ITAF™

3. izdaja

Okvir strokovnega ravnanja za dajanje zagotovil/ revidiranje IS

Slovenski prevod

ISACA®

Zaupanje v informacijske sisteme in korist od njih

Slovenski odsek

About ISACA®

With more than 115,000 constituents in 180 countries, ISACA *(www.isaca.org)* helps business and IT leaders build trust in, and value from, information and information systems. Established in 1969, ISACA is the trusted source of knowledge, standards, networking, and career development for information systems audit, assurance, security, risk, privacy and governance professionals. ISACA offers the Cybersecurity Nexus™, a comprehensive set of resources for cybersecurity professionals, and COBIT®, a business framework that helps enterprises govern and manage their information and technology. ISACA also advances and validates business-critical 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™) credentials. The association has more than 200 chapters worldwide.

Disclaimer

ISACA has designed and created *ITAF™: A Professional Practices Framework for IS Audit/Assurance, 3rd 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, 3rd 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

© 2014 ISACA. All rights reserved. No part of this publication may be used, copied, reproduced, modified, distributed, displayed, stored in a retrieval system or transmitted in any form by any means (electronic, mechanical, photocopying, recording or otherwise) without the prior written authorisation of ISACA. Reproduction and use of all or portions of this publication are permitted solely for academic, internal and non-commercial use and for consulting/advisory engagements, and must include full attribution of the material's source. No other right or permission is granted with respect to this work.

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*

ITAF™: A Professional Practices Framework for IS Audit/Assurance, 3rd Edition

ISACA®

ISACA® *(www.isaca.org)* ima več kot 115.000 članov v 180 državah. Vodjem poslovanja in IT pomaga ustvarjati zaupanje v informacije in informacijske sisteme in korist od njih. Ustanovljena je bila leta 1969 in je zaupanja vreden vir znanja, standardov, mreženja in priložnosti za razvoj kariere za strokovnjake revidiranja, dajanja zagotovil, varnosti, tveganj, zasebnosti in upravljanja informacijskih sistemov (IS). ISACA ponuja Cybersecurity Nexus™, celovit skupek virov za strokovnjake za varnost na internetu, in COBIT®, poslovni okvir, ki podjetjem pomaga upravljati in ravnati z njihovimi informacijami in tehnologijo. ISACA tudi razvija in potrjuje poslovno-kritične veščine in znanje s svetovno priznanimi nazivi 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™). Združenje ima več kot 200 odsekov po vsem svetu.

Izjava o omejitvi odgovornosti

ISACA je zasnovala in ustvarila *ITAF™: Okvir strokovnega ravnanja za dajanje zagotovil/revidiranje IS, 3. 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 enakih 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/revidiranje IS, 3. 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

© 2014 ISACA. Vse pravice pridržane. Noben del te objave se ne sme uporabljati, kopirati, reproducirati, spreminjati, razpošiljati, prikazovati, shranjevati v sistemu za iskanje ali prenašati v kakršni koli obliki ali s kakršnimi koli sredstvi (elektronskimi, mehanskimi, fotokopiranjem, snemanjem ali drugače) brez predhodnega pisnega dovoljena ISACA. Reproduciranje celotnega gradiva ali njegovih delov je dovoljeno samo za akademske, interne in nekomercialne namene ter za svetovalne/posvetovalne posle, pri čemer je treba v celoti navesti avtorske pravice. V zvezi s tem gradivom ni dana nobena druga pravica ali dovoljenje.

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 na naslov: *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/revidiranje IS, 3. izdaja – slovenski prevod; december 2014

Zahvale

ISACA se želi zahvaliti:

Upravnemu odboru ISACA
Tony Hayes, CGEIT, AFCHSE, CHE, FACS, FCPA, FIIA, Vlada Queenslanda, Avstralija, 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
Ramses Gallego, CISM, CGEIT, CCSK, CISSP, SCPM, 6 Sigma Black Belt, Dell, Španija, podpredsednik
Theresa Grafenstine, CISA, CGEIT, CRISC, CGAP, CGMA, CIA, CPA, Predstavniški dom ZD, ZDA, podpredsednik
Vittal Raj, CISA, CISM, CGEIT, CFE. CIA, CISSP, FCA, Kumar & Raj, Indija, podpredsednik
Jeff Spivey, CRISC, CPP, PSP, Security Risk Management Inc., ZDA, podpredsednik
Marc Vael, Ph.D., CISA, CISM, CGEIT, CRISC, CISSP, Valuendo, Belgija, podpredsednik
Gregory T. Grocholski, CISA, The Dow Chemical Co., ZDA, prejšnji mednarodni predsednik
Kenneth L. Vander Wal, CISA, CPA, Ernst & Young LLP (upokojen), ZDA, prejšnji mednarodni predsednik
Christos K. Dimitriadis, Ph.D., CISA, CISM, CRISC, INTRALOT S.A., Grčija, 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
Bernard Battistin, CISA, CMA, Urad generalnega revizorja Kanade, Kanada
Richard Brisebois, CISA, CGA, Kanada
Terry Chrisman, CGEIT, CRISC, GE Money, ZDA
Erik Friebolin, CISA, CISM, CRISC, CISSP, PCI-QSA, ITIL, ZDA
Frank Nielsen, CISA, CGEIT, CCSA,CIA, Nordea, Danska
Hitoshi Ota, CISA, CISM, CGEIT, CRISC, CIA, Mizuho Corporate Bank, Japonska
Carmen Ozores Fernandes, CISA, CRISC, Brazilija
Steven E. Sizemore, CISA, CIA, CGAP, Texas Health and Human Services Commission, ZDA

Komisiji za strokovne standarde in upravljanje kariere
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 LLC, ZDA
Alisdair McKenzie, CISA, CISSP, ITCP, I S Assurance Services, Nova Zelandija
Kameswara Rao Namuduri, Ph.D., CISA, CISM, CISSP, University of North Texas, ZDA
Katsumi Sakagawa, CISA, CRISC, PMP, JIEC Co. Ltd., Japonska
Ian Sanderson, CISA, CRISC, FCA, NATO, Belgija
Timothy Smith, CISA, CISSP, CPA, LPL Financial, ZDA
Todd Weinman, CPS, The Weinman Group, ZDA

Zahvala strokovnjakom, ki so pregledali prevod

ITAF™: Okvir strokovnega ravnanja za dajanje zagotovil/revidiranje IS, 2. in 3. izdaja, sta v slovenščino za Slovenski odsek prevedla poklicna prevajalca, prevod pa so pregledali prostovoljci. V 2. izdaji so bili prevedeni in pregledani prenovljeni standardi, v 3. izdaji pa nove smernice. Vsem članom ISACA in drugim, ki so sodelovali pri pregledu prevedenega Okvira, se najlepše zahvaljujemo.

Strokovnjaki, ki so pregledali prevod standardov:
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

Strokovnjaki, ki so pregledali prevod smernic:
mag. Matija Debelak
mag. Marko Jagodic, CISA, CRISC
Boža Javornik, CISA, CISM
mag. Boštjan Kežmah, CISA
Tadej Kosmačin, CISA
mag. Jožica Kržič, CISA
Martina Toman Pfajfar, CRMA
Janja Zidarn, CRISC

Vsebina

Uvod 6

Kodeks poklicne etike ISACA 9

1. Standardi dajanja zagotovil in revidiranja IS 10
- **Zahteve standardov** 10
- **Splošni standardi** 13
  - 1001 Revizijska listina 14
  - 1002 Organizacijska neodvisnost 15
  - 1003 Strokovna neodvisnost 16
  - 1004 Upravičeno pričakovanje 17
  - 1005 Potrebna poklicna skrbnost 18
  - 1006 Strokovna usposobljenost 19
  - 1007 Trditve 20
  - 1008 Merila 21
- **Izvedbeni standardi** 23
  - 1201 Načrtovanje posla 24
  - 1202 Ocenjevanje tveganja pri načrtovanju 25
  - 1203 Izvedba in nadzor 27
  - 1204 Pomembnost 29
  - 1205 Dokazi 31
  - 1206 Uporaba dela drugih strokovnjakov 33
  - 1207 Nepravilnosti in nezakonita dejanja 34
- **Standardi poročanja** 36
  - 1401 Poročanje 37
  - 1402 Nadaljnja obravnava 39

2. Smernice dajanja zagotovil in revidiranja IS 40
- **Splošne smernice** 40
  - 2001 Revizijska listina 41
  - 2002 Organizacijska neodvisnost 45
  - 2003 Strokovna neodvisnost 49
  - 2004 Upravičeno pričakovanje 57
  - 2005 Potrebna poklicna skrbnost 61
  - 2006 Strokovna usposobljenost 65
  - 2007 Trditve 70
  - 2008 Merila 75
- **Izvedbene smernice** 79
  - 2201 Načrtovanje posla 80
  - 2202 Ocenjevanje tveganja pri revizijskem načrtovanju 85
  - 2203 Izvedba in nadzor 92
  - 2204 Pomembnost 99
  - 2205 Dokazi 104
  - 2206 Uporaba dela drugih strokovnjakov 109
  - 2207 Nepravilnosti in nezakonita dejanja 114
  - 2208 Vzorčenje 121
- **Smernice poročanja** 127
  - 2401 Poročanje 128
  - 2402 Nadaljnja obravnava 134

3. Orodja in tehnike dajanja zagotovil in revidiranja IS 139

Uvod

ITAF je celovit referenčni model vzpostavljanja dobre prakse, ki:
- vzpostavlja standarde, ki obravnavajo vloge in odgovornosti strokovnjakov dajanja zagotovil in revidiranja informacijskih sistemov (odslej IS), strokovno znanje in veščine, skrbnost, ravnanje in zahteve glede poročanja;
- opredeljuje pojme in koncepte, specifične za dajanje zagotovil v zvezi z IS;
- daje navodila, 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 navodila, raziskujejo usmeritve in postopke, pridobijo programe revidiranja in dajanja zagotovil ter sestavijo uspešna poročila.

