporabi računalniškega programa za preizkus podatkovnih datotek naj strokovnjak za revidiranje in dajanje zagotovil za IT ovrednoti kontrole nad programskimi knjižnicami, v katerih so programi, ki se uporabljajo za revizijske namene, da določi, v kolikšnem obsegu so ti programi zaščiteni pred nepooblaščenim spreminjanjem.

4. Spremembe med potekom revizije

4.1 Strategija in načrtovanje

4.1.1 Celotna revizijska strategija in revizijski načrt naj se po potrebi med potekom revizije posodobita in spremenita.

4.1.2 Načrtovanje revizije je nenehen in ponavljajoč se proces. Zaradi nepričakovanih dogodkov, spremenjenih razmer ali revizijskih dokazov, pridobljenih iz izidov revizijskih postopkov, morajo strokovnjaki za revidiranje in dajanje zagotovil za IT morda prilagoditi celotno revizijsko strategijo in posledično tudi načrtovane vrsto, čas in obseg nadaljnjih revizijskih postopkov.

4.1.3 Revizijsko načrtovanje naj upošteva možnost nepričakovanih dogodkov, ki pomenijo velika tveganja za podjetje. Zato mora revizijski načrt omogočati prednostno in tveganju ustrezno obravnavo takih dogodkov v postopkih revidiranja in dajanja zagotovil.

5. Nadzor

5.1 Člani delovne skupine

5.1.1 Strokovnjaki za revidiranje in dajanje zagotovil za IT naj načrtujejo vrsto, čas in obseg vodenja in nadzora članov delovne skupine ter pregled njihovega dela. To načrtovanje je odvisno od mnogih dejavnikov, vključno z velikostjo in zapletenostjo podjetja, področjem revizije, tveganji pomembno napačne navedbe, zmožnostjo in strokovno usposobljenostjo osebja, ki opravlja revizijsko delo, ter obsegom vodenja in nadzora članov delovne skupine na podlagi ocenjenega tveganja pomembno napačne navedbe.

6. Dokumentacija

6.1 Dokumentacija o načrtovanju

6.1.1 Delovno gradivo strokovnjaka za revidiranje in dajanje zagotovil za IT naj vključuje revizijski načrt in program.

6.1.2 Revizijski načrt je lahko dokumentiran na papirju ali v drugi ustrezni in obnovljivi obliki.

6.2 Potrditev načrta

6.2.1 Kolikor je to primerno, naj revizijski načrt, revizijski program in vse poznejše spremembe odobri vodstvo revizije.

6.3 Revizijski program

6.3.1 Strokovnjak za revidiranje in dajanje zagotovil za IT naj praviloma pred začetkom del določi predhodni program pregleda. Ta revizijski program naj bo dokumentiran na način, ki bo strokovnjaku za revidiranje in dajanje zagotovil za IT omogočal dokumentiranje že dokončanega revizijskega dela in pregled dela, ki ga je še treba opraviti. Med delom naj strokovnjak za revidiranje in dajanje zagotovil za IT ocenjuje ustreznost programa na podlagi informacij, zbranih med revizijo. Če strokovnjaki za revidiranje in dajanje zagotovil za IT ugotovijo, da načrtovani postopki niso zadostni, naj program ustrezno spremenijo.

6.3.2 Glede na vire, zahtevane za izvedbo revizije, mora strokovnjak za revidiranje in dajanje zagotovil za IT vključiti v revizijski načrt tudi upravljanje potrebnih kadrovskih virov.

6.3.3 Revizijski načrt naj bo pripravljen tako, da je poleg standardov, določenih v ITAF-u, usklajen z vsemi primernimi zunanjimi zahtevami.

6.3.4 Poleg seznama del, ki jih je treba opraviti, naj strokovnjak za revidiranje in dajanje zagotovil za IT, če je to izvedljivo, pripravi še seznam osebja in drugih potrebnih virov za dokončanje dela, časovni razpored dela in proračun.

6.3.5 Revizijski program in/ali načrt naj bo med potekom revizije prilagojen, tako da se rešijo vse zadeve, ki se pojavijo med revizijo (nova tveganja, napačne predpostavke ali ugotovitve iz že opravljenih postopkov).

7. Datum uveljavitve

7.1 Ta smernica velja za vse revizije IT, ki se začnejo 1. maja 2010.

2202 Ocenjevanje tveganja pri revizijskem načrtovanju (G13)

1. Izhodišča

1.1 Povezava s standardi

1.1.1 Standard S5 (1201) Načrtovanje določa: »Revizor IS mora načrtovati obseg revizije informacijskih sistemov tako, da upošteva cilje revizije in zagotovi skladnost z ustreznimi zakoni in strokovnimi revizijskimi standardi.«

1.1.2 Standard S6 (1203) Izvajanje revizijskih del določa: »Med potekom revizije mora revizor IS pridobiti zadostne in ustrezne dokaze, da se dosežejo revizijski cilji. Revizijski izsledki in ugotovitve morajo biti podprti z ustrezno analizo in razlago teh dokazov.«

1.1.3 V odstavku 2.4.1 smernice za revidiranje informacijskih sistemov G15 (2201) Revizijsko načrtovanje je navedeno: »Ocenjevanje tveganja je potrebno, da se pridobijo utemeljena zagotovila, da bodo pomembne teme med revizijo ustrezno pokrite. S tem ocenjevanjem naj se ugotovijo področja sorazmerno velikega tveganja, da obstajajo pomembne težave.«

1.2 Povezava s postopki

1.2.1 To smernico je mogoče uporabljati v povezavi z revizijskim postopkom za informacijske sisteme P1 Ocenjevanje in vrednotenje tveganja IS.

1.3 Povezava s COBIT-om

1.3.1 Izbira najustreznejšega gradiva v COBIT-u, ki je primerno glede na predmet in obseg določene revizije, temelji na izbiri posebnih COBIT-ovih procesov IT in upoštevanju COBIT-ovih kontrolnih ciljev in z njimi povezanih praks upravljanja. Za izpolnjevanje zahtev glede revizijske dokumentacije revizorjev IS so postopki v COBIT-u, ki bodo najverjetneje ustrezni, izbrani in prilagojeni, razvrščeni na primarne in sekundarne.

1.3.2 PO9 *Ocenjujte in obvladujte tveganja IT* izpolnjuje poslovno zahtevo za IT glede analize in sporočanja tveganj IT in njihovega morebitnega vpliva na poslovne procese in cilje z usmerjanjem v razvoj okvira za obvladovanje tveganj, ki je vključen v okvire za obvladovanje poslovnih in operativnih tveganj, ocenjevanje tveganj, zmanjševanje tveganj in sporočanje preostalega tveganja.

1.3.2 ME2 *Spremljajte in vrednotite notranje kontrole* izpolnjuje poslovno zahtevo za IT glede varovanja uresničevanja ciljev IT in zagotavljanja skladnosti z zakoni, predpisi in pogodbami, ki zadevajo IT, z usmerjanjem v spremljanje procesov notranje kontrole za aktivnosti, povezane z IT, ter določanje ukrepov za izboljševanje.

1.3.5 Sekundarni viri:
- ME3 *Zagotovite skladnost z zunanjimi zahtevami*,
- ME4 *Zagotovite upravljanje IT*.

1.3.6 Najpomembnejša informacijska sodila so:
- primarna: zaupnost, celovitost, razpoložljivost,
- sekundarna: učinkovitost, uspešnost, skladnost in zanesljivost.

1.4 Potreba po smernici

1.4.1 Stopnja revizijskega dela, potrebna za uresničitev določenega revizijskega cilja je subjektivna odločitev revizorja IS. Tveganje, da pride na podlagi revizijskih izsledkov do nepravilnega sklepa (revizijsko tveganje), je eden od vidikov te odločitve. Drugo pa je tveganje, da se bodo na pregledovanem področju pojavile napake (tveganje napake). Priporočene prakse za ocenjevanje tveganja pri izvajanju finančnih revizij so dobro dokumentirane v standardih revidiranja za finančne revizorje, potrebna pa so navodila, kako naj se take tehnike uporabljajo za revizije IS.

1.4.2 Tudi člani poslovodstva se odločajo o tem, koliko nadzora je potrebnega, na podlagi ocene ravni izpostavljenosti tveganju, ki so jo še pripravljeni sprejeti. Nekaj časa trajajoča nezmožnost izvajanja računalniških aplikacij je na primer izpostavljenost tveganju, do katere bi lahko prišlo zaradi nepričakovanih in nezaželenih dogodkov (npr. požara v podatkovnem centru). Izpostavljenost tveganju je mogoče zmanjšati z uvedbo ustrezno zasnovanih kontrol. Te kontrole običajno temeljijo na verjetnostni oceni pojavljanja negativnih dogodkov in so namenjene zmanjševanju take verjetnosti. Požarni alarm na primer ne preprečuje požarov, namenjen pa je zmanjšanju obsega škode zaradi požara.

1.4.3 Ta smernica daje navodila za uporabo standardov revidiranja IS. Revizor IS jo mora upoštevati pri odločanju o tem, kako bo uporabljal standarda revidiranja S5 (1201) in S6 (1203), uporabljati jo mora po strokovni presoji in biti pripravljen utemeljiti vsako odstopanje.

2. Načrtovanje

2.1 Izbira metodologije za ocenjevanje tveganja

2.1.1 Na voljo je veliko metodologij za ocenjevanje tveganja, med katerimi revizor IS lahko izbira. Njihov razpon zajema vse od preprostih razvrstitev na visoko, srednje in nizko tveganje na podlagi presoje revizorja IS pa vse do zapletenih in očitno znanstvenih izračunov, ki dajo številčno oceno tveganja. Revizorji IS naj upoštevajo raven zapletenosti in podrobne razčlenitve, ki je ustrezna za organizacijo, ki jo revidirajo.

2.1.2 Revizorji IS naj v metodologijo vključijo vsaj analizo tveganj za podjetje zaradi izgube razpoložljivosti sistema in kontrol, ki jo podpirajo, integritete podatkov in zaupnosti poslovnih informacij.

2.1.3 Vse metodologije za ocenjevanje tveganj se na določeni točki v procesu (npr. pri dodeljevanju pomembnosti različnim parametrom) naslanjajo na subjektivno presojo. Revizor IS bi moral vedeti, katere subjektivne odločitve so potrebne pri uporabi določene metodologije, in pretehtati, ali take presoje lahko ustrezno opredeli, jih preveri in doseže primerno raven natančnosti.

2.1.4 Pri odločanju o najustreznejši metodologiji za ocenjevanje tveganja morajo revizorji IS upoštevati, na primer:
- vrsto informacij, ki jih je treba zbrati (nekateri sistemi uporabljajo finančne učinke kot edino merilo, kar pa za revizije IS ni vedno ustrezno),
- ceno programske opreme ali drugih licenc, potrebnih za uporabo metodologije,

- kolikšen obseg potrebnih informacij je že na razpolago,
- koliko dodatnih informacij je še treba zbrati, preden bo mogoče pridobiti zanesljiv izid, in kakšni so stroški zbiranja teh informacij (vključno s časom, ki ga bo treba porabiti za njihovo zbiranje),
- mnenja drugih uporabnikov te metodologije in njihove poglede na to, koliko jim je pomagala pri izboljševanju uspešnosti in/ali učinkovitosti njihovih revizij,
- pripravljenost poslovodstva, da sprejme to metodologijo kot sredstvo za določanje vrste in ravni opravljenega revizijskega dela.

2.1.5 Od nobene posamezne metodologije za ocenjevanje tveganja ni mogoče pričakovati, da bo ustrezna v vseh okoliščinah. Razmere, ki vplivajo na revizije, se sčasoma lahko spremenijo. Zato bi moral revizor IS občasno ponovno oceniti ustreznost izbranih metodologij za ocenjevanje tveganja.

2.2 Uporaba ocenjevanja tveganja

2.2.1 Revizorji IS bi morali pri pripravi celovitega revizijskega načrta in pri načrtovanju posebnih revizij uporabiti izbrane tehnike ocenjevanja tveganja. Ocenjevanje tveganja v povezavi z drugimi revizijskimi tehnikami je treba upoštevati pri načrtovanih odločitvah, kot so:

- vrsta, obseg in čas revizijskih postopkov,
- področja ali poslovne funkcije, ki jih je treba revidirati,
- količina časa in virov, ki jih je treba nameniti za revizijo.

2.2.2 Revizor IS mora upoštevati vsako od naslednjih vrst tveganja, da določi njihovo celotno raven:

- tveganje pri delovanju,
- tveganje pri kontroliranju,
- tveganje pri odkrivanju.

2.3 Tveganje pri delovanju

2.3.1 Tveganje pri delovanju je dovzetnost revizijskega področja za napako na način, ki utegne biti posamično ali v povezavi z drugimi napakami pomemben ob predpostavki, da ni bilo nobenih ustreznih notranjih kontrol. Tveganje pri delovanju, povezano z varnostjo operacijskega sistema, je običajno visoko, ker bi spremembe podatkov ali programov ali celo njihovo razkritje zaradi slabosti pri varnosti operacijskega sistema lahko povzročilo napačne poslovodne informacije ali slabšo konkurenčno prednost. Nasprotno pa je tveganje pri delovanju, povezano z varnostjo za nepovezan osebni računalnik, običajno majhno, če se z ustrezno analizo dokaže, da se ne uporablja za poslovno-kritične namene.

2.3.2 Običajno je tveganje pri delovanju za večino revizijskih področij IS visoko, ker morebitni učinki napak običajno segajo na več poslovnih sistemov in mnogo uporabnikov.

2.3.3 Pri ocenjevanju tveganja pri delovanju mora revizor IS upoštevati tako vseobsegajoče kot tudi podrobne kontrole IS. To pa seveda ne velja, kadar se zadolžitev revizorja IS nanaša samo na vseobsegajoče kontrole IS.

2.3.4 Na ravni vseobsegajočih kontrol IS mora revizor IS glede na raven, ki je ustrezna za revizijsko področje, upoštevati:

- neoporečnost vodstva IS ter izkušnje in znanje vodstva IS,
- spremembe v upravljanju IS,
- pritiske na vodstvo IS, ki jih lahko navede na skrivanje ali napačno navajanje informacij (npr. velike poslovno-kritične prekoračitve na projektih, hekerska dejavnost),
- naravo poslovanja in sistemov organizacije (npr. načrti za e-poslovanje, zapletenost sistemov, pomanjkanje celovitih sistemov),
- dejavnike, ki vplivajo na panogo organizacije kot celoto (npr. spremembe v tehnologiji, razpoložljivost osebja IS),
- stopnjo vpliva tretje stranke na nadzor sistemov, ki se revidirajo (npr. zaradi povezanosti dobavne verige, zunanjega izvajanja postopkov IS, skupnih poslovnih projektov in neposrednega dostopa strank),
- izsledke in čas prejšnjih revizij.

2.3.5 Na ravni podrobnih IS kontrol mora revizor IS glede na raven, ki je ustrezna za revizijsko področje, upoštevati:

- izsledke in čas prejšnjih revizij na tem področju,
- zapletenost sistemov na tem področju,
- stopnjo potrebnih ročnih posegov,
- dovzetnost za izgubo ali nezakonito prisvojitev sredstev, ki jih sistem nadzoruje (npr. zaloge, plače),
- verjetnost konic dejavnosti ob določenem času v revizijskem obdobju,
- dejavnosti zunaj običajnih rednih vsakodnevnih obdelav IS (npr. uporaba pomožnih programov operacijskega sistema za spreminjanje podatkov),
- neoporečnost, izkušnje in sposobnosti poslovodstva in osebja, vključenega v uporabo kontrol IS.

2.4 Tveganje pri kontroliranju

2.4.1 Tveganje pri kontroliranju je tveganje, da sistem notranjih kontrol ne bo pravočasno preprečil ali odkril in popravil napake, ki bi se lahko zgodila na revizijskem področju in bi posamično ali v povezavi z drugimi napakami lahko bila pomembna. Tveganje pri kontroliranju, povezano z ročnimi pregledi računalniških dnevnikov, je na primer lahko visoko, ker so zaradi obsega vpisanih informacij dejavnosti, ki jih je treba preiskovati, pogosto lahko spregledane. Tveganje pri kontroliranju računalniško podprtih postopkov za preverjanje računalniško vodenih podatkov je običajno majhno, ker se ti postopki dosledno uporabljajo.

2.4.2 Revizor IS naj oceni tveganje pri kontroliranju kot visoko, razen če so ustrezne notranje kontrole:

- ugotovljene,
- ocenjene kot uspešne,
- preizkušene in dokazano ustrezno delujejo.

2.5 Tveganje pri odkrivanju

2.5.1 Tveganje pri odkrivanju je tveganje, da revizor IS s postopki preizkušanja podatkov ne bo odkril napake, ki bi bila posamično ali v povezavi z drugimi napakami lahko pomembna. Tveganje pri odkrivanju, povezano s prepoznavanjem kršitev varnosti v

aplikacijskem sistemu, je na primer običajno visoko, ker med revizijo dnevniki za celotno obdobje revizije niso na voljo. Tveganje pri odkrivanju, povezano z ugotavljanjem pomanjkanja načrtov za obnovo po katastrofi, pa je običajno majhno, ker je obstoj takih načrtov lahko preveriti.

2.5.2 Pri določanju ravni potrebnih postopkov za preizkušanja podatkov morajo revizorji IS upoštevati:
- ocenjevanje tveganja pri delovanju in
- ugotovitve glede tveganja pri kontroliranju po preizkušanju skladnosti.

2.5.3 Višje kot sta ocenjena tveganje pri delovanju in tveganje pri kontroliranju, več revizijskih dokazov morajo revizorji IS običajno pridobiti iz izvajanja revizijskih postopkov preizkušanja podatkov.

3. Izvajanje revizijskega dela

3.1 Dokumentacija

3.1.1 Revizorji IS morajo proučiti potrebo po dokumentiranju tehnik ali metodologij za ocenjevanje tveganja, uporabljenih za določeno revizijo. Dokumentacija običajno vsebuje:
- opis uporabljene metodologije za ocenjevanje tveganja,
- prepoznane pomembne izpostavljenosti in z njimi povezana tveganja,
- tveganja in izpostavljenosti, ki jih revizor namerava obdelati med revizijo,
- revizijske dokaze, uporabljene v podporo revizorjevi oceni tveganja.