Druga izdaja ITAF-a je vključevala ISACA standarde in navodila za dajanje zagotovil in revidiranje IS, veljavne od 1. novembra 2013. Tretja izdaja ITAF-a vključuje smernice, ki veljajo od 1. septembra 2014. Ko bodo pripravljena in izdana nova navodila, bodo uvrščena v obstoječi okvir.

Odbor ISACA za strokovne standarde in upravljanje kariere je zavezan k obširnemu posvetovanju pri pripravi standardov in navodil za dajanje zagotovil in revidiranje IS. Pred izdajo kateregakoli dokumenta se na mednarodni ravni izda osnutek za splošno javno razpravo. Osnutek za razpravo vključuje spletni vprašalnik, ki bo na voljo na spletni strani *www.isaca.org/standardexposure*. Mnenja lahko pošljete tudi direktorju razvoja strokovnih standardov po e-pošti *standards@isaca.org*.

Pogosta 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 širšo javnost, vključno z uporabniki poročil o dajanju zagotovil in reviziji IS.
- **Kdaj je uporaba ITAF-a primerna?** Uporaba okvira 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 standardi ITAF in z njimi povezana navodila za dajanje zagotovil in revidiranje IS?** Zasnova ITAF-a upošteva, da se strokovnjaki dajanja zagotovil in revidiranja IS srečujejo z različnimi zahtevami in vrstami nalog, od vodenja revizije, osredotočene na IS, do sodelovanja pri finančni reviziji ali reviziji poslovanja. 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 strank opravljajo posle svetovanja in posvetovanja. Rezultat teh nalog so 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, takšno delo ne velja za revizijo; zato strokovnjak dajanja zagotovil in revidiranja IS ne izda uradnega 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 in revidiranja IS. Veljajo za izvajanje vseh nalog in obravnavajo etiko, neodvisnost, nepristranskost in potrebno skrbnost, pa tudi strokovno znanje, usposobljenost in veščine 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 zagotavljajo strokovnjaku za dajanje zagotovil in revidiranje IS informacije in navodila na področju dajanja zagotovil in revidiranja IS. Skladno z navedenimi tremi kategorijami standardov se smernice osredotočajo na različne revizijske pristope, metodologije in s tem povezana gradiva, ki zagotavljajo pomoč pri načrtovanju, izvajanju, 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 tistimi, ki jih izvaja IT.

Tudi smernice ITAF dajanja zagotovil in revidiranja IS se 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; dajejo navodila za njihovo uporabo in so namenjena operacionalizaciji informacij iz navodil. 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 navodila o sistemih za načrtovanja virov podjetja (ERP).

Skladno z zasnovo ITAF kot živega dokumenta so med številkami poglavij namerno vrzeli za prihodnja navodila.

Uporaba ITAF

Standardi so v vseh primerih obvezni. Glagol »morati« označuje obveznost, nujnost. Vsakršna morebitna odstopanja je treba 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 vse opustitve ustreznih poglavij navodil 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 treba njihovo uporabo vedno proučiti.

Orodja in tehnike predstavljajo dopolnilno gradivo in informacije za dodatno pomoč navodilom. 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 strokovnjaku za dajanje zagotovil in revidiranje IS omogočajo pridobitev primernih, ustreznih, 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*.

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

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

Vsaka naloga dajanja zagotovil ali revidiranja IS je neločljivo povezana z več ključnimi predpostavkami, ki so med drugim:
- obravnavano zadevo je mogoče opredeliti in revidirati,
- obstaja velika verjetnost uspešnega dokončanja projekta,
- pristop in metodologija sta nepristranska,
- obseg projekta je zadosten za izpolnitev ciljev dajanja zagotovil in revidiranja IS,
- projekt bo zaključen z nepristranskim, nezavajajočim poročilom.

Standardi, ki jih izdajajo drugi organi za standardizacijo

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

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

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

Kadar strokovnjak za dajanje zagotovil in revidiranje IS navede skladnost s standardi ITAF, vendar obstajajo neskladnosti med standardi ITAF in drugimi navedenimi standardi, bi moral strokovnjak dajanja zagotovil in revidiranja IS pri izvajanju pregledov in poročanju o rezultatih kot prevladujoče standarde uporabiti standarde ITAF, razen če so drugi standardi zahtevani s predpisom.

Izrazi in pomeni

V celotnem dokumentu se uporabljajo običajne besede, ki imajo določen pomen. Za zagotovitev razumljivosti in dosledno uporabo izrazov ter 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-Slo.pdf*).

Pomeni izrazov veljajo za najpogostejše vrste poslov, ki jih izvaja strokovnjak za dajanje zagotovil in revidiranje IS. Ti pomeni so skladni s tistimi, ki jih določata Ameriški inštitut preizkušenih javnih računovodij (AICPA) in Odbor za Mednarodne standarde revidiranja in dajanja zagotovil (IAASB). Vendar naj bi strokovnjaki upoštevali najnovejše izvorne standarde, ki veljajo za določeno vrsto posla, ki ga bodo izvedli. Tako bodo zagotovili, da sledijo najnovejšim, ustreznim strokovnim standardom.

Kodeks poklicne etike ISACA

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

Člani in imetniki nazivov ISACA morajo:

1. podpirati vpeljavo ustreznih standardov in postopkov, namenjenih učinkovitemu vodenju in upravljanju informacijskih sistemov in tehnologij podjetja, vključno z revidiranjem, nadzorovanjem, upravljanjem varnosti in tveganj, ter spodbujati skladnost z njimi;
2. opravljati svoje naloge nepristransko, s potrebno prizadevnostjo in poklicno skrbnostjo, ter skladno s strokovnimi standardi;
3. delovati na zakonit način v interesu deležnikov, pri tem pa vzdrževati visoke standarde ravnanja in osebnostnih lastnosti in ne ogrožati ugleda stroke ali združenja;
4. varovati zasebnost in zaupnost informacij, pridobljenih med opravljanjem nalog, razen če razkritje zahteva pravosodni organ; takšnih informacij ne smejo uporabljati za osebno korist in izdajati neustreznim strankam;
5. ohranjati usposobljenost na svojem področju in sprejemati samo tiste naloge, za katere lahko upravičeno pričakujejo, da jih bodo uspešno opravili s potrebnimi veščinami, znanjem in usposobljenostjo;
6. obveščati ustrezne stranke o rezultatih opravljenega dela, vključno z razkritjem vseh pomembnih dejstev, ki jih poznajo, in bi nerazkrita lahko izkrivila poročanje o rezultatih;
7. podpirati strokovno izobraževanje deležnikov z namenom izboljšanja njihovega razumevanja vodenja in upravljanja informacijskih sistemov ter tehnologij podjetja, vključno z revidiranjem, nadzorovanjem, upravljanjem varnosti in tveganj.

Če se član ali imetnik naziva ISACA ne ravna po Kodeksu poklicne etike, se proti njemu lahko uvede preiskava o njegovem ravnanju in na koncu 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 poudarjene s **krepkim tiskom**, kjer se zahteva skladnost**.** Standarde ITAF je treba redno pregledovati zaradi zagotavljanja nenehnih izboljšav in po potrebi dopolnjevati, da sledijo nastajajočim izzivom na področju dajanja zagotovil in revidiranja IS.

Zahteve standardov

Za lažje sklicevanje 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 po mišljenju kot po zaznavi neodvisni in nepristranski v vseh zadevah, povezanih s posli revidiranja in dajanja zagotovil.

1004 Upravičeno pričakovanje

1004.1 Strokovnjaki dajanja zagotovil in revidiranja IS morajo upravičeno pričakovati, da je posel lahko 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 upravičeno pričakovati, da je glede na obseg posla možno sklepati o obravnavani zadevi in obravnavati kakršne koli omejitve.

1004.3 Strokovnjaki dajanja zagotovil in revidiranja IS morajo upravičeno pričakovati, da se poslovodstvo zaveda obveznosti in zadolžitev pri zagotavljanju primernih, ustreznih in pravočasnih informacij, ki so potrebne za izvedbo posla.