4. Datum uveljavitve

4.1 Ta smernica velja za vse revizije IS, ki se začnejo 1. septembra 2000 ali pozneje. Smernica je bila pregledana in posodobljena ter velja od 1. avgusta 2008**.**

2203 Izvedba in nadzor (G8)

1. Izhodišča

1.1 Povezava s standardi

1.1.1 Standard S5 (1201) Načrtovanje določa: »Revizor IS mora izdelati in dokumentirati revizijski načrt, v katerem so našteti revizijski postopki s podrobnim opisom njihove vrste in ciljev, čas in obseg revizije, cilji revizije in potrebni viri.«

1.1.2 Standard S6 (1203) Izvajanje revizijskih del določa: »Med potekom revizije mora revizor IS pridobiti zadostne, zanesljive in ustrezne dokaze, da se dosežejo revizijski cilji. Revizijski izsledki in ugotovitve morajo biti podprti z ustrezno analizo in razlago teh dokazov. Revizijski proces mora biti dokumentiran z opisi opravljenega revizijskega dela in revizijskimi dokazi, ki podpirajo izsledke in ugotovitve revizorja IS.«

1.1.3 Standard S7 (1401) Poročanje določa: »Revizor IS mora po končani reviziji pripraviti poročilo v primerni obliki. Revizijsko poročilo mora vsebovati področje, cilje, obravnavano obdobje in vrsto, čas in trajanje opravljenega revizijskega dela. Poročilo mora vsebovati izsledke, ugotovitve in priporočila ter vse morebitne pridržke, omejitve ali omejitve področja dela, ki jih ima revizor IS v zvezi z revizijo. Ob izdaji mora biti poročilo revizorja IS podpisano, opremljeno z datumom in predloženo v skladu z določili revizijske listine ali listine o poslu.«

1.1.4 Standard S12 (1204) Revizijska pomembnost določa: »V svojem poročilu mora revizor IS razkriti neučinkovite kontrole ali pomanjkanje kontrol ter pomembnost neučinkovitosti kontrol in možnost, da te slabosti povzročijo bistveno pomanjkljivost ali pomembno slabost.«

1.1.5 Standard S13 (1205) Uporaba dela drugih strokovnjakov določa: »Revizor IS se mora odločiti, ali je delo drugih strokovnjakov ustrezno in popolno, da bo revizor IS lahko sprejel odločitve za zastavljene revizijske cilje. Take odločitve morajo biti jasno dokumentirane.«

1.2 Povezava s COBIT-om

1.2.1 PO1 *Opredelite strateški načrt za IT* izpolnjuje poslovno zahtevo za IT glede ohranjanja ali širjenja poslovne strategije in zahtev upravljanja, pri čemer morajo ostati koristi, stroški in tveganja pregledni, z usmerjanjem v vključevanje IT in poslovnega upravljanja pri preoblikovanju poslovnih zahtev v ponudbo storitev ter na razvoj strategij za izvajanje teh storitev na pregleden in uspešen način.

1.2.2 PO8 *Upravljajte kakovost* izpolnjuje poslovno zahtevo za IT glede zagotavljanja stalnega in merljivega izboljševanja kakovosti opravljanja storitev IT z usmerjanjem v opredelitev sistema vodenja kakovosti (QMS), stalno spremljanje delovanja glede na zastavljene cilje in izvajanje programa za stalno izboljševanje storitev IT.

1.2.3 AI6 *Upravljajte spremembe* izpolnjuje poslovno zahtevo za IT glede odzivanja na poslovne zahteve v skladu s poslovno strategijo, pri čemer se zmanjšujejo napake in ponovni popravki rešitev in storitev, z usmerjanjem v nadzor ocene vpliva, odobritev in uvajanje vseh sprememb v infrastrukturi IT, aplikacijah in tehničnih rešitvah, minimiziranjem napak zaradi nepopolnih specifikacij zahtevkov in zaustavitev vpeljevanja nepooblaščenih sprememb.

1.2.4 DS1 *Opredelite in upravljajte ravni storitev* izpolnjuje poslovno zahtevo za IT glede zagotavljanja uskladitve ključnih storitev IT s poslovno strategijo z usmerjanjem v prepoznavanje zahtev storitev, dogovor o ravni storitev in spremljanje doseganja ravni storitev.

1.2.5 ME2 *Spremljajte in vrednotite notranje kontrole* izpolnjuje poslovno zahtevo za IT glede varovanja uresničevanja ciljev IT in skladnosti z zakoni in predpisi, ki zadevajo IT, z usmerjanjem v spremljanje procesov notranje kontrole za aktivnosti, povezane z IT, ter določanje ukrepov za izboljševanje.

1.2.6 ME3 *Zagotovite skladnost z zunanjimi zahtevami* izpolnjuje poslovno zahtevo za IT glede skladnost z zakoni in predpisi z usmerjanjem v prepoznavanje vseh veljavnih zakonov in predpisov ter ustreznih ravni skladnosti IT in optimizacijo procesov IT za zmanjšanje tveganja neskladnosti.

1.2.7 Najpomembnejša informacijska sodila so:
- primarna: zanesljivost, razpoložljivost, uspešnost in celovitost,
- sekundarna: učinkovitost in zaupnost.

1.3 Potreba po smernici

1.3.1 Namen te smernice je opisati dokumentacijo, ki jo revizor IS pripravi in ohrani v podporo reviziji.

1.3.2 Ta smernica daje navodila za uporabo standardov revidiranja IS. Revizor IS jo mora upoštevati pri odločanju o tem, kako bo uporabljal standarde revidiranja IS, uporabljati jo mora po strokovni presoji in utemeljiti vsako odstopanje.

2. Načrtovanje in izvajanje

2.1 Vsebina dokumentacije

2.1.1 Revizijska dokumentacija za IS obsega zapis opravljenega revizijskega dela in revizijske dokaze, ki podpirajo izsledke, ugotovitve in priporočila revizorja IS. Revizijska dokumentacija mora biti popolna, jasna, strukturirana, opremljena s kazalom in taka, da jo pregledovalec brez težav uporablja in razume. Med drugim se dokumentacija lahko uporablja tudi za:
- prikaz, v kolikšnem obsegu je revizor IS ravnal v skladu s standardi revidiranja IS,
- prikaz izvajanja revizije za uresničitev zahtev iz revizijske listine,
- pomoč pri načrtovanju, izvajanju in pregledovanju revizij,
- pomoč pri pregledu s strani tretje stranke,
- ovrednotenje programa zagotavljanja kakovosti funkcije revidiranja IS,
- podporo v okoliščinah, kot so zavarovalni zahtevki, primeri goljufij, spori in tožbe,
- pomoč pri strokovnem razvoju osebja.

2.1.2 Dokumentacija naj vključuje vsaj:
- pregled prejšnje revizijske dokumentacije;

- načrtovanje in pripravo obsega in ciljev revizije: revizorji IS morajo dobro poznati panogo, poslovno področje, poslovni proces, izdelek, podporo dobaviteljev in celovito okolje, ki ga pregledujejo;
- zapisnike pregledovalnih sestankov s poslovodstvom, sestankov revizijske komisije in drugih z revizijo povezanih sestankov;
- revizijski program in revizijske postopke za uresničitev revizijskih ciljev;
- opravljene revizijske korake in zbrane revizijske dokaze za ovrednotenje prednosti in slabosti v delovanju kontrol;
- revizijske izsledke, ugotovitve in priporočila;
- vsa poročila, ki so bila izdana na podlagi revizijskega dela;
- nadzorni pregled.

2.1.3 Obseg dokumentacije revizorja IS je odvisen od potreb za določeno revizijo in mora med drugim vsebovati zadeve, kot so:

- revizorjevo razumevanje področij, ki jih je treba revidirati, in njihovega okolja;
- revizorjevo razumevanje sistemov za obdelavo informacij in notranjega kontrolnega okolja, kar vključuje:
  - kontrolno okolje,
  - kontrolne postopke,
  - tveganje pri odkrivanju,
  - tveganje pri kontroliranju,
  - uskladitev celotnega tveganja;
- avtor in vir revizijske dokumentacije in datum njenega dokončanja;
- metode, uporabljene za oceno ustreznosti kontrol, obstoj slabosti v delovanju kontrol ali pomanjkanje kontrol in ugotavljanje obstoja kompenzacijskih kontrol;
- revizijski dokazi, vir revizijske dokumentacije in datum njenega dokončanja, kar vključuje:
  - preizkuse skladnosti, ki temeljijo na politiki preizkušanja, postopkih in ločevanju nalog,
  - postopke preizkušanja podatkov, ki temeljijo na analitičnih postopkih, uskladitvi poročil podrobnih testov in drugih revizijskih postopkih preizkušanja podatkov;
- potrditev ustrezne osebe o prejemu revizijskega poročila in ugotovitev;
- odziv revidiranca na priporočila;
- kontrola različic, zlasti kadar je dokumentacija na elektronskih nosilcih podatkov.

2.1.4 Dokumentacija mora vključevati ustrezne informacije, ki jih zahtevajo zakon, državni predpisi ali veljavni strokovni standardi.

2.1.5 Dokumentacijo je treba predložiti revizijski komisiji v pregled in odobritev.

3. Dokumentacija

3.1 Varovanje, hramba in ponovna uporaba

3.1.1 Vzpostaviti je treba usmeritve in postopke za preverjanje in zagotavljanje ustreznega varovanja in hrambe dokumentacije, ki podpira revizijske izsledke in ugotovitve za dovolj dolgo časovno obdobje, da izpolni zakonske, strokovne in organizacijske zahteve.

3.1.2 Dokumentacija mora biti urejena, shranjena in zavarovana na način, ki je primeren za nosilce podatkov, na katerih se hrani; dovolj dolgo mora biti tudi na voljo za ponovno uporabo, da bo zadoščeno prej opredeljenim usmeritvam in postopkom.

4. Datum uveljavitve

4.1 Ta prenovljena smernica velja za vse revizije IS, ki se začnejo 1. septembra 1999 ali pozneje. Smernica je bila pregledana in posodobljena in velja od 1. marca 2008.

2204 Revizijska pomembnost (G6)

1. Izhodišča

1.1 Povezava s standardi

1.1.1 Standard S5 (1201) Načrtovanje določa: »Revizor IS mora načrtovati obseg revizije informacijskih sistemov tako, da upošteva cilje revizije in zagotovi skladnost z ustreznimi zakoni in strokovnimi revizijskimi standardi.«

1.1.2 Standard S10 Upravljanje IT (umaknjen) določa: »Revizor IS mora pregledati in oceniti skladnost z zakonskimi in okoljskimi zahtevami ter zahtevami glede kakovosti informacij, verodostojnosti in varovanja.«

1.1.3 Standard S12 (1204) Revizijska pomembnost določa: »Revizor IS mora upoštevati revizijsko pomembnost in njeno povezanost z revizijskim tveganjem, ko se odloča o vrsti, času in obsegu revizijskih postopkov. Pri načrtovanju revizije mora revizor IS upoštevati morebitne slabosti ali pomanjkanje kontrol in pretehtati, ali bi take slabosti ali pomanjkanje kontrol lahko imele za posledico tudi bistveno pomanjkljivost ali pomembno slabost v informacijskem sistemu. Revizor IS mora upoštevati tudi skupni učinek manjših pomanjkljivosti ali slabosti kontrole in pomanjkanje kontrol, ki se lahko preoblikujejo v bistveno pomanjkljivost ali pomembno slabost v informacijskem sistemu.«

1.1.4 Standard S9 (1207) Nepravilnosti in nezakonita dejanja določa: »Če je revizor IS ugotovil pomembno nepravilnost ali nezakonito dejanje, v katero so vpleteni poslovodstvo ali zaposleni, ki imajo pomembno vlogo pri notranjem kontroliranju, ali pridobil informacije, da utegne obstajati pomembna nepravilnost ali nezakonito dejanje, mora revizor IS o teh zadevah pravočasno obvestiti pristojne za upravljanje.«

1.2 Povezava s COBIT-om

1.2.1 PO5 *Upravljajte investicije IT* »izpolnjuje poslovno zahtevo za IT glede nenehnega in dokazljivega izboljševanja stroškovne učinkovitosti IT in njenega prispevka k dobičkonosnosti podjetja z integriranimi in standardiziranimi storitvami, ki izpolnjujejo pričakovanja končnih uporabnikov z usmerjanjem v uspešne in učinkovite odločitve glede investicij v IT in glede portfelja ter z določitvijo in spremljanjem proračunov IT, usklajenih s strategijo IT in odločitvami glede investicij.«

1.2.2 AI1 *Določite avtomatizirane rešitve* »izpolnjuje poslovno zahtevo za IT glede pretvorbe poslovnih funkcionalnih in kontrolnih zahtev v uspešno in učinkovito zasnovo avtomatiziranih rešitev z usmerjanjem na prepoznavanje tehnično izvedljivih in stroškovno učinkovitih rešitev.«

1.2.3 DS10 *Upravljajte probleme* »izpolnjuje poslovno zahtevo za IT glede zagotavljanja zadovoljstva končnih uporabnikov s ponudbo storitev in ravnmi storitev ter glede zmanjševanja napak in ponovnega dela pri rešitvah in opravljanju storitev z usmerjanjem na beleženje, sledenje in reševanje produkcijskih težav, s proučevanjem osnovnega vzroka vseh bistvenih težav in z določitvijo rešitev za ugotovljene težave pri delovanju.«

1.2.4 DS13 *Upravljajte delovanje* »izpolnjuje poslovno zahtevo za IT glede vzdrževanja celovitosti podatkov in zagotavljanja, da infrastruktura IT lahko vzdrži napake in okvare IT ter po njih okreva z usmerjanjem v doseganje ravni delovanja storitev za načrtovano obdelavo podatkov, pri čemer se zavarujejo občutljivi rezultati ter spremlja in vzdržuje infrastruktura.«

1.2.5 ME4 *Zagotovite upravljanje IT* »izpolnjuje poslovno zahtevo za IT glede združevanja upravljanja IT s cilji upravljanja podjetja, glede skladnosti z zakoni in predpisi z usmerjanjem v pripravo poročil za upravo o strategiji, delovanju in tveganjih IT ter glede odzivanja na zahteve upravljanja v skladu z usmeritvami uprave.«

1.2.6 Izbira najustreznejšega gradiva v COBIT-u, ki je primerno glede na predmet in obseg določene revizije, temelji na izbiri posebnih COBIT-ovih procesov IT in upoštevanju COBIT-ovih kontrolnih ciljev in z njimi povezanih praks upravljanja. Da revizor IS lahko izpolni načelo pomembnosti za revidiranje informacijskih sistemov, so procesi v COBIT-u, ki bodo najverjetneje ustrezni, izbrani in prilagojeni, razvrščeni na primarne in sekundarne, kot je prikazano v nadaljevanju. Proces in kontrolni cilji, ki bodo izbrani in prilagojeni, so lahko različni glede na določen predmet in obseg ter opis nalog in pristojnosti posla.

1.2.7 Sekundarni viri:

- PO8 *Upravljajte kakovost*,
- PO9 *Ocenjujte in obvladujte tveganja IT*,
- AI2 *Nabavite in vzdržujte aplikacijske programe*,
- AI3 *Nabavite in vzdržujte tehnološko infrastrukturo*,
- AI4 *Omogočite delovanje in uporabo*,
- AI5 *Zagotovite vire IT*,
- AI6 *Upravljajte spremembe*,
- DS3 *Upravljajte delovanje in zmogljivost*,
- DS5 *Zagotovite varnost sistemov*,
- DS9 *Upravljajte konfiguracijo*,
- ME1 *Spremljajte in vrednotite delovanje IT*,
- ME2 *Spremljajte in vrednotite notranje kontrole*.

1.2.8 Najpomembnejša informacijska sodila za revizijsko pomembnost so:

- primarna: zaupnost, celovitost, skladnost, zanesljivost,
- sekundarna: učinkovitost, uspešnost, razpoložljivost.

2. Potreba po smernici

2.1 Razlika med revizijo IS in finančno revizijo

2.1.1 Revizorji IS potrebujejo za merjenje pomembnosti drugačno merilo kot finančni revizorji. Finančni revizorji običajno merijo pomembnost, izraženo v denarni vrednosti, saj je tudi vse, kar revidirajo, merjeno in vključeno v poročila v denarni vrednosti.

Revizorji IS pa običajno revidirajo nefinančne zadeve, npr. fizične kontrole dostopa, logične kontrole dostopa, kontrole sprememb v programu in sisteme za upravljanje zaposlenih, nadzor nad proizvodnjo, oblikovanje, kontrolo kakovosti, ustvarjanje gesel, izdelavo kreditnih kartic in zdravstveno oskrbo. Zato utegnejo revizorji IS potrebovati navodila, kako naj ocenjujejo pomembnost, da bodo uspešno načrtovali svoje revizije, kako naj usmerijo svoje napore na področja z velikim tveganjem in kako naj ocenjujejo težo napak ali slabosti, ki jih odkrijejo.

2.1.2 Ta smernica daje navodila za uporabo standardov revidiranja IS o revizijski pomembnosti. Revizor IS naj jo upošteva pri odločanju o tem, kako bo uporabljal standarde revidiranja IS, uporablja naj jo po strokovni presoji in naj bo pripravljen utemeljiti vsako odstopanje.

3. Načrtovanje

3.1 Ocenjevanje pomembnosti

3.1.1 Ocena, kaj je pomembno, je stvar strokovne presoje in vključuje upoštevanje učinka in/ali morebitnega učinka na zmožnost organizacije, da uresniči svoje poslovne cilje pri napakah, opustitvah, nepravilnostih in nezakonitih dejanjih, do katerih bi lahko prišlo zaradi slabosti nadzora na posameznem področju.

3.1.2 Pri ocenjevanju pomembnosti naj revizor IS upošteva:

- skupno raven napake, ki je še sprejemljiva za poslovodstvo, revizorja IS, ustrezne regulativne agencije in druge zainteresirane,
- možnost, da skupni učinek majhnih napak ali slabosti postane pomemben.

3.1.3 Da doseže revizijske cilje, mora revizor IS prepoznati ustrezne kontrolne cilje in na podlagi ravni sprejemljivega tveganja določiti, kaj je treba pregledati. Za posamezen kontrolni cilj je pomembna posamezna kontrola ali skupina kontrol, brez katere kontrolni postopki ne dajo utemeljenega zagotovila, da bo kontrolni cilj dosežen.

3.1.4 Kadar se cilj revizije IS nanaša na sisteme ali postopke, s katerimi se obdelujejo finančne transakcije, je treba pri izvajanju revizije IS upoštevati merilo pomembnosti finančnega revizorja.

3.1.5 Revizor IS mora ugotoviti, kako so določene vloge in zadolžitve ter razvrščeni informacijski viri glede na zaupnost, razpoložljivost in celovitost; kakšna so pravila za kontrolo dostopa pri upravljanju pooblastil in kakšna je razvrstitev informacij glede na stopnjo kritičnosti in izpostavljenosti tveganju. Ocenjevanje naj med drugim zajema preverjanje:

- shranjenih informacij,
- strojne opreme IS,
- arhitekture in programske opreme IS,
- infrastrukture omrežja IS,
- delovanja IS,
- razvojnega in testnega okolja.

3.1.6 Revizor IS mora ugotoviti, ali bi katera od splošnih pomanjkljivosti IT morda lahko postala pomembna. Pomembnost takih pomanjkljivih splošnih kontrol IT je treba ovrednotiti glede na njihov učinek na aplikativne kontrole in ugotoviti, ali so neučinkovite tudi z njimi povezane aplikativne kontrole. Če je razlog za aplikativno pomanjkljivost v splošni kontroli IT, potem je ta pomembna. Če je na primer izračun davka, ki ga izvaja aplikacija, pomembno napačen in je razlog za to v nezadostnih kontrolah upravljanja sprememb tabel davčnih stopenj, potem sta kontrola (izračun), ki temelji na aplikaciji, in splošna kontrola (upravljanje sprememb) pomembno šibki.