1005 Potrebna poklicna skrbnost

1005.1 Strokovnjaki dajanja zagotovil in revidiranja IS morajo pri načrtovanju in izvajanju poslov ter poročanju o izidih ravnati s potrebno poklicno skrbnostjo, vključno z upoštevanjem veljavnih strokovnih standardov za revizijo.

1006 Strokovna usposobljenost

1006.1 Strokovnjaki dajanja zagotovil in revidiranja IS morajo imeti 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 imeti s sodelavci pri nalogi 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, da bi ugotovili, ali je mogoče takšne trditve revidirati in ali so te trditve zadostne, veljavne in ustrezne.

1008 Merila

1008.1 Strokovnjaki dajanja zagotovil in revidiranja IS morajo izbrati merila, po katerih se bo obravnavana zadeva presojala, ki so nepristranska, popolna, ustrezna, merljiva, razumljiva, splošno priznana, predpisana ter na voljo vsem bralcem in uporabnikom poročila.

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

Izvedba

1201 Načrtovanje posla

1201.1 Strokovnjaki dajanja zagotovil in revidiranja IS morajo načrtovati vsak posel dajanja zagotovil in revidiranja IS z namenom, da obravnavajo:
- 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 značilna za posel,
- zahteve glede dokumentacije in poročanja.

1201.2 Strokovnjaki dajanja zagotovil in revidiranja IS morajo pripraviti in dokumentirati projektni načrt posla dajanja zagotovil ali 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 pripravo celotnega načrta revidiranja IS in določitev prednosti za učinkovito dodelitev virov za revizijo IS uporabljena ustrezen pristop in pripadajoča metodologija za oceno tveganja.

1202.2 Strokovnjaki dajanja zagotovil in revidiranja IS morajo pri načrtovanju posameznih poslov prepoznati in oceniti tveganje, ki se nanaša na področje pregleda.

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

1203 Izvedba in nadzor

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

1203.2 Za doseganje revizijskih ciljev in spoštovanje veljavnih strokovnih revizijskih standardov 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 upravičeno pričakujejo, da bodo veščine pridobili med izvajanjem 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 pomanjkanje kontrol in pretehtati, ali bi bila posledica teh slabosti ali pomanjkanja kontrol lahko pomembna pomanjkljivost ali bistvena 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 ali slabosti kontrol in možnost, da se pomanjkanje kontrol prevede v pomembno pomanjkljivost ali bistveno slabost.

1204.4 Strokovnjaki dajanja zagotovil in revidiranja IS morajo v poročilu razkriti:
- 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 proučiti 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, 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, ki niso člani skupine za posel, 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, v katerih 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, če 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 ustrezne 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, nepristranskost in potrebno skrbnost, pa 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 revidiranja IS upoštevati merila, po katerih bo izvajal nalogo (standardi) in v primerjavi s katerimi bo obravnavano zadevo ocenil (merila).

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

Standardi so tukaj vključeni v celoti. Podčrtane besede so opredeljene v poglavju z izrazi. 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 ali 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.

Izrazi

Izraz	Pomen
Posel dajanja zagotovil	Nepristransko preiskovanje dokazov, da bi ocenili postopke upravljanja tveganja, kontroliranja ali upravljanja podjetja. Opomba glede obsega: primeri lahko vključujejo posle v zvezi s financami, uspešnostjo, skladnostjo in varnostjo sistema.
Revizijska listina	Dokument, ki ga odobrijo pristojni za upravljanje in opredeljuje namen, pristojnost in zadolžitve notranje revizije za dajanje zagotovil in revidiranja IS. Revizijska listina naj bi: • vzpostavila položaj notranje revizije za dajanje zagotovil in revidiranja IS v podjetju, • odobrila dostop do zapisov, osebja ter prostorov in opreme, ki so pomembni za opravljanje poslov dajanja zagotovil in revidiranja IS, • določila 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 aktivnosti, ki so namenjene doseganju določenega niza povezanih ciljev.
Neodvisnost	Osvobojenost od okoliščin, ki ogrožajo nepristranskost ali zaznano nepristranskost. Grožnje za nepristranskost 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;
- razkrilo podrobnosti o oslabitvi primernim strankam, če je neodvisnost poslabšana dejansko ali po zaznavi
- se izogibalo nerevizijskim vlogam v pobudah v zvezi z IS, ki niso povezane z revidiranjem in zahtevajo prevzem upravljavskih zadolžitev, saj lahko takšne vloge ogrozijo prihodnjo neodvisnost;
- v revizijski listini ali listini o poslu obravnavalo neodvisnost in odgovornosti revidiranja.

Izrazi

Izraz	Pomen
Oslabitev	Stanje, ki povzroča slabost ali zmanjšano sposobnost za doseganje revizijskih ciljev. Oslabitev organizacijske neodvisnosti in nepristranskosti 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 nepristranskost ali zaznano nepristranskost. Grožnje za nepristranskost 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 so ogroženi poštenost, nepristranskost ali poklicna nezaupljivost podjetja, funkcije 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, nepristranskost in poklicno nezaupljivost.
Nepristranskost	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 po mišljenju kot po zaznavi neodvisni in nepristranski 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 naj bi bili hkrati ves čas zaznani kot neodvisni;
- 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.

Izrazi

Izraz	Pomen
Oslabitev	Stanje, ki povzroča slabost ali zmanjšano sposobnost za doseganje revizijskih ciljev. Oslabitev organizacijske neodvisnosti in nepristranskosti 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 nepristranskost ali videz nepristranskosti. Grožnje za nepristranskost je treba obvladovati na ravni posameznega revizorja, posla, funkcije ali organizacije. Neodvisnost vključuje neodvisnost mišljenja in zaznano neodvisnost.
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 so ogroženi poštenost, nepristranskost 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, nepristranskost in poklicno nezaupljivost.
Nepristranskost	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 upravičeno pričakovati, da je posel lahko 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 upravičeno pričakovati, da je glede na obseg posla možno sklepati o obravnavani zadevi in obravnavati kakršne koli omejitve.

1004.3 Strokovnjaki dajanja zagotovil in revidiranja IS morajo upravičeno pričakovati, da se poslovodstvo zaveda obveznosti in zadolžitev pri zagotavljanju primernih, ustreznih 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 obravnavali vsakršne omejitve posla, ki ga je treba izvesti, vključno z dostopom do primernih, ustreznih in pravočasnih informacij;
- proučili, 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 poslovodstvo 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.

Izrazi

Izraz	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 so izjeme, ki skupaj predstavljajo pomembno pomanjkljivost (vendar ne bistvene slabosti); • **odklonilno mnenje** – ugotovljena je ena 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 Potrebna poklicna skrbnost

Zahteve

1005.1 Strokovnjaki dajanja zagotovil in revidiranja IS morajo pri načrtovanju in izvajanju poslov ter poročanju o izidih ravnati s potrebno poklicno skrbnostjo, vključno z upoštevanjem veljavnih strokovnih standardov za revizijo.

Ključna pojasnila

Strokovnjaki dajanja zagotovil in revidiranja IS naj bi:

- posle opravljali pošteno in skrbno;
- 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 z upoštevanjem njihovega razvoja;
- članom skupine sporočili njihove vloge in odgovornosti ter zagotavljali, da bo skupina upoštevala ustrezne standarde pri izvajanju posla;
- obravnavali vse nejasnosti v zvezi z uporabo standardov med izvajanjem posla;
- ves čas opravljanja posla ohranjali učinkovito komunikacijo z ustreznimi 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: potrebna poklicna skrbnost pomeni primerno skrb in usposobljenost, ne pa nezmotljivosti ali izjemne uspešnosti.

Izrazi

Izraz	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 Potrebna 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 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 imeti s sodelavci pri nalogi 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 ne 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 za uspešno in učinkovito izvedbo 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.

Izrazi

Izraz	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, da bi ugotovili, ali je mogoče takšne trditve revidirati in ali so te trditve zadostne, veljavne in ustrezne.

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 nepristranske in merljive analize;
- zagotovili, da trditve ustrezajo pričakovanjem bralca ali uporabnika z zadostnim znanjem, kadar jih primerja z drugimi predpisanimi standardi, če je trditve oblikovalo poslovodstvo;
- zagotovili, da je trditve preverilo in potrdilo poslovodstvo, če so trditve pripravile 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.

Izrazi

Izraz	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, po katerih se bo obravnavana zadeva presojala, ki so nepristranska, popolna, ustrezna, merljiva, razumljiva, splošno priznana, predpisana ter na voljo vsem bralcem in uporabnikom poročila.

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

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 nepristranskega mnenja ali sklepa, ki ne bo zavajal bralca ali uporabnika. Znano je, da lahko poslovodstvo določi merila, ki ne izpolnjujejo vseh zahtev;
- proučili primernost in razpoložljivost meril, kot jih določa zahtevnost posla;
- če merila niso na voljo, so nepopolna ali predmet osebne razlage, v poročilo dodatno vključili še besedilo, v katerem so merila uporabljena, ter opis in kakršne koli druge informacije, ki so potrebne za zagotovitev poštenosti, nepristranskosti in razumljivosti poročila.

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

- **nepristranskost** – 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, ki bi pri izvedbi lahko vplivala na strokovno oceno pri izvajanju dajanja zagotovil in revidiranja IS;
- **ustreznost** – merila naj bi bila ustrezna 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 naj bi jih zadevni uporabniki ne razlagali preveč različno.

Na sprejemljivost meril vpliva njihova razpoložljivost uporabnikom strokovnega poročila, tako da lahko razumejo podlago za dajanje zagotovil ter ustreznost 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;
- **predpisana** – poiskati bi bilo treba merila, ki izražajo veljavna uradna načela znotraj področja in ustrezajo zadevi. Uradna 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 strokovni 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 razpoložljivosti naj bi se pri izbiri meril za dajanje zagotovil IS upošteval tudi 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. V drugih primerih pa so lahko ustrezna merila panožnih ali trgovinskih združenj. Možni viri meril, navedeni po vrstnem redu 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; razvili so jih 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 tolmačijo zakonodajo samo člani pravne stroke;
- **merila, ki jih določajo podjetja, ki ne sledijo predpisanim postopkom** – ta vključujejo ustrezna 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 nepristranskosti. Merila, pripravljena posebej za dajanje zagotovil in revidiranja IS, so pripravljena v obliki trditev.

Izbrana merila je treba skrbno proučiti. Čeprav je upoštevanje lokalnih zakonov in predpisov pomembno in jih je treba upoštevati kot 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 izpolnjevati. 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.

Izrazi

Izraz	Pomen
Merila	Standardi in merila uspešnosti, ki se uporabljajo za merjenje in predstavitev obravnavane zadeve in na podlagi katerih revizor IS ovrednoti zadevo. Merila naj bi bila: • nepristranska – objektivna in brez predsodkov, • popolna – vključevala naj bi vse ustrezne dejavnike, ki vodijo do sklepa, • ustrezna – nanašala naj bi se na obravnavano zadevo, • merljiva – zagotavljala naj bi dosledno merjenje, • razumljiva. Pri poslih potrjevanja so to merila uspešnosti, s katerimi je mogoče preveriti pisne trditve poslovodstva glede obravnavane zadeve. Izvajalec pride do sklepa 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 poslih dajanja zagotovil in revidiranja IS. Ti standardi veljajo sicer za strokovnjake dajanja zagotovil in revidiranja IS, ki opravljajo katero koli nalogo dajanja zagotovil in revidiranja IS, vendar je skladnost pomembna zlasti pri opravljanju revizije. Zato 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:
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

Standardi so tukaj vključeni v celoti. Podčrtane besede so opredeljene v poglavju z izrazi. 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 obravnavajo:
- **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 značilna za posel,**
- **zahteve glede dokumentacije in poročanja.**

1201.2 Strokovnjaki dajanja zagotovil in revidiranja IS morajo pripraviti in dokumentirati projektni načrt posla dajanja zagotovil ali 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 navodila 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;
- pripravili 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 značilna za posel, 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, da bi jasno določili:
  – 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 ustreznih 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, da bi obravnavali zadeve, 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 zaradi 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 pripravo celotnega načrta revidiranja IS in določitev prednosti za učinkovito dodelitev virov za revizijo IS uporabljena ustrezen pristop in pripadajoča metodologija za oceno tveganja.

1202.2 Strokovnjaki dajanja zagotovil in revidiranja IS morajo pri načrtovanju posameznih poslov prepoznati in oceniti tveganje, ki se nanaša na področje pregleda.

1202.3 Strokovnjaki dajanja zagotovil in revidiranja IS morajo proučiti 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 nalog:

- 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 postopek ocenjevanja tveganj, ki ga uporablja organ nadzora;
- poskušali med načrtovanjem in izvajanjem revizije IS zmanjšati revizijsko tveganje na sprejemljivo raven ter izpolniti cilje revizije z ustrezno oceno z IS povezane obravnavane zadeve in povezanih kontrol;
- pri načrtovanju določenega postopka revidiranja IS upoštevali, da nižji kot je prag pomembnosti, natančnejša so revizijska pričakovanja in večje je revizijsko tveganje;
- za zmanjšanje pomembnejšega tveganja razširili obseg preizkusa kontrol (zmanjšanje tveganja pri nadzoru) in/ali razširili postopke preizkušanja podatkov (zmanjšanje tveganja pri odkrivanju), da bi pridobili dodatna zagotovila.

Izrazi

Izraz	Pomen
Revizijska listina	Dokument, ki ga odobrijo pristojni za upravljanje in opredeljuje namen, pristojnost in zadolžitve notranje revizije. Revizijska listina naj bi: • vzpostavila položaj notranje revizije v podjetju, • odobrila dostop do zapisov, osebja ter prostorov in opreme, ki so pomembni za opravljanje poslov dajanja zagotovil in revidiranja IS, • določila obseg aktivnosti revidiranja.
Revizijsko tveganje	Tveganje za sprejem nepravilnega sklepa na podlagi ugotovitev revizije zajema tri sestavine revizijskega tveganja: • tveganje pri kontroliranju, • tveganje pri odkrivanju, • tveganje pri delovanju.

1202 Ocenjevanje tveganja pri načrtovanju *(nadaljevanje)*

Izrazi

Izraz	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 pomembna 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 glede na dejanja, ki jih je poslovodstvo izvedlo ali bi jih lahko izvedlo (npr. uvajanje kontrol). Glejte tveganje pri kontroliranju.
Pomembnost	Revizijski koncept, ki zadeva pomembnost informacije glede na njen vpliv ali učinek na pregledovano področje. Izraz relativne pomembnosti ali pomembnosti za neko določeno zadevo v kontekstu posla ali 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 Strokovnjaki dajanja zagotovil in revidiranja IS morajo delo opraviti skladno z odobrenim načrtom revidiranja IS in v dogovorjenih rokih, da zajamejo prepoznana tveganja.

1203.2 Za doseganje revizijskih ciljev in spoštovanje veljavnih strokovnih revizijskih standardov 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 upravičeno pričakujejo, da bodo veščine pridobili med izvajanjem 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 posel članom skupine s spretnostmi in izkušnjami, ki ustrezajo zahtevam posla;
- v skupino za revizijo IS vključili zunanje izvajalce, 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 eden ali več članov skupine in nato pregleda drug usposobljen član skupine;
- 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 navedbe 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, pisne ali ustne.

1203 Izvedba in nadzor *(nadaljevanje)*

Povezava s standardi in smernicami

Vrsta	Naslov
Standard	1005 Potrebna 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 pomanjkanje kontrol in pretehtati, ali bi bila posledica teh slabosti ali pomanjkanja kontrol lahko pomembna pomanjkljivost ali bistvena 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 ali slabosti kontrol in možnost, da se pomanjkanje kontrol prevede v pomembno pomanjkljivost ali bistveno slabost.

1204.4 Strokovnjaki dajanja zagotovil in revidiranja IS morajo v poročilu razkriti:
- **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:
- uporabljali koncept pomembnosti pri:
  – načrtovanju in izvajanju posla,
  – ocenjevanju vpliva določenih elementov, postopkov, kontrol ali napak;

  Vsako pomanjkljivost, slabost ali pomanjkanje ustreznih usmeritev, postopkov in kontrol bi bilo treba presojati v posebnih okoliščinah posla.
- upoštevali opredelitve pomembnosti, kjer jih določa zakonodaja ali regulativni 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;
- upoštevali skupni učinek več napak ali nedelujočih kontrol pri ugotavljanju pomembnosti;
- upoštevali ne samo velikost, ampak tudi vrsto pomanjkljivosti pri kontroliranju ter posebne okoliščine pojavljanja pri ocenjevanju skupnega učinka na revizijsko mnenje ali sklep.

Izrazi

Izraz	Pomen
Revizijsko tveganje	Tveganje za sprejem nepravilnega sklepa na podlagi ugotovitev revizije zajemajo tri sestavine revizijskega tveganja: • 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 velja 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 se ne uporabljajo in/ali so neustrezne, • je posredovanje zadeve nadrejenim nujno. 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)*

Izrazi

Izraz	Pomen
Pomembnost	Revizijski koncept, ki zadeva pomembnost informacije glede na njen vpliv ali učinek na pregledovano področje. Izraz relativne pomembnosti ali pomembnosti za neko določeno zadevo v kontekstu posla ali 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, ki 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 usmeritvami;
- pripravili dokumentacijo, ki naj bo:
  - shranjena ter na voljo za določeno obdobje in v obliki, ki sta skladna z usmeritvami 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 preizkušanja 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 za izpolnitev 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 ovrednotijo njeno zanesljivost in postavijo zahteve za nadaljnje preverjanje. Na splošno velja, da je zanesljivost dokazov večja, kadar so ti:
  - v pisni obliki, in ne samo kot ustno izražena mnenja,
  - pridobljeni iz neodvisnih virov,
  - pridobljeni od strokovnjaka samega, in ne od revidirane enote,
  - potrjeni od neodvisne stranke,
  - v hrambi pri neodvisni stranki,
  - rezultat preiskovanja,
  - rezultat 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 točnosti in popolnosti 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 usmeritvami.