3.1.7 Revizor IS mora ovrednotiti pomanjkljivost splošne kontrole IT v zvezi z njenim učinkom na aplikativne kontrole in vse skupaj oceniti glede na druge pomanjkljivosti kontrol. Odločitev poslovodstva, da ne popravi pomanjkljivosti splošne kontrole in njenega s tem povezanega vpliva na kontrolno okolje, bi na primer lahko postala pomembna, če bi skupaj z drugimi pomanjkljivostmi kontrol vplivala na kontrolno okolje.

3.1.8 Revizor IS se mora tudi zavedati, da neuspešna odprava pomanjkljivosti lahko postane pomembna.

3.1.9 Revizor IS mora proučiti možnosti za pridobitev odobritve ustreznih zainteresiranih, s katero potrdijo, da so razkrili pomembne obstoječe slabosti v organizaciji, za katere vedo.

3.1.10 V nadaljevanju so primeri meril, ki jih je treba upoštevati pri ocenjevanju pomembnosti:

- kritičnost poslovnih procesov, podprtih s sistemom ali postopki,
- kritičnost informacijskih podatkovnih baz, podprtih s sistemom ali postopki,
- število in vrsta razvitih aplikacij,
- število uporabnikov informacijskih sistemov,
- število vodij in direktorjev, ki delajo z informacijskimi sistemi, razvrščenih po pooblastilih,
- kritičnost omrežnih komunikacij, podprtih s sistemom ali postopki,
- stroški sistema ali postopkov (strojna oprema, programska oprema, osebje, storitve tretjih strank, režijski stroški ali kombinacija teh),
- morebitni stroški napak (mogoče v smislu izgubljene prodaje, reklamacij v garancijskem roku, nepovračljivih razvojnih stroškov, stroški potrebnih objav opozoril, stroški popravkov, stroški za zdravje in varstvo, nepotrebno visoki stroški proizvodnje, veliko izgub itd.),
- stroški izgube kritičnih in pomembnih informacij v smislu denarja in časa za njihovo ponovno pridobitev,
- učinkovitost protiukrepov,
- število dostopov/transakcij/poizvedb, obdelanih v obdobju,
- vrsta, čas in obseg priprave poročil in vzdrževanja datotek,
- vrsta in količina obdelanih materialov (npr. kadar se premiki zalog evidentirajo brez vrednosti),
- zahteve sporazuma o ravni storitev in stroški morebitnih pogodbenih kazni,
- kazni za nespoštovanje zakonskih, drugih predpisanih in pogodbenih zahtev,
- kazni za nespoštovanje zahtev javnega zdravja in varstva.

3.1.11 Poleg tega, da škodujejo ugledu podjetja, lahko napake v kontroli povzročijo denarne izgube, slabšo konkurenčnost ter izgubo zaupanja ali dobrega imena. Revizor IS mora ovrednotiti tveganja v primerjavi z možnimi protiukrepi.

4. Poročanje

4.1 Opredelitev zadev, o katerih je treba poročati

4.1.1 Pri določanju ugotovitev, sklepov in priporočil, o katerih je treba poročati, mora revizor IS upoštevati tako pomembnost vsake ugotovljene napake kot tudi morebitno pomembnost napak, do katerih bi lahko prišlo zaradi slabosti v delovanju kontrol.

4.1.2 Kadar poslovodstvo uporabi revizijo za to, da pridobi izjavo o zanesljivosti kontrol IS, pomeni mnenje o ustreznosti kontrol brez pridržka, da so vzpostavljene kontrole v skladu s splošno sprejetimi kontrolnimi praksami za doseganje kontrolnih ciljev brez kakršnih koli pomembnih slabosti v delovanju kontrol.

4.1.3 Šteje se, da je slabost v delovanju kontrol pomembna in je zato o njej treba poročati, če zaradi nekontrole ni mogoče utemeljeno zagotoviti, da bo kontrolni cilj dosežen. Če se z revizijskim delom ugotovijo pomembne slabosti v delovanju kontrol, mora revizor IS razmisliti o izdaji mnenja s pridržki ali odklonilnega mnenja o revizijskem cilju.

4.1.4 Glede na cilje revizije naj revizor IS razmisli tudi o tem, da poslovodstvu poroča o slabostih, ki niso pomembne, zlasti kadar so stroški za okrepitev kontrol nizki.

5. Datum uveljavitve

5.1 Ta smernica velja za vse revizije IS, ki se začnejo 1. septembra 1999 ali pozneje. Smernica je bila pregledana in posodobljena in velja od 1. maja 2008**.**

2205 Revizijski dokazi (G2)

1. Izhodišča

1.1 Povezava s standardi

1.1.1 Standard S6 (1203) Izvajanje revizijskih del določa: »Med potekom revizije mora revizor IS pridobiti zadostne, zanesljive in ustrezne revizijske dokaze, da se dosežejo revizijski cilji. Revizijski izsledki in ugotovitve morajo biti podprti z ustrezno analizo in razlago teh dokazov.«

1.1.2 Standard S9 (1207) Nepravilnosti in nezakonita dejanja določa: »Revizor IS mora pridobiti zadostne in ustrezne revizijske dokaze, da ugotovi, ali poslovodstvo ali drugi v organizaciji vedo za ali sumijo na kakršne koli dejanske ali domnevne nepravilnosti in nezakonita dejanja.«

1.1.3 Standard S13 (1205) Uporaba dela drugih strokovnjakov določa: »Revizor IS mora dati ustrezno revizijsko mnenje in vanj vključiti omejitve glede področja dela, kjer zahtevanih dokazov ni pridobil z dodatnimi preizkusnimi postopki.«

1.1.4 Standard S14 (1206) Revizijski dokazi določa: »Revizor IS mora pridobiti zadostne in ustrezne revizijske dokaze, da lahko sprejme razumne sklepe, s katerimi utemelji izide revizije. Revizor IS mora ovrednotiti zadostnost revizijskih dokazov, pridobljenih med revizijo.«

1.1.5 Postopek P7 Nepravilnosti in nezakonita dejanja (umaknjena) navaja: »Čeprav revizor IS ni izrecno odgovoren za odkrivanje ali preprečevanje nepravilnosti, naj revizor IS oceni raven tveganja, da bi se nepravilnosti lahko pojavile. Izid ocenjevanja tveganja in drugih postopkov, izvedenih ob načrtovanju, je treba uporabiti za določitev narave, obsega in časa izvajanja revizijskih postopkov, ki se opravijo med izvajanjem posla.«

1.2 Povezava s COBIT-om

1.2.1 ME 2.3 *Izjeme pri kontrolah* navaja: »Zapisujte informacije o vseh izjemah pri kontrolah in zagotovite, da bo to vodilo v analizo osnovnega vzroka zanje in v popravne ukrepe. Poslovodstvo se mora odločiti, katero izjemo je treba sporočiti posamezniku, ki je odgovoren za to nalogo, in katere izjeme je treba stopnjevati. Poslovodstvo je odgovorno tudi, da o tem obvesti prizadete strani.«

1.3 Potreba po smernici

1.3.1 Namen te smernice je usmeriti revizorja IS, da pridobi zadostne in ustrezne revizijske dokaze in sprejme razumne sklepe, s katerimi utemelji izide revizije.

1.3.2 Ta smernica daje navodila za uporabo standardov revidiranja IS. Revizor IS naj jo upošteva pri odločanju o tem, kako bo uporabljal standarde revidiranja IS, uporablja naj jo po strokovni presoji in naj bo pripravljen utemeljiti vsako odstopanje.

2. Načrtovanje

2.1 Vrste revizijskih dokazov

2.1.1 Opis ustreznih, zanesljivih in zadostnih dokazov je naveden v komentarju standarda S14 (1206).

2.1.2 Pri načrtovanju revizijskega dela naj revizor IS upošteva vrsto revizijskih dokazov, ki jih je treba zbrati, njihovo uporabo za uresničitev revizijskih ciljev in njihove različne stopnje zanesljivosti. Med načeli, ki jih je treba upoštevati, sta neodvisnost in strokovna usposobljenost predlagatelja revizijskih dokazov. Potrditveni revizijski dokazi neodvisne tretje stranke so lahko zanesljivejši od revizijskih dokazov pregledovane organizacije. Fizični revizijski dokazi so na splošno zanesljivejši od navedb posameznika.

2.1.3 Revizor IS naj tudi prouči, ali je preizkušanje kontrol opravila in potrdila neodvisna tretja stranka in ali se je na to preizkušanje mogoče zanesti.

2.1.4 Različne vrste revizijskih dokazov, za katere naj možnost uporabe prouči revizor IS, so med drugim:
- opazovani postopki in obstoj fizičnih predmetov,
- dokumentarni revizijski dokazi,
- navedbe,
- analiza.

2.1.5 Opazovani postopki in obstoj fizičnih predmetov lahko vključujejo opazovanja dejavnosti, premoženja in funkcij IS, kot so:
- zaloga nosilcev podatkov v dislociranem skladišču,
- delujoči varnostni sistem v računalniškem prostoru.

2.1.6 Dokumentarni revizijski dokazi, zapisani na papirju ali drugih nosilcih, lahko vključujejo:
- izide izvlečkov podatkov,
- zapise transakcij,
- izpise izvorne kode,
- račune,
- dnevnike dejavnosti in kontrol,
- dokumentacijo o razvoju sistema.

2.1.7 Revizijski dokazi so lahko tudi navedbe revidirancev, kot so:
- pisne usmeritve in postopki,
- diagrami poteka sistema,
- pisne ali ustne izjave.

2.1.8 Tudi izide analiz informacij s primerjavami, simulacijami, izračuni in sklepanji je mogoče uporabiti kot revizijske dokaze. Tako na primer:
- primerjavo delovanja IS z drugimi organizacijami ali preteklimi obdobji,
- primerjavo pogostosti napak med aplikacijami, transakcijami in uporabniki.

2.2 Razpoložljivost revizijskih dokazov

2.2.1 Pri določanju vrste, časa in obsega postopkov preizkušanja podatkov ter preizkušanja njihove skladnosti, če je to primerno, naj revizor IS upošteva čas, v katerem informacije obstajajo ali so na voljo. Revizijski dokazi, obdelani z elektronsko izmenjavo podatkov

(EDI), elektronsko obdelavo slik dokumentov (DIP) in dinamičnimi sistemi, kot so preglednice, na primer po določenem času lahko niso več obnovljivi, če spremembe v datotekah niso nadzorovane ali nimajo varnostnih kopij. Razpoložljivost dokumentacije bi bila lahko odvisna tudi od usmeritev podjetja glede hrambe dokumentacije.

2.3 Izbira revizijskih dokazov

2.3.1 Revizor IS naj načrtuje uporabo najustreznejših, zanesljivih in zadostnih revizijskih dokazov, ki jih je mogoče pridobiti in so skladni s pomembnostjo cilja revizije ter časa in napora, potrebnega za pridobitev revizijskih dokazov.

2.3.2 Če je revizijski dokaz, pridobljen v obliki ustne navedbe, ključen za revizijsko mnenje ali sklep, naj revizor IS prouči možnost za pridobitev dokumentarne potrditve take navedbe na papirju ali drugem nosilcu. Revizor naj prouči tudi druge možne dokaze za potrditev takih navedb, da zagotovi njihovo zanesljivost.

3. Izvajanje revizijskega dela

3.1 Narava revizijskih dokazov

3.1.1 Revizijski dokazi naj bodo zadostni, zanesljivi, ustrezni in uporabni za oblikovanje mnenja ali podporo ugotovitev in sklepov revizorja IS. Če po presoji revizorja IS pridobljeni revizijski dokazi ne izpolnjujejo teh meril, naj revizor IS pridobi dodatne revizijske dokaze. Izpis izvorne kode, na primer, morda ni ustrezen revizijski dokaz, dokler se z drugimi zbranimi revizijskimi dokazi ne preveri in potrdi, da res predstavlja dejanski program, ki se uporablja v produkcijskem okolju.

3.2 Zbiranje revizijskih dokazov

3.2.1 Postopki za zbiranje revizijskih dokazov so različni glede na informacijski sistem, ki se pregleduje. Revizor IS naj izbere najustreznejši, zanesljiv in zadosten postopek za uresničitev revizijskega cilja. Upoštevati je treba naslednje postopke:

- poizvedovanje,
- opazovanje,
- preiskovanje,
- potrjevanje,
- ponovno izvajanje,
- spremljanje.

3.2.2 Vse navedeno je mogoče izvajati z uporabo ročnih revizijskih postopkov, računalniško podprtih tehnik revidiranja ali kombinacijo obojih. Na primer:

- Sistem, ki uporablja ročne kontrolne seštevke za uskladitev operacij vnosa podatkov je lahko revizijski dokaz, da obstaja kontrolni postopek na podlagi ustrezno usklajenega in obrazloženega poročila. Revizor IS naj pridobi revizijske dokaze s pregledovanjem in preizkušanjem tega poročila.
- Podrobni izpisi transakcij so lahko na voljo samo v strojno berljivi obliki, kar zahteva od revizorja IS, da pridobi revizijske dokaze z uporabo računalniško podprtih tehnik revidiranja. Revizor mora zagotoviti, da je različica ali vrsta računalniško podprte tehnike revidiranja (CAAT), ki jo bo uporabil, posodobljena in/ali popolnoma združljiva z obliko zapisa pregledovanega podrobnega zapisa transakcij.

3.2.3 Če obstaja možnost, da bodo zbrani dokazi postali del pravnega postopka, naj se revizor IS posvetuje z ustreznim pravnim svetovalcem, da ugotovi, ali obstajajo kakšne zahteve, ki bodo vplivale na način zbiranja, predstavitve in razkritja dokazov.

3.3 Revizijska dokumentacija

3.3.1 Revizijske dokaze, ki jih zbere revizor IS, je treba ustrezno dokumentirati in organizirati, da podpirajo ugotovitve in sklepe revizorja IS.

3.3.2 Zaščita in hramba dokazov sta opisani v komentarju standarda S14 (1206).

4. Poročanje

4.1 Omejitev področja dela

4.1.1 Kadar revizor IS meni, da ni mogoče pridobiti zadostnih revizijskih dokazov, naj revizor IS to dejstvo razkrije na način, ki je skladen z obveščanjem o izidih revizije.

5. Datum uveljavitve

5.1 Ta smernica velja za vse revizije informacijskih sistemov, ki se začnejo 1. decembra 1998 ali pozneje. Smernica je bila pregledana in posodobljena in velja od 1. maja 2008**.**

2206 Uporaba dela drugih strokovnjakov (G1)

1. Izhodišča

1.1 Povezava s standardi

1.1.1 Standard S13 (1205) Uporaba dela drugih strokovnjakov določa: »Revizor IS mora, kjer je to primerno, proučiti možnost uporabe dela drugih strokovnjakov za revizijo.«

1.1.2 Standard S6 (1203) Izvajanje revizijskih del pa določa: »Med potekom revizije mora revizor IS pridobiti zadostne, zanesljive in ustrezne dokaze, da se dosežejo revizijski cilji. Revizijski izsledki in ugotovitve morajo biti podprti z ustrezno analizo in razlago teh dokazov.«

1.2 Povezava s CobiT-om

1.2.1 ME 2.5 navaja, naj revizor IS »po potrebi pridobi nadaljnje zagotovilo o popolnosti in uspešnosti notranjih kontrol z neodvisnimi zunanjimi pregledi.« Take preglede lahko opravijo na zahtevo poslovodstva tisti, ki v podjetju skrbijo za skladnost poslovanja s predpisi, ali notranja revizija ali pa jih po naročilu izvedejo zunanji revizorji in svetovalci ali certifikacijski organi. Zagotoviti je treba, da imajo posamezniki, ki izvajajo revizije, dokazilo o ustrezni strokovni usposobljenosti, npr. naziv CISA®.

1.3 Potreba po smernici

1.3.1 Zaradi medsebojne povezanosti obdelave podatkov pri strankah in dobaviteljih ter oddajanja neključnih dejavnosti v izvajanje drugim organizacijam bo (notranji ali zunanji) revizor IS pogosto ugotovil, da dele okolja, ki ga pregleduje, nadzorujejo in pregledujejo tudi druge neodvisne službe ali organizacije. Ta smernica določa, kako naj revizor IS v takih okoliščinah ravna v skladu z navedenim standardom. Skladnost s to smernico ni obvezna, toda revizor IS naj bo pripravljen utemeljiti svoja odstopanja od nje.

1.3.2 Revizorji IS naj pri reviziji upoštevajo možnost uporabe dela drugih strokovnjakov, kadar bi omejitve lahko oslabile revizijsko delo, ki ga je treba opraviti, ali obstajajo morebitne koristi za kakovost revizije. Taki primeri so znanje, potrebno zaradi strokovne narave nalog, ki jih je treba opraviti, skromni razpoložljivi viri za izvedbo revizije in omejeno poznavanje posebnih področij revizije. 'Strokovnjak' bi bil lahko revizor IS iz zunanje revizijske družbe, svetovalec poslovodstvu, strokovnjak za IT ali strokovnjak na revizijskem področju, ki ga je imenovalo najvišje vodstvo ali skupina za revizijo IS. Strokovnjak lahko prihaja iz organizacije ali od zunaj, pomembno je le, da sta zagotovljeni njegova neodvisnost in nepristranskost.

2. Revizijska listina

2.1 Pravice dostopa do dela drugih strokovnjakov

2.1.1 Kadar uporaba dela drugih strokovnjakov ustreza ciljem revizije IS, naj revizor IS preveri, da je v revizijski listini ali listini o poslu posebej določena pravica dostopa revizorja IS do tega dela.

3. Načrtovanje

3.1 Premisleki pri načrtovanju

3.1.1 Kadar revizor IS nima potrebnih veščin ali drugih sposobnosti za opravljanje revizije, mora poiskati strokovno pomoč drugih strokovnjakov; revizor IS mora vsekakor dobro poznati opravljeno delo, vendar se od njega ne pričakuje, da je njegovo znanje na enaki ravni kot znanje strokovnjakov.

3.1.2 Kadar je v revizijo IS vključena uporaba dela drugih strokovnjakov, revizor IS že med načrtovanjem revizijskega dela prouči njihove dejavnosti in učinke teh dejavnosti na cilje revizije IS. V postopek načrtovanja je treba vključiti:

- ocenjevanje neodvisnosti in nepristranskosti drugih strokovnjakov,
- ocenjevanje njihove strokovne usposobljenosti in kvalifikacij,
- seznanjanje z njihovim obsegom dela, pristopom, časovnim razporedom dela in postopki kontrole kakovosti, vključno z oceno, ali so skrbno opravili delo in pripravili delovno gradivo ter poskrbeli za hrambo dokazov svojega dela,
- določitev ravni zahtevanega pregleda.

3.2 Neodvisnost in nepristranskost

3.2.1 Postopki izbiranja in imenovanja, organizacijski status, linija poročanja in učinek danih priporočil na prakse upravljanja so kazalniki neodvisnosti in nepristranskosti drugih strokovnjakov.

3.3 Strokovna usposobljenost

3.3.1 Pri ocenjevanju strokovne usposobljenosti je treba upoštevati kvalifikacije, izkušnje, vire in predložena priporočila drugih strokovnjakov.