1205 Dokazi *(nadaljevanje)*

Izrazi

Izraz	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 proučiti 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, 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, ki niso člani skupine za posel, 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, v katerih 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, če 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 se lahko s tem izboljša 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;
- dokumentirali uporabo dela drugih strokovnjakov v poročilu.

Izrazi

Izraz	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 poslovodstvo ali delovna 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 ustrezna 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 pomembnih napak, pomanjkljivosti pri nadzoru ali napačne navedbe zaradi nepravilnosti in nezakonitih dejanj;
- načrtovali in izvajali postopke za preverjanje ustreznosti notranjih kontrol ter tveganja, da se poslovodstvo izogne kontrolam, ki so namenjene preprečevanju ali odkrivanju nepravilnosti in nezakonitih dejanj;
- ocenili, ali lahko ugotovljene napake, pomanjkljivosti pri nadzoru ali napačne navedbe kažejo na nepravilnost ali nezakonito dejanje. Če takšen znak 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 odgovornosti poslovodstva za načrtovanje in izvajanje notranjih kontrol za preprečevanje in 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 vodenja 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, o katerih so poročali poslovodstvu, pristojnim za upravljanje, regulatorjem in drugim.

1207 Nepravilnosti in nezakonita dejanja *(nadaljevanje)*

Izrazi

Izraz	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 zmerljivem 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 dajejo neposredna poročila o obravnavani zadevi ali pa poročajo o trditvah v zvezi z obravnavano zadevo in ali poročila temeljijo na delu, opravljenem na ravni pregleda ali preiskovanja.

Standarda poročanja sta:
1401 Poročanje
1402 Nadaljnja obravnava

Standarda sta tukaj vključena v celoti. Podčrtane besede so opredeljene v poglavju z izrazi. 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 in odgovore nanje ter njegove trditve;
- ugotovili, ali je revidiranec podpisal in datiral svoje navedbe, s čimer je označil potrditev obveznosti v zvezi s poslom;
- dokumentirali in obdržali v delovnem dokumentu vse pisne ali ustne navedbe, ki so jih prejeli med izvajanjem posla. Navedbe revidiranca naj bi za posle potrjevanja pridobili pisno, da je manjša možnost morebitnih nesporazumov;
- 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;
- opisali v poročilu bistvene ali pomembne slabosti in njihov vpliv na doseganje ciljev posla;
- obravnavali vsebino osnutka poročila z vodstvom obravnavanega področja pred zaključkom in izdajo poročila ter v končno poročilo vključili odziv vodstva 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 ter v poročilu razkrili, da so jih sporočili;
- navedli vsa ločena poročila v končnem poročilu;
- sporočili poslovodstvu revidiranca pomanjkljivosti notranjega kontroliranja, ki niso zelo pomembne, vendar ne brez posledic. V takšnih primerih naj bi pristojne za upravljanje ali odgovorni organ obvestili, da so te pomanjkljivosti notranjega kontroliranja sporočili poslovodstvu revidiranca;
- navedli standarde, ki veljajo pri izvajanju naloge, in po potrebi poročali o vsakršni neskladnosti s temi standardi.

1401 Poročanje *(nadaljevanje)*

Izrazi

Izraz	Pomen
Ustrezne 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 nepristranskega 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.
Primerne informacije	Ustrezne (tj. primerne za predvideni namen), zanesljive (tj. točne, preverljive in iz nepristranskega 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 ustrezne 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 vodstva učinkovito izvedeni ali da je poslovodstvo sprejelo tveganje neukrepanja.

Zunanji strokovnjaki dajanja zagotovil ali revidiranja IS se smejo zanašati na notranje revidiranje IS, da bo glede na obseg in pogoje posla nadaljevalo obravnavo 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:
- 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;
- procese, postopke, metodologije in pristope dajanja zagotovil in revidiranja IS, ki bi jih strokovnjak dajanja zagotovil in revidiranja IS moral upoštevati pri izvajanju aktivnosti dajanja zagotovil in revidiranja IS.

Splošne smernice

Splošne smernice so:
2001 Revizijska listina
2002 Organizacijska neodvisnost
2003 Strokovna neodvisnost
2004 Upravičeno pričakovanje
2005 Potrebna poklicna skrbnost
2006 Strokovna usposobljenost
2007 Trditve
2008 Merila

Smernice so tukaj vključene v celoti. Za povezave s posameznimi standardi obiščite *www.isaca.org/standard*.

2001 Revizijska listina

Smernica je predstavljena v naslednjih poglavjih:
1. Namen smernice in povezava s standardi
2. Vsebina smernice
3. Povezava s standardi in procesi v COBIT 5
4. Izrazi
5. Datum uveljavitve

1. Namen smernice in povezava s standardi

1.0 Uvod

V tem poglavju so razjasnjeni:
1.1 Namen smernice
1.2 Povezava s standardi
1.3 Uporaba izrazov 'revidiranje' in 'strokovnjaki'

1.1 Namen

1.1.1 Namen te smernice je pomagati strokovnjakom dajanja zagotovil in revidiranja IS pri pripravi revizijske listine. Revizijska listina določa namen, zadolžitve, pristojnosti in odgovornost pri dajanju zagotovil in revidiranju IS.

1.1.2 Strokovnjaki dajanja zagotovil in revidiranja IS naj bi upoštevali to smernico pri odločanju, kako izvajati standard, uporabiti strokovno presojo pri njegovi uporabi, utemeljiti vsako odstopanje in po potrebi poiskati dodatna navodila.

1.2 Povezava s standardi

1.2.1 Standard 1001 Revizijska listina
1.2.2 Standard 1002 Organizacijska neodvisnost
1.2.3 Standard 1003 Strokovna neodvisnost

1.3 Uporaba izrazov

1.3.1 V nadaljnjem besedilu:
- se 'dajanje zagotovil in revidiranje IS' imenuje 'revidiranje';
- se 'strokovnjaki dajanja zagotovil in revidiranja IS' imenujejo 'strokovnjaki'.

2. Vsebina smernice

2.0 Uvod

Poglavje o vsebini smernice je sestavljeno tako, da daje informacije o naslednjih ključnih temah posla dajanja zagotovil in revidiranja IS:
2.1 Pooblastilo
2.2 Vsebina revizijske listine

2.1 Pooblastilo

2.1.1 Strokovnjaki bi morali imeti jasno pooblastilo za izvedbo revidiranja. To pooblastilo je običajno dokumentirano v revizijski listini, ki naj bi jo uradno potrdili pristojni za upravljanje, npr. upravni odbor ali nadzorni svet in revizijska komisija. Kjer obstaja revizijska listina za revidiranje kot celoto, bi morala vsebovati tudi pooblastilo za dajanje zagotovil in revidiranje IS.

2.2 Vsebina revizijske listine

2.2.1 V revizijski listini naj bi bili jasno obravnavani štirje vidiki: namen, zadolžitev, pristojnost in odgovornost. Ti vidiki so opredeljeni v naslednjih poglavjih.

2.2.2 **Namen** revizijske listine in funkcije revidiranja naj bi vseboval naslednje točke:
- smotri/cilji revizijske listine, ki dajejo funkcijski in organizacijski okvir, v katerem deluje funkcija revidiranja;
- izjava o poslanstvu in cilji funkcije revidiranja, ki vnašajo strukturiran pristop za ovrednotenje in izboljšanje zasnove in operativne uspešnosti postopkov upravljanja tveganj, sistema notranjih kontrol in struktur vodenja informacijskih sistemov;
- obseg funkcije revidiranja, ki je lahko določen za celotno podjetje ali za določeno organizacijsko enoto v podjetju;
- upravljanje, ki podrobno določa organ, ki odobri revizijsko listino in revidiranje.