3.4 Predmet in obseg dela in pristop

3.4.1 Predmet in obseg dela in pristop bosta praviloma opredeljena v pisni revizijski listini, opisu nalog in pristojnosti ali listini o poslu drugega strokovnjaka.

3.5 Zahtevana raven pregleda

3.5.1 Narava, čas in obseg zahtevanih revizijskih dokazov bodo odvisni od pomembnosti ter predmeta in obsega dela drugega strokovnjaka. Že pri načrtovanju mora revizor IS opredeliti raven pregleda, ki je potrebna za zagotovitev zadostnih zanesljivih, ustreznih in uporabnih revizijskih dokazov, da se uspešno dosežejo celoviti cilji revizije IS. Revizor IS mora pregledati končno poročilo, revizijski program in revizijsko delovno gradivo drugega strokovnjaka. Revizor IS naj tudi pretehta, ali je potrebno dodatno preverjanje dela drugega strokovnjaka.

4. Izvajanje revizijskega dela

4.1 Pregled delovnega gradiva drugega strokovnjaka

4.1.1 Revizor IS mora imeti dostop do vsega delovnega gradiva, ki ga je pripravil strokovnjak, ter do dokazne dokumentacije in poročil drugih strokovnjakov, če tak dostop ne povzroča pravnih vprašanj.

4.1.2 Kadar pa dostop do strokovnjakovih zapisov ustvarja pravna vprašanja in torej takega dostopa ni na voljo, naj revizor IS ustrezno določi in sklene, v kolikšnem obsegu bo uporabil strokovnjakovo delo in se nanj zanesel.

4.1.3 Pri pregledovanju delovnega gradiva drugega strokovnjaka naj revizor IS opravi dovolj revizijskega dela, da lahko potrdi, da je bilo delo drugega strokovnjaka ustrezno načrtovano, nadzorovano, dokumentirano in pregledano, da določi ustreznost in zadostnost s tem pridobljenih revizijskih dokazov in se odloči, v kolikšni meri bo uporabil in se zanesel na strokovnjakovo delo. Oceniti je treba tudi skladnost z ustreznimi strokovnimi standardi. Revizor IS naj oceni, ali je delo drugih strokovnjakov primerno in dovolj popolno, da revizor IS lahko pride do ustreznega sklepa glede na zastavljene cilje revizije in tak sklep tudi dokumentira.

4.1.4 Na podlagi ocene dela in delovnega gradiva drugih strokovnjakov naj revizor IS uporabi dodatne preizkusne postopke za pridobitev zadostnih in ustreznih revizijskih dokazov, kadar uporaba dela drugih strokovnjakov ne zagotavlja zadostnih in ustreznih revizijskih dokazov.

4.1.5 Če tudi opravljeni dodatni preizkusni postopki ne zagotovijo zadostnih in ustreznih revizijskih dokazov, mora revizor IS izdati ustrezen revizijski sklep in po potrebi vključiti omejitev predmeta in obsega.

4.2 Pregled poročil(a) drugega strokovnjaka

4.2.1 Revizor IS naj opraviti zadostne preglede končnega poročila in/ali končnih poročil drugega strokovnjaka, da lahko potrdi, da je bil opravljen obseg dela, kot je določen v revizijski listini, opisu nalog in pristojnosti ali listini o poslu, da so upoštevane vse bistvene predpostavke, ki so jih uporabili drugi strokovnjaki, in da je poslovodstvo soglašalo z ugotovitvami in sklepi, ki so vključeni v poročilo.

4.2.2 Morda je primerno, da tudi poslovodstvo predloži svoje poročilo o revidiranih enotah in s tem potrdi, da je prvo odgovorno za sisteme notranje kontrole. V takem primeru naj revizor IS poročili poslovodstva in strokovnjaka prouči skupaj.

4.2.3 Revizor IS naj oceni uporabnost in ustreznost poročil, ki so jih izdali drugi strokovnjaki, in upošteva vse bistvene izsledke, o katerih so poročali drugi strokovnjaki. Odgovornost revizorja IS je, da oceni učinek izsledkov in ugotovitev drugega strokovnjaka na celotni revizijski cilj ter da preveri in potrdi, da je opravljeno vse dodatno delo, ki je potrebno za uresničitev celotnega revizijskega cilja.

4.2.4 Na poročilo strokovnjaka se je mogoče zanesti tudi, če je strokovnjaka najel drug del organizacije. V nekaterih primerih je zato potreben manjši obseg področij IS, ki jih je treba pregledati pri reviziji, čeprav revizor IS nima dostopa do dokazne dokumentacije in delovnega gradiva. Pri dajanju mnenja za take primere naj bi bil revizor IS previden.

4.2.5 Če je revizor IS za oblikovanje svojega mnenja uporabil poročilo drugega strokovnjaka, naj bodo sestavni del poročila revizorja IS tudi njegova mnenja/pripombe o sprejemljivosti in pomembnosti strokovnjakovega poročila.

5. Nadaljnja obravnava

5.1 Izvajanje priporočil

5.1.1 Kadar je to primerno, naj revizor IS prouči, v kolikšnem obsegu je poslovodstvo izvajalo priporočila drugih strokovnjakov. Pri tem naj tudi oceni, ali se je poslovodstvo zavezalo v ustreznih rokih popraviti pomanjkljivosti zadeve, ki so jih odkrili drugi strokovnjaki, in kakšno je sedanje stanje teh zadev.

6. Datum uveljavitve

6.1 Ta smernica velja za vse Revizije IS, ki se začnejo 1. junija 1998 ali pozneje. Smernica je bila pregledana in posodobljena in velja od 1. marca 2008**.**

2207 Nepravilnosti in nezakonita dejanja (G9)

1. Izhodišča

1.1 Povezava s standardi

1.1.1 Standard S3 (1005) Poklicna etika in standardi določa: »Revizor IS mora zagotavljati potrebno poklicno skrbnost, vključno z upoštevanjem ustreznih strokovnih revizijskih standardov.«

1.1.2 Standard S5 (1201) Načrtovanje določa: »Revizor IS mora načrtovati obseg revizije informacijskih sistemov, tako da upošteva cilje revizije in zagotovi skladnost z ustreznimi zakoni in strokovnimi revizijskimi standardi.«

1.1.3 Standard S6 (1203) Izvajanje revizijskih del določa: »Med potekom revizije mora revizor IS pridobiti zadostne, zanesljive in ustrezne dokaze, da se dosežejo revizijski cilji. Revizijski izsledki in ugotovitve morajo biti podprti z ustrezno analizo in razlago teh dokazov.«

1.1.4 Standard S7 (1401) Poročanje določa: »Revizor IS mora po končani reviziji pripraviti poročilo v primerni obliki. Revizijsko poročilo mora vključevati področje, cilje, obravnavano obdobje in vrsto, čas in trajanje opravljenega revizijskega dela. Poročilo mora vsebovati izsledke, ugotovitve in priporočila ter vse morebitne pridržke, omejitve ali omejitve področja dela, ki jih ima revizor IS v zvezi z revizijo.«

1.1.5 Standard S9 (1207) Nepravilnosti in nezakonita dejanja obravnava zahteve in premisleke revizorjev IS glede nepravilnosti in nezakonitih dejanj.

1.2 Povezava s COBIT-om

1.2.1 Izbira najustreznejšega gradiva v COBIT-u, ki je primerno glede na predmet in obseg določene revizije, temelji na izbiri posameznih COBIT-ovih procesov IT in upoštevanju COBIT-ovih kontrolnih ciljev ter z njimi povezanih praks upravljanja. Da bi revizorji IS lahko obravnavali in presojali nepravilnosti in nezakonita dejanja, so procesi v COBIT-u, ki bodo za to najverjetneje ustrezni, izbrani in prilagojeni, razvrščeni v primarne in sekundarne. Postopki in kontrolni cilji, ki jih je treba izbrati in prilagoditi, se lahko razlikujejo glede na posamezen predmet in obseg ter opis nalog in pristojnosti posla.

1.2.2 Primarni procesi v COBIT-u so:

- PO5 *Upravljajte investicije IT*,
- PO7 *Upravljajte človeške vire v sektorju IT*,
- PO9 *Ocenjujte in obvladujte tveganja IT*,
- PO10 *Upravljajte projekte*,
- AI1 *Določite avtomatizirane rešitve*,
- AI5 *Zagotovite vire IT*,
- ME2 *Spremljajte in vrednotite notranje kontrole*,
- ME3 *Zagotovite skladnost z zunanjimi zahtevami*,
- ME4 *Zagotovite upravljanje IT*.

1.2.3 Sekundarni procesi v COBIT-u so:

- PO3 *Določite tehnološko usmeritev*,
- PO4 *Opredelite procese, organizacijo in razmerja IT*,
- PO8 *Upravljajte kakovost*,
- DS7 *Izobrazite in usposobite uporabnike*,
- DS10 *Upravljajte probleme*,
- ME1 *Spremljajte in vrednotite delovanje IT*.

1.2.4 Najustreznejša COBIT-ova informacijska sodila so:

- primarna: skladnost, zaupnost, celovitost in razpoložljivost,
- sekundarna: zanesljivost, uspešnost in učinkovitost.

1.3 Potreba po smernici

1.3.1 Namen te smernice je dati revizorjem IS navodila za obravnavanje nepravilnih ali nezakonitih dejavnosti, na katere utegnejo naleteti med izvajanjem revizijskih poslov.

1.3.2 Standard S9 (1207) Nepravilnosti in nezakonita dejanja obravnava zahteve in premisleke revizorjev IS glede nepravilnosti in nezakonitih dejanj. Ta smernica daje navodila za uporabo standardov revidiranja IS. Revizor IS naj jo upošteva pri odločanju o tem, kako bo uporabljal standarde revidiranja IS, uporablja naj jo po strokovni presoji in naj bo pripravljen utemeljiti vsako odstopanje.

2. Opredelitev pojmov

2.1 Negoljufive nepravilne dejavnosti

2.1.1 Vseh nepravilnosti ne bi smeli obravnavati kot goljufive dejavnosti. Določitev goljufivih dejavnosti je odvisna od zakonske opredelitve goljufije v državi, kjer se izvaja revizija. Nepravilnosti vključujejo, vendar niso omejene le na namerno izogibanje kontrolam, da se prikrivajo ponavljajoče se goljufije, nepooblaščena uporaba sredstev ali storitev, in napeljevanje na tovrstne dejavnosti ali pomoč pri njihovem prikrivanju. Negoljufive nepravilnosti pa so med drugim lahko:

- namerne kršitve sprejete politike upravljanja,
- namerne kršitve predpisov,
- namerno napačne navedbe ali opustitve informacij, ki se nanašajo na revidirano področje ali organizacijo kot celoto,
- huda malomarnost,
- nenamerna nezakonita dejanja.

2.2 Nepravilnosti in nezakonita dejanja

2.2.1 Nepravilnosti in nezakonita dejanja lahko vključujejo dejavnosti, vendar niso omejena le na te dejavnosti, kot so:

- goljufija, to je vsako dejanje, ki vključuje zavajanje za pridobitev nezakonite prednosti,

- dejanja, ki vključujejo neskladnost z zakoni in predpisi, vključno z neizpolnjevanjem veljavnih zakonov in predpisov sistemov IT,
- dejanja, ki vključujejo neskladnost s sporazumi in pogodbami organizacije s tretjimi strankami, kot so banke, dobavitelji, prodajalci, izvajalci storitev in drugi zainteresirani,
- spreminjanje, ponarejanje ali prenarejanje zapisov ali dokumentov (v elektronski obliki ali na papirju),
- zmanjšanje ali opustitev učinkov transakcij iz zapisov ali dokumentov (v elektronski obliki ali na papirju),
- neustrezno ali namerno dopuščanje uhajanja zaupnih informacij,
- evidentiranje transakcij finančnih ali drugih zapisov (v elektronski obliki ali na papirju), ki nimajo podlage in se zanje ve, da so napačni,
- nezakonita prisvojitev in zloraba sredstev IS in drugih sredstev,
- namerna ali nenamerna dejanja, ki kršijo pravice intelektualne lastnine, kot so avtorske pravice, blagovne znamke ali patenti,
- dovolitev nepooblaščenega dostopa do informacij in sistemov,
- napake v finančnih ali drugih zapisih, ki so posledica nepooblaščenega dostopa do podatkov in sistemov.

2.2.2 Ugotovitev, da je določeno dejanje nezakonito, naj na splošno temelji na nasvetu dobro obveščenega strokovnjaka, ki ima pravno izobrazbo, ali pa je treba počakati na končno odločitev sodišča. Revizor IS naj obravnava predvsem učinek ali morebitni učinek nepravilnega ravnanja, ne glede na to, ali gre za sum ali dokaz nezakonitega dejanja.

3. Odgovornosti

3.1 Odgovornosti poslovodstva

3.1.1 Predvsem poslovodstvo je odgovorno za to, da prepreči in odkrije nepravilnosti in nezakonita dejanja.

3.1.2 Za pridobitev sprejemljivih zagotovil, da so nepravilnosti in nezakonita dejanja preprečena ali pravočasno odkrita, poslovodstvo praviloma uporablja naslednja sredstva:

- oblikovanje, uvajanje in vzdrževanje sistemov notranjih kontrol, da prepreči in odkrije nepravilnosti ali nezakonita dejanja. Notranje kontrole vključujejo pregled transakcij in postopke odobritve ter vodstvene preglede;
- usmeritve in postopke za vodenje ravnanja zaposlenih;
- postopke za potrjevanje in spremljanje skladnosti;
- oblikovanje, uvajanje in vzdrževanje primernih sistemov za poročanje, beleženje in upravljanje incidentov v zvezi z nepravilnostmi ali nezakonitimi dejanji.

3.1.3 Poslovodstvo mora revizorju IS razkriti vse, kar ve o kakršnih koli domnevnih, slutenih ali dokazanih nepravilnostih ali nezakonitih dejanjih na prizadetih področjih in o ukrepih poslovodstva, če so bili izvedeni.

3.1.4 Kadar koli gre za domnevno, sluteno ali odkrito nepravilno ali nezakonito dejanje ali ravnanje, mora poslovodstvo pomagati pri preiskovanju in poizvedovanju.

3.2 Odgovornosti revizorjev IS

3.2.1 Revizor IS mora proučiti, ali bo v revizijski listini ali listini o poslu opredelil odgovornosti poslovodstva in revizije v zvezi s preprečevanjem in odkrivanjem nepravilnosti ter poročanjem o njih, tako da bodo te jasno razumljene za vse revizijsko delo. Kadar so te odgovornosti že dokumentirane v usmeritvah organizacije ali podobnem dokumentu, naj revizijska listina vključuje izjavo o tem.

3.2.2 Revizor IS mora razumeti, da mehanizmi nadzora ne izločijo vseh možnosti pojavljanja nepravilnosti ali nezakonitih dejanj. Revizor IS je odgovoren za ocenitev tveganja pojavov nepravilnosti ali nezakonitih dejanj, ovrednotenje vpliva ugotovljenih nepravilnosti ter zasnovo in izvedbo preizkusov, ki so primerni glede na naravo revizijskega posla. Utemeljeno je pričakovati, da bo revizor IS odkril:

- nepravilnosti ali nezakonita dejanja, ki bi lahko imela pomemben učinek na revidirano področje ali organizacijo kot celoto,
- slabosti v notranjih kontrolah, zaradi katerih pomembne nepravilnosti ali nezakonita dejanja ne bi bila preprečena ali odkrita.

3.2.3 Revizor IS ni strokovno odgovoren za preprečevanje ali odkrivanje nepravilnosti ali nezakonitih dejanj. Revizija ne more jamčiti, da bodo nepravilnosti odkrite. Tudi če je revizija ustrezno načrtovana in izvedena, nepravilnosti lahko ostanejo neodkrite, npr. če gre za nedovoljeno dogovarjanje med zaposlenimi, nedovoljeno dogovarjanje med zaposlenimi in ljudmi zunaj organizacije ali če je poslovodstvo samo vpleteno v te nepravilnosti. Revizor IS naj prouči, ali bo to točko dokumentiral v revizijski listini ali listini o poslu.

3.2.4 Kadar ima revizor IS posebno informacijo o obstoju nepravilnost ali nezakonitega dejanja, je dolžan izvesti postopke za njihovo odkrivanje in preiskavo ter o njej poročati.

3.2.5 Revizor IS naj obvesti revizijsko komisijo (ali enakovreden organ) in poslovodstvo, kadar odkrije stanje ali razmere večjega tveganja za morebitno nepravilnost ali nezakonito dejanje, pa čeprav to še ni odkrito.

3.2.6 Revizor IS mora primerno dobro poznati področje, da lahko prepozna dejavnike tveganja, ki utegnejo prispevati k nastanku nepravilnega ali nezakonitega dejanja.

3.2.7 Revizorji IS morajo zagotoviti, da so ves čas trajanja revizijskega posla neodvisni od predmeta.

3.2.8 Pri podrobnejši razpravi o odgovornostih revizorjev naj se revizorji IS sklicujejo na standard S9 (1207) Nepravilnosti in nezakonita dejanja.

4. Ocenjevanje tveganja

4.1 Načrtovanje ocenjevanja tveganja

4.1.1 Revizor IS naj oceni tveganje pojava nepravilnosti ali nezakonitih dejanj, povezanih z revidiranim področjem, pri čemer naj uporabi ustrezno metodologijo. Pri pripravi te ocene naj revizor IS upošteva dejavnike, kot so:

- organizacijske značilnosti, kot so na primer podjetniška etika, organizacijska struktura, ustreznost nadzora, struktura plač in nagrad, pritiski za uspešno poslovanje podjetja, usmeritev organizacije,
- zgodovina organizacije, pojavi nepravilnosti v preteklosti in dejavnosti, ki so jim sledile za ublažitev ali zmanjšanje z nepravilnostmi povezanih izsledkov,
- nedavne spremembe v poslovodstvu, operacijah ali sistemih IS ter sedanja strateška usmeritev organizacije,

- vplivi novih strateških partnerstev,
- vrste sredstev, ki jih organizacija ima, ali storitev, ki jih ponuja, in njihova dovzetnost za nepravilnosti,
- ocenjevanje moči ustreznih kontrol in možnosti, da se vzpostavljene kontrole ne upoštevajo ali da se jim je mogoče izogniti,
- veljavne predpisane ali zakonske zahteve,
- notranje usmeritve, kot so spodbujanje opozarjanja na nepravilnosti, politika do trgovanja na podlagi notranjih informacij in etični kodeks zaposlenih in poslovodstva,
- razmerja zainteresiranih in finančni trgi,
- zmožnosti človeških virov,
- zaupnost in celovitost ključnih tržnih informacij,
- zgodovina revizijskih izsledkov iz prejšnjih revizij,
- panoga in konkurenčno okolje, v katerem organizacija deluje,
- izsledki pregledov, opravljenih zunaj predmeta in obsega revizije, kot so izsledki svetovalcev, skupin za zagotavljanje kakovosti ali posebnih preiskovanj poslovodstva,
- izsledki, ki so se pokazali med rednim poslovanjem,
- procesna dokumentacija in sistem vodenja kakovosti,
- tehnična dognanost in zahtevnost informacijskega sistema ali sistemov, ki podpirajo revidirano področje,
- lastni razviti/vzdrževani aplikacijski sistemi namesto paketne programske opreme za ključne poslovne sisteme,
- vpliv nezadovoljstva zaposlenih,
- morebitni delavci na čakanju, oddajanje del zunanjim izvajalcem, odtujitev poslovnih sredstev ali prestrukturiranje,
- obstoj sredstev, ki so zelo dovzetna za nezakonito prisvojitev,
- slabo organizacijsko, finančno in/ali poslovno delovanje,
- odnos poslovodstvo do etičnih vprašanj,
- nepravilnosti in nezakonita dejanja, ki so običajna za določeno panogo ali so se dogajala v podobnih organizacijah.

4.1.2 Pri ocenjevanju tveganj bi bilo treba upoštevati samo tiste dejavnike, ki so pomembni za organizacijo in so predmet revizijskega posla, vključno z dejavniki tveganja, ki se nanašajo na:
- nepravilnosti ali nezakonita dejanja, ki vplivajo na finančno-računovodske evidence,
- nepravilnosti ali nezakonita dejanja, ki nimajo učinka na finančne evidence, vplivajo pa na organizacijo,
- druge nepravilnosti ali nezakonita dejanja, ki se nanašajo na zadostnost kontrol v organizaciji.

4.1.3 V okviru procesa načrtovanja in ocenjevanja tveganja naj revizor IS povpraša poslovodstvo o zadevah, kot so:
- kako oni razumejo raven tveganja nepravilnosti in nezakonitih dejanj v organizaciji,
- ali poznajo nepravilnosti in nezakonita dejanja, ki so se ali bi se lahko zgodila v organizaciji ali proti njej,
- kako spremljajo ali obvladujejo tveganje nepravilnosti ali nezakonitih dejanj,
- katere postopke so vzpostavili za obveščanje ustreznih zainteresiranih o obstoju tveganja nepravilnosti ali nezakonitih dejanj,
- kateri nacionalni in regionalni zakoni veljajo v državi, v kateri družba posluje, in v kolikšni meri pravna služba sodeluje z odborom za obvladovanje tveganj in revizijsko komisijo?

5. Načrtovanje revizijskega dela

5.1 Načrtovanje posla

5.1.1 Revizor IS sicer ni izrecno odgovoren za odkrivanje ali preprečevanje nezakonitih dejanj ali nepravilnosti, vendar naj oblikuje postopke za odkrivanje nezakonitih dejanj ali nepravilnosti na podlagi ocenjene stopnje tveganja, da bi do njih lahko prišlo.

5.1.2 Pri načrtovanju posla naj revizor IS pridobi razumevanje o zadevah, kot so:
- osnovno razumevanje delovanja in ciljev organizacije,
- notranje kontrolno okolje,
- usmeritve in postopki za vodenje ravnanja zaposlenih,
- postopki za potrjevanje in spremljanje skladnosti,
- pravno in ureditveno okolje, v katerem organizacija deluje,
- mehanizem, ki ga organizacija uporablja za doseganje, spremljanje in zagotavljanje skladnosti z zakoni in predpisi, ki vplivajo na organizacijo.

5.2 Postopek izvedbe posla

5.2.1 Revizor IS naj oblikuje postopke za izvedbo posla tako, da upošteva ugotovljene ravni tveganja za nepravilnosti in nezakonita dejanja.

5.2.2 Izide ocenjevanja tveganja in druge ob načrtovanju izvedene postopke je treba uporabiti za to, da se določijo narava, obseg in čas postopkov, izvedenih med revizijskim poslom.

5.2.3 Revizor IS naj pri vodstvu IT in poslovodstvu uporabnika (kot je ustrezno) poizve, kako zagotavljajo skladnost z zakoni in predpisi.

5.2.4 Revizor IS naj izide ocenjevanja tveganja uporabi za to, da določi naravo, čas in obseg preizkušanja, potrebnega za pridobitev zadostnih revizijskih dokazov za sprejemljivo zagotovilo, da so prepoznane:
- nepravilnosti, ki bi lahko pomembno vplivale na revidirano področje ali na organizacijo kot celoto,
- slabosti v delovanju kontrol, zaradi katerih ne bi bilo mogoče preprečiti ali odkriti pomembne nepravilnosti,
- vse bistvene pomanjkljivosti v zasnovi ali delovanju notranjih kontrol, ki bi utegnile vplivati na zmožnost izdajatelja, da zabeleži, obdela in združi poslovne podatke ter o njih poroča.

5.3 Ovrednotenje izidov postopkov izvedbe posla

5.3.1 Revizor IS naj pregleda izide postopkov izvedbe posla, da ugotovi, ali so se morda pokazali znaki nepravilnosti ali nezakonitih dejanj.

5.3.2 Pri izvajanju tega ocenjevanja je treba pregledati dejavnike tveganja iz 4. poglavja te smernice na podlagi dejansko izvedenih postopkov in tako pridobiti utemeljena zagotovila, da so bila obdelana vsa prepoznana tveganja.

5.3.3 Ocenjevanje naj vključuje tudi ocenitev izidov postopkov, da se ugotovi, ali obstajajo nedokumentirani dejavniki tveganja.

6. Izvajanje revizijskega dela

6.1 Odziv na morebitna nezakonita dejanja

6.1.1 Med revizijskim poslom lahko revizor IS opazi znake obstoja nepravilnosti ali nezakonitih dejanj. Če prepozna znake nezakonitega dejanja, naj revizor IS pretehta njihov morebitni učinek na predmet revizijskega posla, poročilo in organizacijo.

6.1.2 Kadar koli revizor IS pridobi informacije o morebitnem nezakonitem dejanju, naj pri delu upošteva naslednje korake:
- spozna naravo dejanja,
- razume okoliščine, v katerih se je zgodilo,
- pridobi zadostne podporne informacije za ovrednotenje učinka nepravilnosti ali nezakonitega dejanja,
- izvede dodatne postopke, da določi učinek nepravilnosti ali nezakonitega dejanja in ugotovi, ali obstajajo še dodatna dejanja.

6.1.3 Revizor IS naj sodeluje z ustreznim osebjem organizacije (kot je osebje za organizacijsko varnost), pa tudi s poslovodstvom (če je le mogoče na ustrezni ravni nad vpletenimi), da ugotovi, ali je res prišlo do nepravilnosti ali nezakonitega dejanja, in kakšen je njihov učinek.

6.1.4 Kadar je v nepravilnost vpleten član poslovodstva, naj revizor IS ponovno pretehta zanesljivost predstavitve, ki jo je dalo poslovodstvo. Kot je bilo že omenjeno, mora revizor IS praviloma sodelovati z ustrezno ravnijo vodstva, ki je nadrejena posamezniku, povezanem z nepravilnostjo ali nezakonitim dejanjem.

6.1.5 Če okoliščine jasno ne kažejo na kaj drugega, naj revizor IS predpostavlja, da pri nepravilnosti ali nezakonitem dejanju ne gre le za enkraten pojav.

6.1.6 Revizor IS naj pregleda tudi ustrezne dele notranjih kontrol organizacije, da ugotovi, zakaj niso preprečile ali odkrile pojava nepravilnosti ali nezakonitega dejanja.

6.1.7 Revizor IS naj ponovno pretehta prejšnjo oceno zadostnosti, delovanja in učinkovitosti notranjih kontrol organizacije.

6.1.8 Kadar revizor IS prepozna razmere za obstoj (možnih ali dejanskih) nepravilnosti ali nezakonitih dejanj, naj spremeni in dopolni izvedene postopke, da potrdi ali reši zadevo, ki jo je odkril med izvajanjem posla. Obseg takih sprememb ali dodatnih postopkov je odvisen od presoje revizorja IS glede na:
- vrsto nepravilnosti ali nezakonitega dejanja, ki se je morda zgodilo,
- zaznano tveganje njegove pojavnosti,
- možen učinek na organizacijo, kar zajema tudi finančne učinke in vpliv na dobro ime organizacije,
- verjetnost ponovnega pojava podobnih nepravilnosti ali nezakonitih dejanj,
- možnost, da je poslovodstvo vedelo za nepravilnost ali nezakonito dejanje ali je bilo celo vpleteno vanj,
- morebitne ukrepe organa upravljanja in/ali poslovodstva,
- možnost, da je do neskladnosti z zakoni in predpisi prišlo nenamerno,
- verjetnost, da bodo zaradi neskladnosti s predpisi podjetju naložene pomembna globa ali druge sankcije, npr. odvzem pomembnega dovoljenja,
- učinek na javni interes, ki je lahko posledica nepravilnosti.

6.2 Učinek ugotovitve nepravilnosti

6.2.1 Če so bile odkrite nepravilnosti, naj revizor IS oceni učinek teh dejavnosti na revizijske cilje in na zanesljivost zbranih revizijskih dokazov. Poleg tega naj revizor IS razmisli, ali bo nadaljeval revizijo, če:
- se zdi, da je učinek nepravilnosti tako bistven, da ne bo mogoče pridobiti zadostnih in zanesljivih revizijskih dokazov,
- revizijski dokazi kažejo, da so bili poslovodstvo ali zaposleni, ki imajo bistveno vlogo pri notranjih kontrolah naročnika, pri nepravilnostih udeleženi ali so jih dopuščali.

6.3 Učinek ugotovitve kazalnikov nepravilnosti

6.3.1 Če revizijski dokazi kažejo, da so se lahko zgodile nepravilnosti, mora revizor IS:
- priporočiti poslovodstvu, da zadevo podrobno razišče ali ustrezno ukrepa. Če revizor IS sumi, da je poslovodstvo vpleteno v nepravilnost, naj ugotovi, kdo je ustrezna odgovorna oseba v organizaciji, ki ji je treba o teh ugotovitvah poročati. Če se izkaže, da notranje poročanje ni mogoče, naj se revizor IS posvetuje z revizijsko komisijo in pravnim svetovalcem o tem, ali je priporočljivo o izsledkih poročati zunaj organizacije in kakšna so s tem povezana tveganja;
- izvesti ustrezne ukrepe, da podpre revizijske izsledke, ugotovitve in priporočila.

6.4 Pravna obravnava

6.4.1 Če revizijski dokazi kažejo, da bi nepravilnost lahko vključevala tudi nezakonito dejanje, naj revizor IS prouči možnost, da sam neposredno poišče pravni nasvet ali da to priporoči poslovodstvu. Revizor IS lahko, če želi, opredeli odgovornost za pravne stroške v revizijski listini ali listini o poslu.

7. Poročanje

7.1 Notranje poročanje

7.1.1 Odkritje nepravilnosti je treba pravočasno sporočiti ustreznim osebam v organizaciji. Obvestilo mora biti naslovljeno na raven poslovodstva, ki je nadrejena tisti, za katero obstaja sum pojava nepravilnosti. Poleg tega je treba o nepravilnostih poročati nadzornemu svetu, revizijski komisiji nadzornega sveta ali enakovrednemu organu, razen če gre za zadeve, ki so očitno nebistvene glede finančnega učinka in ki ne kažejo pomembnih slabosti v delovanju kontrol. Če revizor IS sumi, da so vpletene vse ravni poslovodstva, potem je treba o izsledkih zaupno poročati organom upravljanja organizacije, kot so nadzorni svet, guvernerji, skrbniki ali revizijska komisija, v skladu s krajevno veljavnimi predpisi in zakoni.

7.1.2 Revizor IS naj pri poročanju o nepravilnosti ali nezakonitem dejanju uporabi strokovno presojo. Revizor IS naj se o izsledkih ter naravi, času in obsegu vseh nadaljnjih postopkov, ki jih je treba opraviti, pogovori z ustrezno ravnijo poslovodstva, ki je vsaj za eno

stopnjo nadrejena domnevno vpletenim osebam. V takih okoliščinah je še posebej pomembno, da revizor IS ohrani neodvisnost. Pri določanju ustreznih oseb, ki jim bo poročal o nepravilnosti ali nezakonitem dejanju, naj revizor IS upošteva vse pomembne okoliščine, vključno z možnostjo, da je vpleteno tudi višje poslovodstvo.

7.1.3 Skrbno je treba razmisliti o notranjem razdeljevanju poročil o nepravilnostih. Pojavnost in učinek nepravilnosti sta občutljivi zadevi in poročanje o njiju je povezano s tveganji, ki so med drugim:
- nadaljnja zloraba slabosti v delovanju kontrol kot posledica objave njihovih podrobnosti,
- izguba strank, dobaviteljev in investitorjev, če pride do (pooblaščenega ali nepooblaščenega) razkritja zunaj organizacije,
- izguba ključnega osebja in poslovodstva, vključno s tistimi, ki niso bili vpleteni v nepravilnost, ker je upadlo zaupanje v poslovodstvo in prihodnost organizacije.

7.1.4 Revizor IS naj upošteva, da o nepravilnostih poroča ločeno od vseh drugih revizijskih zadev, če bi to pomagalo pri nadzoru nad razdeljevanjem poročila.

7.1.5 Poročilo revizorja IS naj vsebuje:
- kritične usmeritve in prakse, ki jih je sprejela organizacija,
- pri kakršnih koli odstopanjih od splošno sprejetih standardov razloge poslovodstva za tako odstopanje in revizorjevo mnenje o takih odstopanjih.

7.1.6 Revizor IS naj si prizadeva, da se izogne opozarjanju kogar koli, ki utegne biti vpleten ali vključen v nepravilnost ali nezakonito dejanje, da zmanjša možnost, da bi ti posamezniki uničili ali prikrili dokaze.

7.2 Zunanje poročanje

7.2.1 Zunanje poročanje je lahko zakonska ali druga predpisana obveznost. Obveznost lahko velja za poslovodstvo organizacije ali za posameznike, ki so vključeni v odkrivanje nepravilnosti, ali za oboje. Ne glede na odgovornost organizacije, da prijavi nezakonito dejanje ali nepravilnost, dolžnost zaupnosti do organizacije revizorju IS preprečuje, da bi prijavil katere koli morebitne ali ugotovljene nepravilnosti ali nezakonita dejanja. Toda v nekaterih okoliščinah se od revizorja IS lahko zahteva, da razkrije nepravilnost ali nezakonito dejanje. To se nanaša na zadeve, kot so:
- skladnost z zakonskimi ali drugimi predpisanimi zahtevami,
- zahteve zunanjega revizorja,
- sodni poziv priči ali odredba sodišča,
- agencija za financiranje ali vladna agencija v skladu z zahtevami za revizijo podjetij, ki prejemajo državno finančno pomoč.

7.2.2 Kadar je zahtevano zunanje poročanje, mora poročilo pred zunanjo objavo potrditi ustrezna raven vodstva revizije in ga je treba vnaprej pregledati tudi skupaj s poslovodstvom revidiranca, razen če to preprečujejo veljavni predpisi ali posebne okoliščine revizije. Primeri posebnih okoliščin, ki utegnejo preprečiti pridobitev soglasja poslovodstva revidiranca, so med drugim:
- dejavna vpletenost poslovodstva revidiranca v nepravilnost,
- nedejavna privolitev poslovodstva revidiranca v nepravilnost.

7.2.3 Če se poslovodstvo revidiranca ne strinja z zunanjo objavo poročila in je zunanje poročanje zakonska ali sicer predpisana obveznost, naj revizor IS razmisli o posvetovanju z revizijsko komisijo in pravnim svetovalcem o tem, ali je priporočljivo o izsledkih poročati zunaj organizacije in kakšna so s tem povezana tveganja. V nekaterih pravnih sistemih je revizor IS lahko zaščiten s pogojno imuniteto. Toda tudi v okoliščinah, ko so revizorji IS zaščiteni z imuniteto, naj skušajo pred takim razkritjem poiskati pravno pomoč in nasvet, da si zagotovijo, da so dejansko zaščiteni s tako imuniteto.

7.2.4 Revizor IS naj z odobritvijo vodstva revizije pravočasno preda poročilo ustreznim regulativnim organom. Če organizacija ne razkrije znane nepravilnosti ali nezakonitega dejanja ali če od revizorja IS zahteva, da utaji te izsledke, mora revizor IS poiskati pravno pomoč in nasvet.

7.2.5 Kadar je revizorju IS znano, da je poslovodstvo dolžno prijaviti goljufive dejavnosti zunanji organizaciji, mora revizor IS uradno obvestiti poslovodstvo o tej dolžnosti.

7.2.6 Če je nepravilnost odkril revizor IS, ki ni član skupine za zunanjo revizijo, naj revizor IS prouči možnost, da poročilo pravočasno odda zunanjim revizorjem.

7.3 Omejitev predmeta in obsega revizije

7.3.1 Kadar sta predmet in obseg revizije omejena, naj revizor IS vključi pojasnilo o naravi in učinku te omejitve v revizijsko poročilo. Do take omejitve lahko pride, če
- revizor IS ni mogel opraviti nadaljnjega dela, ki je po njegovem mnenju potrebno za izpolnitev prvotnih revizijskih ciljev in v podporo revizijskim ugotovitvam, npr. zaradi nezanesljivih revizijskih dokazov, pomanjkanja virov ali omejitev, ki jih je revizijskim dejavnostim postavilo poslovodstvo;
- poslovodstvo ni izvedlo preiskav, ki jih je priporočil revizor IS.

8. Datum uveljavitve

8.1 Ta smernica velja za vse revizije IS, ki se začnejo 1. marca 2000 ali pozneje. Ta smernica je bila pregledana in posodobljena, združena s smernico G19 Nepravilnosti in nezakonita dejanja, ki jo zdaj nadomešča, ter velja od 1. septembra 2008.

2208 Revizijsko vzorčenje (G10)

1. Izhodišča

1.1 Povezava s standardi

1.1.1 Standard S6 (1203) Izvajanje revizijskih del določa: »Med potekom revizije mora revizor IS pridobiti zadostne, zanesljive in ustrezne dokaze, da se dosežejo revizijski cilji. Revizijski izsledki in ugotovitve morajo biti podprti z ustrezno analizo in razlago teh dokazov.«

1.2 Povezava s COBIT-om

1.2.1 Izbira najustreznejšega gradiva v COBIT-u, ki je primerno glede na predmet in obseg določene revizije, temelji na izbiri posebnih COBIT-ovih procesov IT in upoštevanju COBIT-ovih kontrolnih ciljev ter z njimi povezanih praks upravljanja. Za izpolnitev zahteve za revizijsko vzorčenje revizorjev IS so procesi v COBIT-u, ki bodo najverjetneje ustrezni, izbrani in prilagojeni, tu razvrščeni v primarne in sekundarne. Procesni in kontrolni cilji, ki jih je treba izbrati in prilagoditi, so lahko različni glede na posebno področje in obseg ter opis nalog in pristojnosti posla.

1.2.2 ME2 *Spremljajte in vrednotite notranje kontrole* izpolnjuje poslovno zahtevo za IT glede varovanja uresničevanja ciljev IT in ravnanja v skladu z zakoni, predpisi in pogodbami, povezanimi z IT, z usmerjanjem na spremljanje procesov notranje kontrole za aktivnosti, povezane z IT, ter določanje ukrepov za izboljševanje.