2001 Revizijska listina *(nadaljevanje)*

2.2.3 **Zadolžitev** funkcije revidiranja naj bi vsebovale naslednje točke:

- načela delovanja, ki podrobneje opisujejo in naštevajo različne cilje revidiranja;
- neodvisnost, ki podrobno opredeljuje izvajanje zahtev glede neodvisnosti funkcije revidiranja in strokovnjakov, kot je opisano v standardih 1002 Organizacijska neodvisnost in 1003 Strokovna neodvisnost;
- odnos do zunanje revizije, ki podrobno določa razmerje med funkcijo revidiranja in zunanjim revizorjem:
  – sestajanje z zunanjimi revizorji za uskladitev dela, da je čim manj podvajanja,
  – zagotavljanje dostopa do delovnega gradiva, dokumentacije in dokazov strokovnjakov,
  – upoštevanje načrtovanega dela zunanjih revizorjev pri pripravi revizijskega načrta za prihodnje obdobje;
- pričakovanja revidiranca, ki podrobno določajo storitve in izdelke, ki jih revidiranci lahko pričakujejo od revidiranja in strokovnjakov:
  – opis ugotovljenih težav, posledic in možnih rešitev, ki se nanašajo na področje zadolžitev revidiranca,
  – možnost vključitve odziva poslovodstva in popravljalnih ukrepov, sprejetih na podlagi ugotovitev v revizijskem poročilu. To vključuje tudi sklicevanja na zadevne sporazume o ravni storitev (SLA) za zadeve, kot so dostava poročil, odgovor na pritožbe revidiranca, kakovost storitve, pregled izvedbe, proces poročanja in dogovor o ugotovitvah;
- obveznosti revidiranca, ki podrobno določajo zadolžitve revidiranca, npr. vsi revidiranci bi morali biti na razpolago in pomagati revizijski funkciji in strokovnjakom pri izpolnjevanju dodeljenih zadolžitev;
- komuniciranje z revidiranci, ki podrobno določa pogostnost in komunikacijske kanale, po katerih bo potekala komunikacija.

2.2.4 **Pristojnost** funkcije revidiranja naj bi vsebovala naslednje točke:

- pravica dostopa strokovnjakov do pomembnih informacij, sistemov, zaposlenih in prostorov pri izvajanju revizijskega posla. Funkcija revidiranja, ki jo zastopajo strokovnjaki, je pri izvajanju revizijskega posla:
  – pooblaščena za popoln, prost in neomejen dostop do vsakega in vseh zapisov, dokumentacije, sistemov in lokacij in lahko za pridobitev dostopa za pomoč zaprosi poslovodstvo,
  – pristojna, da zahteva kakršne koli informacije od vsakega zaposlenega, svetovalca ali pogodbenega izvajalca;
- morebitne omejitve pristojnosti funkcije revidiranja in strokovnjakov;
- procesi, ki bodo revidirani in je za njihovo revizijo pristojna funkcija revidiranja; funkcija revidiranja lahko na primer sama določi postopke, ki jih bo revidirala, po revizijskem načrtu na podlagi ocene tveganj.

2.2.5 **Odgovornost** funkcije revidiranja naj bi vsebovala naslednje točke:

- organizacijska struktura, vključno z linijama poročanja organu nadzora in poslovodstvu; pri revidiranju naj bi bil na primer zagotovljen prost in neomejen dostop do organa nadzora in njegovih članov;
- poročanje, ki podrobno določa format, vsebino in prejemnike sporočila o izidu vsakega revizijskega posla, npr. funkcija revidiranja bo po vsakem revizijskem poslu izdala pisno revizijsko poročilo in ga razposlala ustreznim deležnikom, vključno z obsegom posla, izvedenimi ukrepi, ugotovitvami, priporočili, odzivom poslovodstva in sprejetimi popravljalnimi ukrepi;
- uspešnost funkcije revidiranja, ki podrobno določa redno poročanje o izvajanju revidiranja v primerjavi z revizijskim načrtom in proračunom; funkcija revidiranja bo na primer vsako četrtletje poročala organu nadzora o svojem namenu, zadolžitvah in pristojnosti ter o uspešnosti glede na revizijski načrt in proračun;
- skladnost s standardi, ki podrobno določa standarde, po katerih se bodo ravnali funkcija revidiranja in strokovnjaki; funkcija revidiranja in strokovnjaki se bodo na primer ravnali in delovali po vseh standardih in smernicah ISACA za dajanje zagotovil in revidiranje IS;
- proces zagotavljanja kakovosti (npr. pogovori, ankete o zadovoljstvu strank, pregledi uspešnosti izvedbe poslov) za boljše razumevanje potreb in pričakovanj revidirancev, pomembnih za funkcijo revidiranja. Po potrebi je treba te potrebe ovrednotiti glede na revizijsko listino zaradi izboljšanja storitve ali spremembe njene izvedbe ali revizijske listine. Neodvisni zunanji pregledi kakovosti omogočajo funkciji revidiranja, da oceni svojo skladnost z veljavnimi standardi, tveganje in kontrolni okvir podjetja, optimalno uporabo virov in uporabo dobrih praks. Neodvisen zunanji pregled kakovosti funkcije revidiranja bi bilo treba izvesti najmanj enkrat na pet let, da se vzdržuje skladnost s standardi ISACA za dajanje zagotovil in revidiranje IS;
- pravila kadrovanja za revizijske posle, npr. določitev najkrajšega možnega roka, pred katerim strokovnjaki ne bodo razporejeni na revizijske posle na področjih, na katerih so izvajali nerevizijske storitve, ki slabijo neodvisnost. V revizijski listini bi moralo biti tudi določeno, ali se strokovnjaki smejo vključevati v opravljanje nerevizijskih storitev ter katere so vrsta, čas in obseg takih storitev; s tem se zagotovi, da neodvisnost ni oslabljena. To bi lahko odpravilo ali zelo zmanjšalo potrebo, da je za vsako nerevizijsko storitev treba pridobiti posebno pooblastilo za vsak primer posebej;
- zaveza funkcije revidiranja za stalno izobraževanje strokovnjakov; funkcija revidiranja se na primer zaveže, da bo strokovnjakom zagotovila najmanj 40 ur usposabljanja na leto;
- dogovorjeno ukrepanje glede obnašanja funkcije revidiranja in strokovnjakov, na primer kazni, če ena ali druga stran ne izpolni svojih zadolžitev.

2001 Revizijska listina *(nadaljevanje)*

2.2 Vsebina revizijske listine (nadaljevanje)

2.2.6 Drugi vidiki, ki bi jih bilo treba upoštevati in dodati v revizijsko listino, so:

- pregledovanje ter spreminjanje in dopolnjevanje listine, kar je naloga funkcije revidiranja. Redno bi morali presojati, ali so namen, zadolžitve, pristojnosti in odgovornost, kot so opredeljene v revizijski listini, še ustrezni in o izidu presoje obveščati revizijsko komisijo;
- pridobitev odobritve sprememb in dopolnitev revizijske listine od pristojnih za upravljanje;
- vključevanje s tem povezanih dokumentov, kot so sklicevanja na zadevne standarde, smernice, usmeritve, okvire, priročnike itd.

3. Povezava s standardi in procesi v COBIT 5

3.0 Uvod

To poglavje daje pregled ustreznih:
3.1 Povezav s standardi
3.2 Povezav s procesi v COBIT 5
3.3 Drugih navodil

3.1 Povezava s standardi

V tabeli je pregled:

- najpomembnejših standardov ISACA za dajanje zagotovil in revidiranje IS, ki jih neposredno podpira ta smernica;
- tistih zahtev standardov, ki so najpomembnejše za to smernico.

Opomba: Naštete so samo tiste zahteve standardov, ki so pomembne za to smernico.

Naslov standarda	Pomembne zahteve standarda
1001 Revizijska listina	Pri dajanju zagotovil in revidiranju IS mora biti revidiranje ustrezno dokumentirano v revizijski listini, pri čemer morajo biti navedeni namen, zadolžitev, pristojnost in odgovornost. Pri dajanju zagotovil in revidiranju IS mora biti revizijska listina usklajena in potrjena na ustrezni ravni v podjetju.
1002 Organizacijska neodvisnost	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	Strokovnjaki dajanja zagotovil in revidiranja IS morajo biti tako po mišljenju kot po zaznavi neodvisni in nepristranski v vseh zadevah, povezanih s posli revidiranja in dajanja zagotovil.

3.2 Povezava s procesi v COBIT 5

V tabeli je pregled najpomembnejšega:

- procesa v COBIT 5,
- namena procesa v COBIT 5.

Posebne aktivnosti, ki se izvajajo kot del teh procesov, so v *COBIT 5: Omogočanje procesov*.

Proces v COBIT 5	Namen procesa
MEA02 Spremljajte, vrednotite in ocenjujte sistem notranjih kontrol.	Ključnim deležnikom omogočite pregled nad ustreznostjo sistema notranjih kontrol in s tem zagotovite zaupanje v delovanje, vero v doseganje ciljev podjetja in ustrezno razumevanje preostalega tveganja.

3.3 Druga navodila

Pri izvajanju standardov in smernic naj strokovnjaki po potrebi poiščejo še druga navodila. Za dajanje zagotovil in revidiranje IS jih lahko pridobijo:

- od kolegov v podjetju,
- od poslovodstva,
- od organov upravljanja v podjetju, npr. od revizijske komisije,
- od strokovnih organizacij,
- iz drugih strokovnih navodil (npr. knjig, člankov, drugih smernic).