1.2.3 ME3 *Zagotovite skladnost z zunanjimi zahtevami* izpolnjuje poslovno zahtevo za IT glede skladnosti z zakoni in predpisi z usmerjanjem na prepoznavanje vseh veljavnih zakonov in predpisov in ustreznih ravni skladnosti IT in optimizacijo procesov IT za zmanjšanje tveganja neskladnosti.

1.2.4 Primarni procesi so:

- PO8 *Upravljajte kakovost*,
- PO9 *Ocenjujte in obvladujte tveganja IT*,
- AI6 *Upravljajte spremembe*,
- ME2 *Spremljajte in vrednotite notranje kontrole*,
- ME3 *Zagotovite skladnost z zunanjimi zahtevami*.

1.2.5 Najpomembnejša informacijska sodila pa so:

- primarna: učinkovitost, celovitost, zanesljivost in skladnost,
- sekundarna: zaupnost, uspešnost in razpoložljivost.

1.3 Potreba po smernici

1.3.1 Namen te smernice je dati revizorju IS navodila za zasnovo in izbiro revizijskega vzorca in za ovrednotenje izidov vzorca. Z ustreznim vzorčenjem in ovrednotenjem bodo izpolnjene zahteve po 'zadostnih, zanesljivih, ustreznih in uporabnih dokazih, podprtih z ustrezno analizo'.

1.3.2 Revizor IS naj upošteva izbiro tehnik, s katerimi pridobi statistično reprezentativni vzorec za preverjanje skladnosti ali preizkušanje podatkov.

1.3.3 Primeri preizkušanja skladnosti kontrol, za katera bi lahko upoštevali vzorčenje, so med drugim uporabnikova pooblastila dostopa, postopki za kontrolo sprememb v programu, postopkovna dokumentacija, programska dokumentacija, nadaljnja obravnava izjem, pregled dnevnikov in revizija licenc za programsko opremo.

1.3.4 Primeri preizkušanja podatkov, za katera bi lahko upoštevali vzorčenje, so med drugim ponovno izvajanje zapletenih izračunov (npr. izračuna obresti) na vzorcu obračunov, vzorcu transakcij za potrditev dokazne dokumentacije itd.

1.3.5 Ta smernica daje navodila za uporabo standardov revidiranja IS. Revizor IS jo mora upoštevati pri odločanju o tem, kako doseči izvajanje standarda S6; uporabljati jo mora po strokovni presoji in mora biti pripravljen utemeljiti vsako odstopanje.

1.3.6 Drugi koristni viri za revizijsko vzorčenje so še Mednarodni standard revidiranja MSR 530 Revizijsko vzorčenje, ki ga je izdala Mednarodna zveza računovodskih strokovnjakov (IFAC).

2. Izvajanje revizijskega dela

2.1 Revizijsko vzorčenje

2.1.1 Pri uporabi statističnih ali nestatističnih metod vzorčenja naj revizor IS oblikuje in izbere revizijski vzorec, opravi revizijske postopke in ovrednoti izide vzorca, da pridobi zadostne, zanesljive, ustrezne in uporabne revizijske dokaze.

2.1.2 Pri oblikovanju revizijskega mnenja revizorji IS pogosto ne proučijo vseh razpoložljivih informacij, ker utegne biti to težko izvedljivo, do veljavnih ugotovitev pa lahko pridejo z revizijskim vzorčenjem.

2.1.3 Revizijsko vzorčenje je opredeljeno kot uporaba revizijskih postopkov na manj kot 100 odstotkih populacije, kar revizorju IS omogoča ocenitev revizijskih dokazov za nekatere značilnosti izbranih postavk, na podlagi česar lahko oblikuje sklep, ali kar mu pomaga pri oblikovanju sklepa o tej populaciji.

2.1.4 Statistično vzorčenje vključuje uporabo tehnik, iz katerih je mogoče pridobiti matematično zgrajene ugotovitve v zvezi z dano populacijo.

2.1.5 Nestatistično vzorčenje ne temelji na statističnih metodah in njegovih izidov ni mogoče ekstrapolirati na celotno populacijo, ker že vzorec sam verjetno ni reprezentativna populacija.

2.2 Oblikovanje vzorca

2.2.1 Pri oblikovanju velikosti in sestave revizijskega vzorca naj revizorji IS upoštevajo posebne revizijske cilje, naravo populacije ter metode vzorčenja in izbiranja.

2.2.2 Revizor IS mora upoštevati, da je treba k oblikovanju in analizi vzorcev pritegniti ustrezne specialiste.

2.2.3 Vzorčna enota je odvisna od namena vzorca. Za preizkušanje skladnosti kontrol se običajno uporablja vzorčenje po atributih, kjer je vzorčna enota dogodek ali transakcija (npr. kontrola, kot je potrditev računa). Za preizkušanje podatkov se pogosto uporablja vzorčenje po spremenljivkah ali ocenitvah, kjer je vzorčna enota pogosto denarna.

2.2.4 Revizor IS mora upoštevati posamezne revizijske cilje, ki jih je treba doseči, in revizijske postopke, s katerimi bodo ti cilji najverjetneje lahko doseženi. Poleg tega je treba, kadar je revizijsko vzorčenje ustrezno, upoštevati tudi naravo iskanih revizijskih dokazov in morebitne možnosti napake.

2.2.5 Populacija je celoten zbir podatkov, iz katerih želi revizor IS vzeti vzorec, da pride do sklepa o populaciji. Zato mora biti populacija, iz katere se jemlje vzorec, ustrezna in preverjeno popolna za posamezni revizijski cilj.

2.2.6 Pri učinkovitem in uspešnem oblikovanju vzorca je lahko ustrezna pomoč tudi stratifikacija. Stratifikacija je razdelitev populacije na podpopulacije izrecno opredeljenih podobnih značilnosti, tako da vsaka vzorčna enota lahko pripada samo enemu stratumu.

2.2.7 Pri določanju velikosti vzorca mora revizor IS upoštevati tveganje pri vzorčenju, količino napak, ki bi bila še sprejemljiva, in kolikšen obseg napak je pričakovan.

2.2.8 Tveganje pri vzorčenju izhaja iz možnosti, da se ugotovitev revizorja IS lahko razlikuje od ugotovitve, do katere bi prišel, če bi po istem revizijskem postopku pregledal celotno populacijo. Poznamo dve vrsti tveganja pri vzorčenju:

- tveganje napačnega sprejetja – tveganje, da je pomembno napačna navedba ocenjena kot neverjetna, kadar je populacija dejansko pomembno napačno navedena,
- tveganje napačne zavrnitve – tveganje, da je pomembno napačna navedba ocenjena kot verjetna, kadar populacija dejansko ni pomembno napačno navedena.

2.2.9 Na velikost vzorca vpliva raven tveganja pri vzorčenju, ki jo je revizor IS pripravljen sprejeti. Tveganje pri vzorčenju je treba obravnavati tudi glede na model revizijskega tveganja in njegove sestavine, tveganje pri delovanju, tveganje pri kontroliranju in tveganje pri odkrivanju.

2.2.10 Dopustna napaka je največja napaka v populaciji, ki so jo revizorji IS pripravljeni sprejeti in pri tem še vedno ugotoviti, da je revizijski cilj dosežen. Za postopke preizkušanja podatkov je dopustna napaka povezana s presojo revizorja IS o pomembnosti. Pri preizkusih skladnosti je to največja stopnja odstopanja od predpisanega kontrolnega postopka, ki jo je revizor IS pripravljen sprejeti.

2.2.11 Če revizor IS pričakuje, da bodo v populaciji napake, je treba običajno pregledati večji vzorec, kot če jih v njem ni pričakovati, da se lahko ugotovi, da dejanska napaka v populaciji ni večja od načrtovane dopustne napake. Manjše velikosti vzorca so utemeljene, kadar se pričakuje, da je populacija brez napak. Pri določanju pričakovane napake v populaciji naj revizor IS upošteva zadeve, kot so količina napak, ugotovljenih v prejšnjih revizijah, spremembe v postopkih organizacije in dokazi, ki so na voljo iz ocenitve sistema notranje kontrole in izidov analitičnih pregledov.

2.3 Izbira vzorca

2.3.1 Običajno se uporabljajo štiri metode vzorčenja. Statistične metode vzorčenja so:

- Naključno vzorčenje zagotovi, da imajo vse kombinacije vzorčnih enot v populaciji enako možnost, da so izbrane.
- Sistematično vzorčenje vključuje izbiranje vzorčnih enot z uporabo določenega intervala med izbirami, pri čemer se prvi interval začne naključno. Taki primeri so vzorčenje po denarni enoti ali izbira po tehtani vrednosti, pri čemer ima vsaka posamezna denarna vrednost (npr. 1 USD) v populaciji enako možnost, da je izbrana. Ker posamezne denarne enote običajno ni mogoče pregledovati ločeno, je za pregledovanje izbrana postavka, ki vključuje to denarno enoto. Ta metoda sistematično tehta izbiro v korist večjih količin, vendar pa še vedno daje enako možnost izbire vsaki denarni vrednosti. Drug primer pa je izbiranje vsake n-te vzorčne enote.

Nestatistične metode vzorčenja so:

- Vzorčenje na slepo – revizor IS izbere vzorec brez kakršne koli strukturirane tehnike, pri čemer se izogiba kakršne koli zavestne pristranskosti ali napovedljivosti. Vendar pa se na analizo na slepo izbranega vzorca pri oblikovanju sklepa o populaciji ne sme zanašati.
- Vzorčenje po presoji – revizor IS izbere vzorec po lastni presoji (npr. vse vzorčne enote nad določeno vrednostjo, vse za posebno vrsto izjeme, vse negativno, vsi novi uporabniki). Vedeti je treba, da po presoji izbran vzorec nima statistične podlage in izidov ne bi smeli ekstrapolirati na celo populacijo, ker je tak vzorec malo verjetno reprezentativna populacija.

2.3.2 Revizor IS naj izbere vzorec tako, da bo vzorec pričakovana reprezentativna populacija glede na značilnosti, ki se preizkušajo; torej naj uporabi statistične metode vzorčenja. Da ohrani revizijsko neodvisnost, mora revizor IS zagotoviti, da je populacija popolna, in nadzorovati izbiro vzorca.

2.3.3 Da je vzorec lahko reprezentativna populacija, mora biti za vse vzorčne enote v populaciji zagotovljena enaka ali znana verjetnost, da so izbrane, to pa zagotavljajo statistične metode vzorčenja.

2.3.4 Običajno se uporabljata dve metodi izbiranja: izbiranje po evidencah in izbiranje po količinskih merilih (npr. denarne enote). Običajne metode za izbiranje po evidencah so:

- naključno izbran vzorec (statistični vzorec),
- na slepo izbran vzorec (nestatistično),
- po presoji izbran vzorec (nestatistično: velika verjetnost, da vodi v pristranske sklepe).

Običajne metode za izbiranje po količinskih merilih so:

- naključno izbran vzorec (statistični vzorec po denarnih enotah),
- po določenem intervalu izbran vzorec (statistični vzorec je izbran z uporabo določenega intervala),
- celični vzorec (statistični vzorec, za katerega se uporabita naključna izbira in interval).

2.4 Dokumentacija

2.4.1 Revizijsko delovno gradivo naj vključuje dovolj podrobnosti za jasen opis ciljev vzorčenja in uporabljenih postopkov vzorčenja. Delovno gradivo naj vključuje vir populacije, uporabljeno metodo vzorčenja, parametre vzorčenja (npr. naključna začetna številka ali metoda, po kateri je bil določen naključni začetek, interval vzorčenja), izbrane vrednosti vzorca, podrobnosti izvedenih revizijskih preizkusov in dobljenih ugotovitev.

2.5 Ovrednotenje rezultatov vzorca

2.5.1 Potem ko so bili za vsako vzorčno postavko izvedeni revizijski postopki, ki ustrezajo določenemu revizijskemu cilju, naj revizor IS analizira vse odkrite morebitne napake v vzorcu, da ugotovi, ali so to dejansko napake, in če je to primerno, kakšna je narava teh napak in kakšen je vzrok zanje. Če je bila uporabljena statistična metoda vzorčenja, je treba napake, ki so ocenjene kot resnične napake, projicirati kot ustrezne za celo populacijo.

2.5.2 Vse odkrite morebitne napake v vzorcu je treba pregledati, da se ugotovi, ali so to dejansko napake. Revizor IS naj upošteva kakovostne vidike napak. To so med drugim narava in vzrok napake ter možen učinek napake na druge faze revizije. Napake, ki so posledica okvare avtomatiziranega procesa, imajo običajno širši vpliv na pogostost napak, kot jih ima človeška napaka.

2.5.3 Če pričakovanih revizijskih dokazov o posebni vzorčni postavki ni mogoče pridobiti, lahko morda revizor IS pridobi zadostne ustrezne revizijske dokaze z izvedbo drugih možnih postopkov za izbrano postavko.

2.5.4 Revizor IS naj upošteva projiciranje izidov vzorca na populacijo z metodo projiciranja, ki je skladna z metodo za izbiranje vzorčne enote. Projiciranje vzorca lahko vključuje tudi ocenitev verjetne napake v populaciji in oceno vseh nadaljnjih napak, ki morda niso bile odkrite zaradi nenatančnosti uporabljene tehnike skupaj s kakovostnimi vidiki ugotovljenih napak.

2.5.5 Revizor IS naj s primerjavo med projicirano napako populacije in dopustno napako tudi prouči, ali so napake v populaciji morda večje od dopustne napake, pri čemer naj upošteva izide drugih revizijskih postopkov, pomembnih za cilj revizije. Če projicirana napaka populacije presega dopustno napako, mora revizor IS ponovno oceniti tveganje pri vzorčenju, in če je to tveganje nesprejemljivo, razmisliti o razširitvi revizijskega postopka ali o izvedbi drugih možnih revizijskih postopkov.

3. Datum uveljavitve

3.1 Ta smernica velja za vse revizije IS, ki se začnejo 1. marca 2000 ali pozneje. Smernica je bila pregledana in posodobljena in velja od 1. avgusta 2008**.**

Smernice poročanja

Smernici poročanja sta:
2401 Poročanje (G20)
2402 Nadaljnja obravnava (G35)

Smernici sta na tem mestu vključeni v celoti. Za povezave na posamezne standarde obiščite *www.isaca.org/standard*.

2401 Poročanje (G20)

1. Izhodišča

1.1 Povezava s standardi ISACA

1.1.1 Standard S7 (1401) Poročanje določa: »Revizor IS mora po končani reviziji pripraviti poročilo v primerni obliki. Iz poročila morajo biti razvidni organizacija, predvideni prejemniki in morebitne omejitve glede razširjanja. Revizijsko poročilo mora navajati področje, cilje, obravnavano obdobje in vrsto, čas in trajanje opravljenega revizijskega dela. Poročilo mora vsebovati izsledke, ugotovitve in priporočila ter vse morebitne pridržke, omejitve ali omejitve področja dela, ki jih ima revizor IS v zvezi z revizijo.«

1.2 Opredelitev pojmov

1.2.1 Zadeva ali področje dejavnosti so posebne informacije, obdelane v poročilu in povezanih postopkih strokovnjaka za revidiranje in dajanje zagotovil za IT. Vključuje lahko zadeve, kot so zasnova ali delovanje notranjih kontrol v skladu s prakso ali standardi ali določenimi zakoni in predpisi o varovanju zasebnosti.

1.2.2 Posel potrditvenega poročanja je posel, pri katerem strokovnjak za revidiranje in dajanje zagotovil za IT preiskuje uradne trditve poslovodstva v zvezi z določeno zadevo ali pa neposredno zadevo samo. Poročilo strokovnjaka za revidiranje in dajanje zagotovil za IT vsebuje mnenje o naslednjih zadevah:

- Vsebina zadeve: ta poročila se nanašajo bolj neposredno na zadevo samo kot na uradno trditev. V nekaterih situacijah poslovodstvo ne bo moglo izdati uradne trditve o zadevi. Tak primer so storitve IT, ki so oddane v izvajanje tretji stranki. Poslovodstvo običajno ne bo moglo dati uradne trditve o kontrolah, za katere je odgovorna tretja stranka. Zato bo moral strokovnjak za revidiranje in dajanje zagotovil za IT verjetneje poročati neposredno o zadevi sami in ne o uradni trditvi poslovodstva.
- Uradna trditev poslovodstva o učinkovitosti kontrolnih postopkov.
- Poročila o preiskavah, pri čemer strokovnjak za revidiranje in dajanje zagotovil za IT izda mnenje o določeni zadevi. Ti posli lahko vključujejo poročila o kontrolah, ki jih je uvedlo poslovodstvo, in o učinkovitosti njihovega delovanja.

Ta smernica je usmerjena v prvo vrsto od navedenih mnenj. Če so v opisu nalog in pristojnosti zahtevana mnenja druge vrste, bo morda treba zahteve poročanja ustrezno prilagoditi.

1.2.3 Kontrolni cilji so cilji poslovodstva, ki se uporabijo kot okvir za razvijanje in uvajanje kontrol (kontrolnih postopkov).

1.2.4 Kontrole ali kontrolni postopki pomenijo usmeritve in postopke, ki se uvedejo za doseganje kontrolnih ciljev, na katere se nanašajo.

1.2.5 Slabosti v delovanju kontrol pomenijo pomanjkljivost v zasnovi ali delovanju kontrolnega postopka. Slabosti v delovanju kontrol imajo na področju določene dejavnosti lahko za posledico pomembna tveganja, ki niso zmanjšana na sprejemljivo raven (pomembna tveganja so tista, ki ogrožajo uresničevanje ciljev na področju dejavnosti, ki se pregleduje). Slabosti v delovanju kontrol so lahko pomembne, če se zasnova ali delovanje enega ali več kontrolnih postopkov ne zmanjša na sorazmerno nizko raven tveganja, da pride zaradi nezakonitega dejanja ali nepravilnosti do napačnih navedb in ustrezni kontrolni postopki teh ne odkrijejo.

1.2.6 Merila so standardi in primerjalne analize, ki se uporabljajo za merjenje in predstavitev zadeve in na podlagi katerih strokovnjak za revidiranje in dajanje zagotovil za IT zadevo tudi ovrednoti. Merila oziroma sodila morajo biti:

- nepristranska – objektivna in brez predsodkov,
- merljiva – zagotavljajo dosledno merjenje,
- popolna – vključujejo vse ustrezne dejavnike, potrebne za doseganje ugotovitev,
- ustrezna – nanašajo se na vsebino zadeve.

1.2.7 Posel neposrednega poročanja je posel, pri katerem poslovodstvo ne da nobene pisne uradne trditve o učinkovitosti svojih kontrolnih postopkov in strokovnjak za revidiranje in dajanje zagotovil za IT da mnenje, na primer glede učinkovitosti kontrolnih postopkov, neposredno o zadevi sami.

1.2.8 Struktura notranjega nadzora (notranje kontrole) so dinamični, med seboj povezani procesi, na katere vplivajo organ upravljanja, poslovodstvo in vse drugo osebje; zasnovana je zato, da daje sprejemljivo zagotovilo za uresničevanje naslednjih splošnih ciljev:

- uspešnost, učinkovitost in gospodarnost delovanja,
- zanesljivost poslovodstva,
- skladnost z veljavnimi zakoni, predpisi in notranjimi usmeritvami.

1.2.9 Na strategije poslovodstva za doseganje teh splošnih ciljev vplivata zasnova in delovanje naslednjih sestavin:

- kontrolno okolje,
- informacijski sistem,
- kontrolni postopki.

1.3 Potreba po smernici

1.3.1 Ta smernica določa, kako naj strokovnjak za revidiranje in dajanje zagotovil za IT ravna v skladu s standardi ISACA za revidiranje in dajanje zagotovil za IT in COBIT, kadar poroča o kontrolah informacijskega sistema podjetja in o kontrolnih ciljih, ki so z njimi povezani.

2. Uvod

2.1 Namen te smernice

2.1.1 Namen te smernice je dati usmeritev strokovnjakom za revidiranje in dajanje zagotovil za IT, ki morajo poročati o učinkovitosti kontrolnih postopkov za določeno področje dejavnosti:

- vodstvu podjetja na ravni organa upravljanja in/ali na poslovodni ravni ali
- določeni tretji stranki, na primer regulatorju ali drugemu revizorju.

2.1.2 Strokovnjak za revidiranje in dajanje zagotovil za IT je lahko zadolžen tudi za poročanje o učinkovitosti zasnove ali učinkovitosti delovanja.

3. Dajanje zagotovil

3.1 Vrste storitev

3.1.1 Strokovnjak za revidiranje in dajanje zagotovil za IT lahko opravlja katero koli od tu naštetih storitev:
- revizijo (neposredno ali potrditveno),
- pregled (neposreden ali potrditven),
- dogovorjene postopke.

3.2 Revizija in pregled

3.2.1 Revizija zagotavlja visoko, vendar ne popolno (absolutno) raven zagotovila o učinkovitosti kontrolnih postopkov. To je običajno izraženo kot sprejemljivo zagotovilo ob priznavanju dejstva, da je popolno zagotovilo mogoče redko doseči zaradi dejavnikov, kot so potreba po presoji, uporaba preizkušanja, naravne omejitve delovanja notranje kontrole, in ker je veliko dokazov, ki jih ima na voljo strokovnjak za revidiranje in dajanje zagotovil za IT, po svoji naravi prej prepričljivih kot neizpodbitnih.

3.2.2 Pregled zagotavlja zmerno raven zagotovila o učinkovitosti kontrolnih postopkov. Raven dobljenega zagotovila je manjša, kot ga daje revizija, ker je obseg dela manj obsežen kot pri reviziji, vrsta, čas in obseg izvedenih postopkov pa ne dajejo zadostnih in ustreznih revizijskih dokazov, da bi strokovnjak za revidiranje in dajanje zagotovil za IT lahko izrazil pozitivno mnenje. Cilj pregleda je omogočiti strokovnjaku za revidiranje in dajanje zagotovil za IT, da potrdi, ali je na podlagi postopkov njegovo pozornost pritegnilo kar koli, zaradi česar strokovnjak za revidiranje in dajanje zagotovil za IT meni, da na podlagi opredeljenih sodil kontrolni postopki niso bili uspešni (izraženo nikalno zagotovilo).

3.2.3 Tako revizije kot pregledi kontrolnih postopkov vključujejo:
- načrtovanje posla,
- ovrednotenje učinkovitosti zasnove kontrolnih postopkov,
- preizkušanje učinkovitosti delovanja kontrolnih postopkov (med revizijo in pregledom so razlike v vrsti, času in obsegu preizkušanja),
- oblikovanje sklepa in poročanje o zasnovi in učinkovitosti delovanja kontrolnih postopkov na podlagi opredeljenih sodil:
  - sklep za revizijo je izražen kot pozitivno mnenje in daje visoko raven zagotovila,
  - sklep za pregled je izražen kot izjava negativnega zagotovila in daje le zmerno raven zagotovila.

3.3 Dogovorjeni postopki

3.3.1 Izvajanje dogovorjenih postopkov se ne konča z izražanjem kakršnega koli zagotovila strokovnjaka za revidiranje in dajanje zagotovil za IT. Strokovnjak za revidiranje in dajanje zagotovil za IT je zadolžen za izvedbo določenih postopkov, da zagotovi zahtevane informacije tistim strankam, ki so se dogovorile za postopke, ki jih je treba izvesti. Strokovnjak za revidiranje in dajanje zagotovil za IT izda poročilo o dejanskih izsledkih tistim strankam, ki so se dogovorile za postopke. Iz tega poročila izoblikujejo prejemniki svoje lastne ugotovitve, ker strokovnjak za revidiranje in dajanje zagotovil za IT ni sam določil vrste, časa in obsega postopkov, da bi lahko izrazil kakršno koli zagotovilo. Poročilo je omejeno na tiste stranke (npr. regulativni organ), ki so se dogovorile za postopke, ki jih je treba izvesti, saj drugi ne poznajo razlogov za te postopke in bi njihove izide lahko napačno razlagali.

3.4 Poročanje o dogovorjenih postopkih

3.4.1 Poročilo o dogovorjenih postopkih naj bo v obliki postopkov in izsledkov. Poročilo naj vsebuje:
- naslov, ki vključuje besedo neodvisen,
- identifikacijske podatke določenih strank,
- podatke za prepoznavanje vsebine zadeve (ali pisno uradno trditev, ki se nanjo nanaša) in naravo posla,
- identifikacijske podatke o pristojni stranki,
- izjavo, da je za vsebino zadeve zadolžena pristojna stranka,
- izjavo, da so izvedeni postopki tisti, za katere so se dogovorile stranke, navedene v poročilu,
- izjavo, da so za zadostnost postopkov izključno odgovorne določene stranke same, in izjavo o omejitvi odgovornosti za zadostnost postopkov,
- seznam izvedenih postopkov (ali sklic nanje) in izsledkov, ki se nanje nanašajo,
- izjavo, da strokovnjak za revidiranje in dajanje zagotovil za IT ni bil najet za preiskavo zadeve in je tudi ni opravil,
- izjavo, da bi strokovnjak za revidiranje in dajanje zagotovil za IT, če bi izvedel dodatne postopke, lahko opazil še druge in bi o njih poročal,
- izjavo o omejitvi uporabe poročila, ker je namenjeno samo za uporabo določenih strank.

3.5 Pooblastilo za posel

3.5.1 Kadar je treba prevzeti posel, da se izpolni predpisana ali podobno naložena zahteva, je pomembno, da ima strokovnjak za revidiranje in dajanje zagotovil za IT zadostna zagotovila, da je ta vrsta posla dovoljena po ustreznem zakonu ali drugem viru pooblastila za posel. Če obstaja kakršna koli negotovost, je priporočeno, da se strokovnjak za revidiranje in dajanje zagotovil za IT in/ali stranka, ki ga za posel imenuje, obrne na ustreznega regulatorja ali drugo stranko, ki je odgovorna za postavljanje ali urejanje zahtev, in se dogovori za vrsto posla in zagotovilo, ki ga je treba pridobiti.

3.5.2 Strokovnjak za revidiranje in dajanje zagotovil za IT, od katerega se pred dokončanjem posla zahteva, da posel spremeni iz revizije v pregled ali posel za dogovorjene postopke, mora proučiti ustreznost takega dejanja in ne more soglašati s spremembo, če zanjo ni razumne utemeljitve. Sprememba na primer ni ustrezna, če je zahtevana zaradi prilagojenega poročila.

4. Revizijsko mnenje za IS

4.1 Omejitve

4.1.1 Mnenje strokovnjaka za revidiranje in dajanje zagotovil za IT temelji na postopkih, za katere se je odločil, da so potrebni, da zbere zadostne in ustrezne dokaze, vendar so ti dokazi po svoji naravi prej prepričljivi kot neizpodbitni. Zagotovilo, ki ga da strokovnjak za revidiranje in dajanje zagotovil za IT o učinkovitosti notranjih kontrol, je torej omejeno zaradi same narave notranjih kontrol in omejitev pri delovanju katerih koli notranjih kontrol. Med temi omejitvami so med drugim:

- običajna zahteva poslovodstva, da stroški notranjega nadzora ne presegajo pričakovanih koristi;
- večina notranjih kontrol je navadno bolj usmerjena v rutinske kot nerutinske transakcije oziroma dogodke;
- možnost za človekovo napako zaradi malomarnosti, raztresenosti ali utrujenosti, napačnega razumevanja navodil in napačne presoje;
- možnost, da se notranje kontrole zaobidejo z nedovoljenim dogovarjanjem med zaposlenimi ali s strankami zunaj podjetja;
- možnost, da bi oseba, ki je odgovorna za izvajanje notranje kontrole lahko zlorabila to odgovornost, npr. član poslovodstva, ki zavrne izvajanje kontrolnega postopka;
- možnost, da za poslovodstvo ne veljajo enake notranje kontrole kot za druge zaposlene;
- možnost, da postanejo notranje kontrole neustrezne zaradi spremenjenih okoliščin in se poslabša skladnost s postopki.

4.1.2 Navade, kultura in upravljanje sistemov (podjetniškega vodenja in IT) lahko sicer zavirajo nepravilnosti poslovodstva, ne morejo pa jih popolnoma odpraviti. Učinkovito kontrolno okolje lahko zmanjša verjetnost takih nepravilnosti. Dejavniki kontrolnega okolja, kot so uspešen organ upravljanja, revizijska komisija in notranjerevizijska funkcija lahko omejijo nepravilno ravnanje poslovodstva. Nasprotno pa neučinkovito kontrolno okolje izniči učinkovitost kontrolnih postopkov v ustroju notranjega nadzora. Na primer: čeprav ima podjetje ustrezne kontrolne postopke za IT v zvezi s skladnostjo z okoljskimi predpisi, si poslovodstvo lahko močno prizadeva prikriti informacije o vsaki odkriti kršitvi, ki bi lahko negativno vplivala na ugled podjetja v javnosti. Na učinkovitost ali pomembnost notranjih kontrol lahko vplivajo tudi dejavniki, kot so sprememba lastništva ali nadzora, spremembe v poslovodstvu ali med zaposlenimi ali razvoj dogodkov na trgu ali v panogi, v kateri podjetje posluje.

4.2 Poznejši dogodki

4.2.1 Včasih se po času ali obdobju, v katerem je bila zadeva preizkušena, vendar še pred datumom poročila strokovnjaka za revidiranje in dajanje zagotovil za IT, zgodijo dogodki, ki pomembno vplivajo na zadevo in zahtevajo prilagoditev ali razkritje v predstavitvi zadeve ali uradne trditve. Take pojave imenujemo poznejši dogodki. Pri opravljanju potrditvenega posla naj strokovnjaki za revidiranje in dajanje zagotovil za IT upoštevajo informacije o poznejših dogodkih, s katerimi so seznanjeni. Vendar pa strokovnjaki za revidiranje in dajanje zagotovil za IT niso zadolženi za odkrivanje poznejših dogodkov.

4.2.2 Strokovnjaki za revidiranje in dajanje zagotovil za IT naj povprašajo poslovodstvo, ali vedo za kakršne koli poznejše dogodke, ki so se zgodili do datuma poročila strokovnjakov za revidiranje in dajanje zagotovil za IT in bi lahko pomembno učinkovali na zadevo ali uradno trditev.

4.3 Ugotovitve in poročanje

4.3.1 Strokovnjak za revidiranje in dajanje zagotovil za IT naj ugotovi, ali je pridobil zadostne in ustrezne dokaze v podporo svojim sklepom v poročilu. Pri pripravi poročila je treba upoštevati vse pomembne pridobljene dokaze, ne glede na to, ali informacije zadevo potrjujejo ali jim nasprotujejo. Kadar je dano mnenje, naj bo to podprto z izidi kontrolnih postopkov na podlagi opredeljenih sodil.

4.3.2 Poročilo strokovnjaka za revidiranje in dajanje zagotovil za IT o učinkovitosti kontrolnih postopkov naj vključuje:

- naslov;
- naslovnika;
- opis obsega revizije, ime podjetja ali dela podjetja, na katero se zadeva nanaša, kar vključuje:
  - podatke za prepoznavanje ali opis področja dejavnosti,
  - sodila, ki so bila uporabljena kot podlaga za sklepno ugotovitev strokovnjaka za revidiranje in dajanje zagotovil,
  - čas ali obdobje, na katero se nanaša delo, ocenjevanje ali merjenje zadeve,
  - izjavo, da je za vzdrževanje učinkovitega ustroja notranjega nadzora, vključno s kontrolnimi postopki za to področje dejavnosti, odgovorno poslovodstvo;
- pri potrditvenem poslu tudi izjavo s podatki o viru uradne trditve poslovodstva o učinkovitosti kontrolnih postopkov;
- izjavo, da je strokovnjak za revidiranje in dajanje zagotovil za IT ta posel izvedel zato, da izrazi mnenje o učinkovitosti kontrolnih postopkov;
- opredelitev namena, za katerega je bilo pripravljeno poročilo strokovnjaka za revidiranje in dajanje zagotovil za IT, in podatki o tistih, ki so do njega upravičeni, ter izjava o neprevzemanju odgovornosti, če se poročilo uporabi v kakršen koli drug namen ali če ga uporabi kdo drug;
- opis uporabljenih sodil ali razkritje vira teh sodil;
- izjavo, da je bila revizija izvedena v skladu s standardi ISACA za revidiranje IS ali drugimi veljavnimi strokovnimi standardi;
- nadaljnje pojasnjevalne podrobnosti o spremenljivkah, ki vplivajo na dano zagotovilo in druge informacije, kot je ustrezno;
- kadar je to primerno, naj ločeno poročilo vključuje priporočila za popravljalne ukrepe in odziv poslovodstva;
- odstavek, v katerem je navedeno, da je lahko prišlo do kakšnih napačnih navedb zaradi napak ali goljufije, ki so zaradi omejitev pri delovanju katere koli notranje kontrole ostale neodkrite. Poleg tega naj bo v tem odstavku tudi navedeno, da je projiciranje ocene notranje kontrole za finančno poročanje za naslednja obdobja povezano s tveganjem, da ta notranje lahko postane neustrezna zaradi spremenjenih okoliščin ali da se lahko poslabša raven njene skladnosti z usmeritvami ali postopki. Revizija ni zasnovana za odkrivanje vseh slabosti v kontrolnih postopkih, ker se ne izvaja neprekinjeno skozi celo obdobje in ker so preizkusi kontrolnih postopkov izvedeni po metodi vzorčenja. Če je strokovnjak za revidiranje in dajanje zagotovil za IT izrazil mnenje s pridržki, naj bo vključen tudi odstavek z opisom pridržkov;

- izraženo mnenje o tem, ali sta bila zasnova in delovanje kontrolnih postopkov v vseh pomembnih pogledih za zadevno področje dejavnosti učinkovita;
- podpis strokovnjaka za revidiranje in dajanje zagotovil za IT;
- naslov strokovnjaka za revidiranje in dajanje zagotovil za IT;
- datum poročila strokovnjaka za revidiranje in dajanje zagotovil za IT. V večini primerov je datiranje poročila urejeno z veljavnimi strokovnimi standardi. V vseh drugih primerih pa naj bo datum poročila enak datumu dokončanja dela na terenu.

4.3.3 Pri poslu neposrednega poročanja poroča strokovnjak za revidiranje in dajanje zagotovil za IT neposredno o zadevi sami in ne o uradni trditvi o njej. Poročilo naj se sklicuje samo na zadevo posla in naj ne vsebuje nobenega sklicevanja na uradno trditev poslovodstva o zadevi.

4.3.4 Kadar strokovnjak za revidiranje in dajanje zagotovil za IT prevzame posel pregleda, naj bo v poročilu navedeno, da se sklep nanaša samo na zasnovo in učinkovitost delovanja in da je bilo delo strokovnjaka za revidiranje in dajanje zagotovil za IT v zvezi z učinkovitostjo delovanja omejeno predvsem na poizvedbe, preiskovanje, opazovanje in le minimalno preizkušanje delovanja notranjih kontrol. Poročilo vključuje izjavo, da revizija ni bila izvedena, da dajejo izvedeni postopki manjše zagotovilo kot revizija in da revizijsko mnenje ni izraženo. V izraženem zagotovilu v nikalni obliki je navedeno, da strokovnjak za revidiranje in dajanje zagotovil za IT ni opazil ničesar, zaradi česar bi menil, da so bili kontrolni postopki podjetja za zadevno področje dejavnosti v katerem koli pomembnem pogledu na podlagi opredeljenih sodil neučinkoviti.

4.3.5 Med izvajanjem posla strokovnjak za revidiranje in dajanje zagotovil za IT lahko opazi slabosti v delovanju kontrol. Strokovnjak za revidiranje in dajanje zagotovil za IT naj ustrezni ravni poslovodstva pravočasno poroča o vsaki ugotovljeni slabosti v delovanju kontrol. Postopki za vsak posel so zasnovani zato, da se zberejo zadostni ustrezni dokazi za oblikovanje sklepa v skladu s pogoji za posel. Če v pogojih za posel ni posebne zahteve, strokovnjak za revidiranje in dajanje zagotovil za IT ni dolžan zasnovati postopkov, s katerimi bi ugotovil zadeve, o katerih bi bilo primerno poročati poslovodstvu.

5. Datum uveljavitve

5.1 Ta smernica velja za vse revizije informacijskih sistemov, ki se začnejo 16. septembra 2010 ali pozneje**.**

2402 Nadaljnja obravnava (G35)

1. Izhodišča

1.1 Povezava s standardi

1.1.1 Standard S8 (1402) Nadaljnja obravnava določa: »Po poročanju o izsledkih in priporočilih mora revizor IS zahtevati in ovrednotiti ustrezne informacije, da ugotovi, ali je poslovodstvo pravočasno ustrezno ukrepalo.«

1.2 Povezava s COBIT-om

1.2.1 Kontrolni cilj na visoki ravni M3 (*Pridobite neodvisno zagotovilo*) navaja: »… pridobitev neodvisnega zagotovila, da se poveča zaupanje med organizacijami, strankami in tretjimi strankami kot izvajalci.«

1.2.2 Kontrolni cilj na visoki ravni M4 (*Zagotovite neodvisno revizijo*) navaja: »… zagotovitev neodvisne revizije, da se poveča stopnja zaupanja in izkoristijo najboljši nasveti iz prakse.«

1.2.3 Podrobni kontrolni cilj M4.8 (*Nadaljnja obravnava*) navaja: »Za reševanje revizijskih pripomb je odgovorno poslovodstvo. Revizorji naj zahtevajo in ovrednotijo ustrezne informacije o prejšnjih izsledkih, ugotovitvah in priporočilih, da ugotovijo, ali so bili pravočasno vpeljani ustrezni ukrepi.«

1.3 Referenčno gradivo COBIT-a

1.3.1 Izbira najustreznejšega gradiva v COBIT-u, ki je primerno glede na področje in obseg določene revizije, temelji na izbiri posebnih COBIT-ovih procesov IT in upoštevanju COBIT-ovih kontrolnih ciljev ter z njimi povezanih praks upravljanja. Za izpolnjevanje zahtev so procesi v COBIT-u, ki bodo najverjetneje ustrezni, izbrani in prilagojeni, tu razvrščeni kot primarni. Procesni in kontrolni cilji, ki jih je treba izbrati in prilagoditi, so lahko različni glede na obseg ter opis nalog in pristojnosti posla.