2001 Revizijska listina *(nadaljevanje)*

4. Izrazi

Izraz	Pomen
Revizijska listina	Dokument, ki ga odobrijo pristojni za upravljanje in opredeljuje namen, pristojnost in zadolžitve notranje revizije za dajanje zagotovil in revidiranja IS. Revizijska listina naj bi: • vzpostavila položaj notranje revizije za dajanje zagotovil in revidiranja IS v podjetju, • odobrila dostop do zapisov, osebja ter prostorov in opreme, ki so pomembni za opravljanje poslov dajanja zagotovil in revidiranja IS, • določila 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 aktivnosti, ki so namenjene doseganju določenega niza povezanih ciljev.
Neodvisnost	Osvobojenost od okoliščin, ki ogrožajo nepristranskost ali zaznano nepristranskost. Grožnje za nepristranskost je treba obvladovati na ravni posameznega revizorja, posla, funkcije ali organizacije. Neodvisnost vključuje neodvisnost mišljenja in zaznano neodvisnost.

5. Datum uveljavitve

5.1 Datum uveljavitve Ta smernica velja za vse posle dajanja zagotovil in revidiranja IS, ki se začnejo 1. septembra 2014 ali pozneje.

2002 Organizacijska neodvisnost

Smernica je predstavljena v naslednjih poglavjih:
1. Namen smernice in povezava s standardi
2. Vsebina smernice
3. Povezava s standardi in procesi v COBIT 5
4. Izrazi
5. Datum uveljavitve

1. Namen smernice in povezava s standardi

1.0 Uvod

V tem poglavju so razjasnjeni:
1.1 Namen smernice
1.2 Povezava s standardi
1.3 Uporaba izrazov ‘revidiranje’ in ‘strokovnjaki’

1.1 Namen

1.1.1 Namen te smernice je obravnavati neodvisnost funkcije dajanja zagotovil in revidiranja IS v podjetju. Upoštevani so trije pomembni vidiki:
- položaj funkcije dajanja zagotovil in revidiranja IS v podjetju,
- raven, ki ji funkcija dajanja zagotovil in revidiranja IS poroča v podjetju,
- izvajanje nerevizijskih storitev v podjetju s strani vodstva in strokovnjakov dajanja zagotovil in revidiranja IS.

1.1.2 Ta smernica daje navodila za presojo organizacijske neodvisnosti in podrobno določa razmerje med organizacijsko neodvisnostjo ter revizijsko listino in revizijskim načrtom.

1.1.3 Strokovnjaki dajanja zagotovil in revidiranja IS naj bi upoštevali to smernico pri odločanju, kako izvajati standard, uporabiti strokovno presojo pri njegovi uporabi, utemeljiti vsako odstopanje in po potrebi poiskati dodatna navodila.

1.2 Povezava s standardi

1.2.1 Standard 1001 Revizijska listina
1.2.2 Standard 1002 Organizacijska neodvisnost
1.2.3 Standard 1003 Strokovna neodvisnost
1.2.4 Standard 1004 Upravičeno pričakovanje
1.2.5 Standard 1006 Strokovna usposobljenost

1.3 Uporaba izrazov

1.3.1 V nadaljnjem besedilu:
- se ‘dajanje zagotovil in revidiranje IS’ imenuje ‘revidiranje’;
- se ‘strokovnjaki dajanja zagotovil in revidiranja IS’ imenujejo ‘strokovnjaki’.

2. Vsebina smernice

2.0 Uvod

Poglavje o vsebini smernice je sestavljeno tako, da daje informacije o naslednjih ključnih temah posla dajanja zagotovil in revidiranja IS:
2.1 Položaj v podjetju
2.2 Raven poročanja
2.3 Nerevizijske storitve
2.4 Presoja neodvisnosti
2.5 Revizijska listina in revizijski načrt

2002 Organizacijska neodvisnost *(nadaljevanje)*

2.1 Položaj v podjetju

2.1.1 Da bi bila omogočena organizacijska neodvisnost, bi morala imeti funkcija revidiranja v podjetju položaj, ki ji omogoča opravljanje zadolžitev brez vmešavanja. To je mogoče doseči z:

- vzpostavitvijo funkcije revidiranja v revizijski listini kot neodvisne funkcije ali oddelka zunaj operativnih oddelkov. Funkciji revidiranja ne bi smele biti dodeljene nobene operativne zadolžitve ali aktivnosti;
- zagotavljanjem, da funkcija revidiranja poroča tisti ravni v podjetju, ki ji omogoča organizacijsko neodvisnost. Poročanje vodji operativnega oddelka bi lahko ogrozilo organizacijsko neodvisnost, kot je podrobneje opisano v poglavju 2.2.

2.1.2 Funkcija revidiranja se bi morala izogibati opravljanju nerevizijskih vlog in pobud za IS, ki zahtevajo prevzemanje poslovodnih zadolžitev, ker bi take vloge lahko oslabile njeno prihodnjo neodvisnost. Neodvisnost in odgovornost funkcije revidiranja bi morali biti obravnavani v revizijski listini, kot je opisano v standardu 1001 Revizijska listina.

2.2 Raven poročanja

2.2.1 Funkcija revidiranja bi morala poročati tisti ravni v podjetju, ki ji omogoča popolno organizacijsko neodvisnost pri delovanju. Neodvisnost naj bi bila opredeljena v revizijski listini in funkcija revidiranja bi jo morala redno, najmanj enkrat na leto potrditi poslovodstvu in pristojnim za upravljanje.

2.2.2 Za zagotavljanje organizacijske neodvisnosti funkcije revidiranja je treba pristojnim za upravljanje (npr. nadzornemu svetu) sporočati v vednost in/ali odobritev:

- načrt revizijskih virov in proračun,
- revizijski načrt (na podlagi tveganj),
- spremljanje uspešnosti, ki jo funkcija revidiranja izvaja za revidiranje IS,
- spremljanje pomembnih omejitev obsega ali virov.

2.2.3 Za zagotavljanje organizacijske neodvisnosti funkcije revidiranja je potrebna izrecna podpora organa nadzora in izvršnega vodstva.

2.3 Nerevizijske storitve

2.3.1 V mnogih podjetjih poslovodstvo in osebje IS pričakujejo, da se sme funkcija revidiranja vključevati v izvajanje nerevizijskih storitev. To vključuje sodelovanje strokovnjakov pri pobudah za IS in v projektnih skupinah za IS v svetovalnih ali posvetovalnih vlogah s polnim ali krajšim delovnim časom.

2.3.2 Na splošno velja, da rutinska in administrativna opravila ali aktivnosti v zvezi z manj pomembnimi zadevami niso vodstvene zadolžitve in zato ne slabijo neodvisnosti. Nerevizijske storitve, ki prav tako ne slabijo neodvisnosti ali nepristranskosti, če se izvajajo ustrezni zaščitni ukrepi, vključujejo rutinsko svetovanje o tveganju in kontrolah informacijske tehnologije.

2.3.3 Za nerevizijske storitve, navedene v nadaljevanju, pa velja, da slabijo neodvisnost in nepristranskost, ker bi bile z njimi povzročene grožnje tako pomembne, da jih nobeni zaščitni ukrepi ne bi mogli zmanjšati na sprejemljivo raven:

- prevzemanje upravljavskih zadolžitev ali izvajanje upravljavskih aktivnosti;
- pomembno vključevanje strokovnjakov v nadziranje ali izvajanje snovanja, razvijanja, preizkušanja, nameščanja, konfiguriranja ali delovanja informacijskih sistemov, ki so bistveni ali pomembni za obravnavano zadevo posla revidiranja ali dajanja zagotovil;
- snovanje kontrol za informacijske sisteme, ki so pomembni ali bistveni za obravnavano zadevo tekočih ali načrtovanih prihodnjih revizijskih poslov;
- delovanje v upravljavski vlogi, v kateri so strokovnjaki zadolženi za samostojno ali skupno sprejemanje poslovodnih odločitev ali potrjevanje usmeritev in standardov;
- svetovanje, ki je glavna podlaga za poslovodne odločitve.

2.3.4 Izvajanje nerevizijskih storitev na področjih, ki so ali bodo v prihodnosti obravnavana zadeva revizijskega posla, prav tako predstavlja grožnjo neodvisnosti, ki bi jo bilo z zaščitnimi ukrepi težko premagati. V taki situaciji bi lahko prišlo do zaznave, da sta zaradi opravljanja nerevizijskih storitev na tem področju oslabljeni tako neodvisnost kot nepristranskost funkcije revidiranja in strokovnjakov. Funkcija revidiranja in strokovnjaki bi morali ugotovili, ali je mogoče vpeljati ustrezne zaščitne ukrepe, ki bi dovolj ublažili take dejanske ali zaznane grožnje neodvisnosti.

2.3.5 Podrobnejša navodila za obvladovanje teh groženj neodvisnosti lahko najdete v standardu 1003 Strokovna neodvisnost in z njim povezani smernici 2003.