1.3.2 Primarni procesi so:

- M3 *Pridobite neodvisno zagotovilo*,
- M4 *Zagotovite neodvisno revizijo*.

1.3.3 Najpomembnejša informacijska sodila za usposobljenost so:

- primarna: učinkovitost, uspešnost, zaupnost, celovitost in skladnost,
- sekundarna: razpoložljivost in zanesljivost.

1.4 Namen smernice

1.4.1 Namen te smernice je dati usmeritev revizorjem IS, ki so vključeni v nadaljnjo obravnavo priporočil in revizijskih pripomb, danih v poročilih.

1.4.2 Ta smernica daje navodila pri uporabi standarda revidiranja informacijskih sistemov S8 (1402) Nadaljnja obravnava.

1.5 Uporaba smernice

1.5.1 Pri uporabi te smernice naj revizor IS upošteva njena navodila v povezavi z drugimi ustreznimi standardi in smernicami ISACA.

2. Nadaljnja obravnava

2.1 Opredelitev pojma

2.1.1 Nadaljnjo obravnavo revizorjev IS je mogoče opredeliti kot »proces, s katerim ugotovijo ustreznost, uspešnost in pravočasnost ukrepov, ki jih je sprejelo poslovodstvo na podlagi opažanj in priporočil iz poročila o poslu, vključno s tistimi, ki so jih navedli zunanji revizorji in drugi.«[1]

2.1.2 Postopek nadaljnje obravnave je treba vzpostaviti zato, da pomaga dati sprejemljivo zagotovilo, da vsak pregled, ki so ga opravili revizorji IS, prinaša organizaciji optimalne koristi prav z zahtevo, da se v skladu z zavezami poslovodstva izvajajo dogovorjeni ukrepi, ki izhajajo iz pregledov, ali da poslovodstvo spozna in sprejme tveganja pri delovanju zaradi odlaganja ali neuvedbe predlaganih ukrepov.

2.2 Predlagani ukrepi poslovodstva

2.2.1 V okviru razprav revizorja IS z organizacijo, v kateri je opravil revizijski posel, mora revizor IS doseči dogovor o izidih posla in po potrebi o načrtu ukrepanja za izboljšanje delovanja.

2.2.2 Poslovodstvo mora določiti datum izvedbe, to je datum, ko bo vsak predlagani ukrep dokončno izveden.

2.2.3 Potem ko je poslovodstvo predlagane aktivnosti o izvedbi predlaganih ukrepov ali drugačnem reševanju priporočil in revizijskih pripomb iz poročila sporočilo revizorju IS na razgovoru ali mu jih je posredovalo na drug način, se ti ukrepi vpišejo v končno poročilo kot odgovor poslovodstva skupaj z zagotovljenim datumom izvedbe.

2.2.4 Če revizor IS in organizacija, v kateri je bil opravljen revizijski posel, ne soglašata o določenem priporočilu ali revizijski pripombi, so v sporočilu o poslu lahko navedeni obe stališči in razlogi za nesoglašanje. Pisne pripombe organizacije se lahko vključijo kot dodatek k poročilu o poslu. Druga možnost pa je, da so stališča organizacije predstavljena v samem poročilu ali v spremnem pismu. Višje poslovodstvo (ali revizijska komisija, če obstaja) se mora potem odločiti, katero stališče bodo podprli. Če višje poslovodstvo (ali revizijska komisija) v določenem primeru podpre stališče organizacije, revizorju IS tega določenega priporočila ni treba naprej obravnavati, razen če se upošteva, da sta se pomembnost in velikost učinka opažanja/pripombe spremenila zaradi sprememb v okolju IS (glej točko 2.4.3).

2.2.5 Med nekaterimi pregledi, kot so preduvedbeni pregledi aplikacijskega sistema, se o izsledkih lahko tekoče poroča projektni skupini in/ali poslovodstvu, pogosto v obliki izjav o zadevah. V takih primerih je treba tekoče spremljati tudi ukrepe za reševanje takih zadev. Če so se priporočila iz izjave o zadevi začela izvajati, se ob priporočilu v končnem poročilu lahko navede “uresničeno” ali “se izvaja”. Poročati pa je treba tudi o priporočilih, ki so “uresničena” ali “se izvajajo”.

[1] Institute of Internal Auditors (IIA), “Practice Advisory 2500.A1-1,” 2002

2.3 Postopki nadaljnje obravnave

2.3.1 Postopki za nadaljnjo obravnavo morajo biti vzpostavljeni in vključujejo:
- zapis časovnega okvira, v katerem se mora poslovodstvo odzvati na dogovorjena priporočila,
- oceno odgovora poslovodstva,
- preverjanje in potrditev odgovora, če je ocenjen kot ustrezen (glej poglavje 2.7),
- nadaljnjo obravnavo, če je primerna,
- postopek obveščanja, s katerim se nerešena vprašanja in nezadovoljivi odgovori/ukrepi pošiljajo naprej na ustrezne ravni vodstva,
- proces za dajanje sprejemljivega zagotovila, da poslovodstvo prevzema s tem povezana tveganja, če popravljalni ukrepi zamujajo ali njihova uvedba ni bila predlagana.

2.3.2 Avtomatiziran sledilni sistem ali podatkovna baza lahko pomaga pri izvajanju nadaljnje obravnave.

2.3.3 Dejavniki, ki jih je treba upoštevati pri določanju ustreznih postopkov nadaljnje obravnave, so:
- vse spremembe v okolju IS, ki lahko vplivajo na pomembnost opažanja, ki je vključeno v poročilo,
- pomembnost ugotovitve ali priporočila iz poročila,
- možen posledični učinek, če popravljalni ukrep ne bo uspel,
- stopnja napora in stroškov, potrebnih za popravilo zadeve iz poročila,
- zahtevnost popravljalnega ukrepa,
- predvideni rok.

2.3.4 Če revizor IS dela v notranjem revizijskem okolju, je treba zadolžitev za nadaljnjo obravnavo opredeliti v pisni listini o dejavnosti notranje revizije.

2.4 Trajanje in časovni razpored nadaljnje obravnave

2.4.1 Vrsta, čas in obseg nadaljnje obravnave naj bi se ravnali po pomembnosti izsledkov, navedenih v poročilu, in učinkov, če popravni ukrepi ne bodo izvedeni. Trajanje nadaljnje obravnave po reviziji IS v primerjavi s prvotnim poročanjem je stvar strokovne presoje in je odvisno od števila premislekov, kot so narava ali velikost s tem povezanih tveganj in stroški za organizacijo.

2.4.2 Dogovorjene izide v zvezi z zelo tveganimi zadevami bi bilo treba nato obravnavati že kmalu po datumu, določenem za ukrepanje, in jih nato postopoma spremljati naprej.

2.4.3 Ker je nadaljnja obravnava neločljiv sestavni del revizijskega postopka IS, bi jo bilo treba časovno načrtovati hkrati z drugimi koraki, ki jih je treba izvesti pri vsakem pregledu. Na določeno nadaljnjo obravnavo in na čas in trajanje teh dejavnosti lahko vplivajo izidi pregleda, določijo pa se lahko po posvetovanju z linijskim poslovodstvom.

2.4.4 Pri določenem poročilu se lahko potem obravnavajo izvajanja vseh odgovorov poslovodstva kljub različnim datumom njihove uvedbe, za katere se je poslovodstvo zavezalo. Drug pristop pa je, da se potem obravnavajo posamezni odgovori poslovodstva glede na datume njihove izvedbe, dogovorjene s poslovodstvom.

2.5 Odlaganje nadaljnje obravnave

2.5.1 Revizor IS je zadolžen za pripravo časovnega razporeda nadaljnje obravnave kot dela razporejanja dela pri pripravi zadolžitev. Časovni razpored nadaljnjih obravnav naj temelji na vsebovanem tveganju in izpostavljenosti ter na stopnji težavnosti in pomembnosti rokov za izvedbo popravljalnih ukrepov.

2.5.2 Lahko se tudi zgodi, da revizor IS presodi, da ustni ali pisni odgovor poslovodstva kaže, da glede na sorazmerno pomembnost opažanja ali priporočila zadostuje že sprejeti ukrep. V takih okoliščinah se dejanska nadaljnja obravnava za potrditev stanja lahko izvede kot del naslednjega posla, ki bo obravnaval zadevni sistem ali zadevo.

2.6 Oblika odzivanja na nadaljnjo obravnavo

2.6.1 Najuspešnejši način za sprejemanje odzivov poslovodstva na nadaljnjo obravnavo je odgovor v pisni obliki, saj to pomaga utrditi in potrditi odgovornost poslovodstva za ukrepanje in dosežen napredek v nadaljnji obravnavi. Pisni odgovori tudi zagotavljajo natančen zapis ukrepov, odgovornosti in trenutnega stanja. Revizor IS lahko sprejme tudi ustne odgovore in jih sam zapiše, te zapise pa naj, če je le mogoče, potrdi še poslovodstvo. Odgovoru je lahko priloženo tudi dokazilo o ukrepanju ali izvajanju priporočil.

2.6.2 Revizor IS lahko zahteva in/ali prejema od poslovodstva obdobne tekoče podatke za ovrednotenje napredka, ki ga je poslovodstvo doseglo pri izvajanju dogovorjenih ukrepov, zlasti v zvezi z zelo tveganimi zadevami in popravnimi ukrepi, ki potrebujejo več časa za dokončanje.

2.7 Vrsta in obseg nadaljnje obravnave

2.7.1 Običajno bo revizor IS zahteval od organizacije stanje nadaljnje obravnave kmalu po predlaganem datumu uvedbe nekaterih ali vseh dogovorjenih ukrepov. To lahko vključuje tudi preoblikovanje končnega poročila, tako da dobi organizacija v njem prostor, v katerem lahko dokumentira podrobnosti ukrepov, sprejetih za izvajanje priporočila.

2.7.2 Organizacija bo običajno dobila časovni okvir, v katerem mora odgovoriti s podrobnimi podatki o ukrepih, sprejetih za izvajanje priporočila.

2.7.3 Odgovor poslovodstva s podrobnimi podatki o sprejetih ukrepih naj, če je le mogoče, ovrednoti revizor IS, ki je izvajal prvotni pregled. Kadar koli je to mogoče, bi bilo treba pridobiti tudi revizijske dokaze o sprejetih ukrepih. Na primer dokazilo, da so bili postopki dokumentirani, ali dokazilo, da je bilo izdelano ustrezno poročilo poslovodstva.

2.7.4 Kadar poslovodstvo daje informacije o sprejetih ukrepih za izvajanje priporočila in revizor IS dvomi v dane informacije ali uspešnost sprejetega ukrepa, naj opravi ustrezne preizkuse ali druge revizijske postopke, da pred dokončanjem nadaljnje obravnave potrdi dejanski položaj ali stanje.

2.7.5 Kot del nadaljnje obravnave naj revizor IS oceni, ali so neizvedeni izsledki še ustrezni ali pomembnejši. Revizor IS lahko odloči, da izvedba določenega priporočila ni več primerna. To se lahko zgodi, če so se spremenili aplikacijski sistemi, če so bile vpeljane kompenzacijske kontrole ali če so se spremenili poslovni cilji ali prednostne naloge, tako da je prvotno tveganje uspešno odpravljeno ali bistveno zmanjšano. Na enak način pa lahko sprememba v okolju IS poveča pomembnost učinka nekega prejšnjega opažanja in potrebo po njegovi rešitvi.

2.7.6 Morda bo treba načrtovati posel nadaljnje obravnave, da se preveri izvajanje kritičnih/pomembnih ukrepov.
2.7.7 Mnenje revizorja IS o nezadovoljivih odgovorih ali ukrepih poslovodstva je treba sporočiti vodstvu na ustrezni ravni.

2.8 Sprejetje tveganj s strani poslovodstva

2.8.1 Poslovodstvo je odgovorno za odločanje o ustreznem ukrepanju v odgovor na opažanja in priporočila iz poročila o poslu. Revizor IS je odgovoren za ocenjevanje ustreznosti ukrepanja poslovodstva in pravočasnosti rešitev zadev, navedenih kot opažanja in priporočila v poročilu o poslu.
2.8.2 Višje poslovodstvo se lahko odloči, da sprejme tveganje, če se stanje zaradi stroškov ali drugih premislekov ne popravi. Nadzorni svet (ali revizijsko komisijo, če obstaja) je treba obvestiti o odločitvi višjega poslovodstva glede vseh bistvenih opažanj in priporočil posla.
2.8.3 Kadar je revizor IS prepričan, da je organizacija sprejela višino preostalega tveganja, ki za organizacijo ni ustrezna, se mora revizor IS o zadevi pogovoriti z notranjo revizijo in višjim poslovodstvom. Če revizor IS ne soglaša z odločitvijo glede preostalega tveganja, morata revizor IS in višje poslovodstvo predložiti zadevo v reševanje nadzornemu svetu (ali revizijski komisiji, če obstaja).

2.9 Nadaljnja obravnava zunanje revizije s strani notranjega revizorja IS

2.9.1 Zadolžitve za nadaljnjo obravnavo za tekoče dejavnosti notranje revizije morajo biti dodeljene v revizijski listini za funkcijo notranje revizije IS, za druge revizijske naloge pa v listini o poslu.
2.9.2 Odvisno od obsega in pogojev posla in v skladu z ustreznimi standardi revidiranja IS se zunanji revizorji IS lahko zanesejo na funkcijo notranje revizije IS za izvajanje nadaljnje obravnave dogovorjenih priporočil.

3. Svetovalni posli

3.1 Svetovalni posli

3.1.1 Svetovalni posli ali storitve so lahko opredeljeni kot »dejavnosti svetovanja in sorodnih storitev za stranke, katerih vrsta in obseg sta dogovorjena s stranko in ki so namenjene dodani vrednosti in boljšemu delovanju organizacije. Primeri take dejavnosti so pravno in drugo svetovanje, omogočanje lažjega poslovanja, zasnova procesov in usposabljanje.« Vrsta in obseg posla morata biti dogovorjena pred začetkom posla.
3.1.2 Revizor IS naj spremlja izide svetovalnih poslov v obsegu, dogovorjenem z organizacijo. Različne vrste spremljanja so lahko ustrezne za različne vrste svetovalnih poslov. Temeljitost spremljanja je lahko odvisna od dejavnikov, kot so izrecen interes poslovodstva za izide posla ali ocena revizorja IS o tveganjih projekta in/ali s poslom ugotovljena možna dodatna vrednost za organizacijo.

4. Poročanje

4.1 Poročanje o nadaljnji obravnavi

4.1.1 Poročilo o stanju dogovorjenih popravnih ukrepov, ki izhajajo iz poročila o reviziji IS, vključno s še neizvedenimi dogovorjenimi priporočili, bi bilo treba predložiti revizijski komisiji, če je bila ta ustanovljena, sicer pa ustrezni ravni vodstva organizacije.
4.1.2 Če revizor IS med poznejšim poslom ugotovi, da ukrep, ki ga je poslovodstvo navedlo kot »uresničenega«, dejansko ni bil uresničen, je treba to sporočiti višjemu poslovodstvu in revizijski komisiji, če obstaja.
4.1.3 Če so bili izvedeni vsi dogovorjeni popravljalni ukrepi, se poročilo s podrobnostmi o vseh uvedenih/uresničenih ukrepih lahko pošlje višjemu poslovodstvu (ali revizijski komisiji, če ta obstaja).

5. Datum uveljavitve

5.1 Ta smernica velja za vse revizije informacijskih sistemov, ki se začnejo 1. marca 2006. Celoten pojmovnik izrazov lahko najdete na spletni strani ISACA na naslovu *www.isaca.org/glossary* (slovenski prevod je na naslovu *http://www.isaca.si/dokumenti/naslovka/ISACA_Glossary_Translation-SI_1303.pdf*)**.**

3. Orodja in tehnike dajanja zagotovil in revidiranja IS

Orodja in tehnike zagotavljajo dodatne primere za strokovnjake revidiranja in dajanja zagotovil. Ta razdelek lahko vključuje sklice na druge relevantne in zanesljive vire, kot tudi na ISACA:

- Bele knjige, *www.isaca.org/whitepapers* (brezplačne PDF datoteke);
- Programi revizije/dajanja zagotovil, *www.isaca.org/auditprograms* (brezplačne Word datoteke za člane ISACA);
- Družina produktov COBIT 5, *www.isaca.org/cobit;*
- Referenčne strokovne serije in serije o upravljanju tveganj, *www.isaca.org/Knowledge-Center/ITAF-IT-Assurance-Audit-/Pages/Reference-Series.aspx* (na voljo v ISACA Bookstore);
- Kolumne o osnovah revidiranja IT v Journal-u, IT Audit Basics, *www.isaca.org/Knowledge-Center/ITAF-IT-Assurance-Audit-/IT-Audit-Basics/Pages/IT-Audit-Basics-Articles.*aspx (brezplačen dostop);

Vsi izdelki raziskav ISACA so navedeni na strani *www.isaca.org/Knowledge-Center/Research/Pages/All-Deliverables.aspx.*

Za dodatne informacije o tem, kako dobiti določeno publikacijo ISACA, obiščite *www.isaca.org/bookstore ali pošljite e-mail bookstore@isaca.org*.

Obrazec za posredovanje pripomb
(Comment Submission Form)

Zanima nas vaš odziv na ITAF in kakršne koli dopolnitve/spremembe, ki bi jih lahko predlagali. Zagotovite prosim podrobne informacije o vašem predlogu, kot tudi razlog za spremembo. Svoje komentarje posredujte direktorju razvoja strokovnih standardov prek faksa na +1.847.253.1443, e-pošte *standards@isaca.org* ali po pošti na ISACA, 3701 Algonquin Road, Suite 1010, Rolling Meadows, IL 60008, USA, komentarje k prevodu pa tajniku odseka na *tajnik@isaca.si*.
We are interested in your reaction to ITAF and any additions/revisions you might suggest. Please provide detailed information about your suggestion as well as your rationale for the revision. Submit your comments to the attention of the director of professional standards development via fax at +1.847.253.1443, e-mail to standards@isaca.org or mail to ISACA, 3701 Algonquin Road, Suite 1010, Rolling Meadows, IL 60008, USA, and the comments regarding translation to tajnik@isaca.si.

Ime*/Name*: _____

Organizacija*/Organisation*: _____

Država*/Country:* _____ E-pošta*/E-mail*: _____

Razdelek*/Section*: _____

Predlagana sprememba*/Suggested revision*: _____

_____

_____

_____

_____

Razlog za spremembo*/Reason for the revision*: _____

_____

_____

_____

_____

_____

_____

_____

_____

_____

Hvala!/Thank you!

www.isaca.org

Delo je iz angleške različice ISACA® ITAF™: Okvir strokovnega ravnanja za dajanje zagotovil/revizijo IS, 2. izdaja,
s soglasjem ISACA v slovenščino prevedel Slovenski odsek ISACA.
Slovenski odsek ISACA prevzema vso odgovornost za pravilnost in skladnost prevoda z izvirnikom.
info@isaca.si | www.isaca.si