2002 Organizacijska neodvisnost *(nadaljevanje)*

2.4 Presoja neodvisnosti

2.4.1 Neodvisnost bi morali redno presojati funkcija revidiranja in strokovnjaki. Tako presojo je treba opraviti letno za funkcijo revidiranja in pred vsakim poslom za strokovnjake, kot je opisano v Standardu 1003 Strokovna neodvisnost. Pri presoji je treba upoštevati dejavnike, kot so:

- spremembe v osebnih razmerjih,
- finančni interesi,
- naloge in zadolžitve na prejšnjem delovnem mestu.

2.4.2 Funkcija revidiranja bi morala razkriti vsa morebitna vprašanja, povezana z organizacijsko neodvisnostjo, in se o njih pogovoriti z upravnim odborom/nadzornim svetom ali pristojnimi za upravljanje. Rešitev je treba najti in potrditi v revizijski listini ali revizijskem načrtu.

2.5 Revizijska listina in revizijski načrt

2.5.1 V revizijski listini bi moralo biti v okviru zadolžitev podrobno opredeljeno uveljavljanje organizacijske neodvisnosti funkcije revidiranja. Poleg podrobne opredelitve neodvisnosti bi morale biti v revizijski listini vključene tudi možne slabitve neodvisnosti.

2.5.2 Organizacijska neodvisnost bi se morala odražati v revizijskem načrtu. Funkciji revidiranja bi moralo biti omogočeno, da neodvisno določi obseg načrta brez omejitev s strani izvršnega vodstva.

3. Povezava s standardi in procesi v COBIT 5

3.0 Uvod

To poglavje daje pregled ustreznih:
3.1 Povezav s standardi
3.2 Povezav s procesi v COBIT 5
3.3 Drugih navodil

3.1 Povezava s standardi

V tabeli je pregled:

- najpomembnejših standardov ISACA, ki jih neposredno podpira ta smernica;
- tistih zahtev standardov, ki so najpomembnejše za to smernico.

Opomba: Naštete so samo tiste zahteve standardov, ki so pomembne za to smernico.

Naslov standarda	Pomembne zahteve standarda
1001 Revizijska listina	Pri dajanju zagotovil in revidiranju IS mora biti revidiranje ustrezno dokumentirano v revizijski listini, pri čemer morajo biti navedeni namen, zadolžitev, pristojnost in odgovornost. Pri dajanju zagotovil in revidiranju IS mora biti revizijska listina usklajena in potrjena na ustrezni ravni v podjetju.
1002 Organizacijska neodvisnost	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	Strokovnjaki dajanja zagotovil in revidiranja IS morajo biti tako po mišljenju kot po zaznavi neodvisni in nepristranski v vseh zadevah, povezanih s posli revidiranja in dajanja zagotovil.
1004 Upravičeno pričakovanje	Strokovnjaki dajanja zagotovil in revidiranja IS morajo upravičeno pričakovati, da je glede na obseg posla možno sklepati o obravnavani zadevi in obravnavati kakršne koli omejitve.
1006 Strokovna usposobljenost	Strokovnjaki dajanja zagotovil in revidiranja IS morajo imeti 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.

2002 Organizacijska neodvisnost *(nadaljevanje)*

3.2 Povezava s procesi v COBIT 5

V tabeli je pregled najpomembnejših:
- procesov v COBIT 5,
- namenov procesov v COBIT 5.

Posebne aktivnosti, ki se izvajajo kot del teh procesov, so v *COBIT 5: Omogočanje procesov*.

Proces v COBIT 5	Namen procesa
EDM01 Zagotovite postavitev in vzdrževanje okvira vodenja.	Zagotovite dosleden pristop, povezan in usklajen z načinom upravljanja podjetja. Da bodo odločitve za IT sprejete v skladu s strategijami in cilji podjetja, zagotovite, da so procesi, povezani z IT, uspešno in pregledno nadzorovani, da je skladnost z zakonskimi in drugimi predpisanimi zahtevami potrjena in da so izpolnjene upravljavske zahteve za člane organa nadzora.
APO01 Upravljajte okvir upravljanja IT.	Zagotovite dosleden način upravljanja, da omogočite izpolnitev zahtev za vodenje podjetja, ki vključujejo upravljavske procese, organizacijske strukture, vloge in zadolžitve, zanesljive in ponovljive aktivnosti ter veščine in sposobnosti.
MEA02 Spremljajte, vrednotite in ocenjujte sistem notranjih kontrol.	Ključnim deležnikom omogočite pregled nad ustreznostjo sistema notranjih kontrol in s tem zagotovite zaupanje v delovanje, vero v doseganje ciljev podjetja in ustrezno razumevanje preostalega tveganja.

3.3 Druga navodila

Pri izvajanju standardov in smernic naj strokovnjaki po potrebi poiščejo še druga navodila. Za dajanje zagotovil in revidiranje IS jih lahko pridobijo:
- od kolegov v podjetju in/ali zunaj njega, npr. prek strokovnih združenj ali strokovnih skupin na družbenih omrežjih,
- od poslovodstva,
- od organov upravljanja v podjetju, npr. od revizijske komisije,
- iz drugih strokovnih navodil (npr. knjig, strokovnih člankov, drugih smernic).

4. Izrazi

Izraz	Pomen
Neodvisnost	Osvobojenost od okoliščin, ki ogrožajo nepristranskost ali zaznano nepristranskost. Grožnje za nepristranskost je treba obvladovati na ravni posameznega revizorja, posla, funkcije ali organizacije. Neodvisnost vključuje neodvisnost mišljenja in zaznano neodvisnost.
Nepristranskost	Zmožnost nepristranskega presojanja, izražanja mnenja in podajanja priporočil.

5. Datum uveljavitve

5.1 Datum uveljavitve

Ta smernica velja za vse posle dajanja zagotovil in revidiranja IS, ki se začnejo 1. septembra 2014 ali pozneje.

2003 Strokovna neodvisnost

Smernica je predstavljena v naslednjih poglavjih:
1. Namen smernice in povezava s standardi
2. Vsebina smernice
3. Sklicevanja in preslikave
4. Izrazi
5. Datum uveljavitve

1. Namen smernice in povezava s standardi

1.0 Uvod

V tem poglavju so razjasnjeni:
1.1 Namen smernice
1.2 Povezava s standardi
1.3 Uporaba izrazov 'revidiranje' in 'strokovnjaki'

1.1 Namen

1.1.1 Namen te smernice je dati okvir, ki strokovnjaku dajanja zagotovil in revidiranja IS omogoča, da:
- ugotovi, kdaj bi bila neodvisnost lahko ali bi lahko bila zaznana kot oslabljena;
- razmisli o morebitnih drugih možnih pristopih k revidiranju, kadar je neodvisnost ali bi lahko bila zaznana kot oslabljena;
- zmanjša ali odpravi vpliv strokovnjakov dajanja zagotovil in revidiranja IS, ki opravljajo nerevizijske vloge, funkcije in storitve, na neodvisnost;
- določi zahteve za razkritja, kadar bi bila neodvisnost lahko ali bi lahko bila zaznana kot oslabljena.

1.1.2 Strokovnjaki dajanja zagotovil in revidiranja IS bi morali upoštevati to smernico pri odločanju, kako izvajati standard, uporabiti strokovno presojo pri uporabi, utemeljiti vsako odstopanje in po potrebi poiskati dodatna navodila.

1.2 Povezava s standardi

1.2.1 Standard 1002 Organizacijska neodvisnost
1.2.2 Standard 1003 Strokovna neodvisnost
1.2.3 Standard 1005 Potrebna poklicna skrbnost

1.3 Uporaba izrazov

1.3.1 V nadaljnjem besedilu:
- se 'dajanje zagotovil in revidiranje IS' imenuje 'revidiranje';
- se 'strokovnjaki dajanja zagotovil in revidiranja IS' imenujejo 'strokovnjaki'.

2. Vsebina smernice

2.0 Uvod

Poglavje o vsebini smernice je sestavljeno tako, da daje informacije o naslednjih ključnih temah posla dajanja zagotovil in revidiranja IS:
2.1 Miselni okvir
2.2 Grožnje in zaščitni ukrepi
2.3 Obvladovanje groženj
2.4 Nerevizijske storitve ali vloge
2.5 Nerevizijske storitve ali vloge, ki ne slabijo neodvisnosti
2.6 Nerevizijske storitve ali vloge, ki slabijo neodvisnost
2.7 Pomembnost neodvisnosti pri izvajanju nerevizijskih storitev ali vlog
2.8 Upravljanje dopustnosti nerevizijskih storitev ali vlog
2.9 Poročanje

2003 Strokovna neodvisnost *(nadaljevanje)*

2.1 Miselni okvir

2.1.1 Mnoge različne okoliščine ali kombinacije okoliščin so lahko pomembne pri presoji ogrožanja neodvisnosti. Nemogoče je opredeliti vsako situacijo, ki ogroža neodvisnost, in določiti ustrezno ukrepanje. Zato ta smernica vzpostavlja miselni okvir, ki zahteva, da strokovnjak prepozna, ovrednoti in rešuje grožnje za neodvisnost. Pristop miselnega okvira pomaga izpolnjevati standarde neodvisnosti in upošteva mnoge različne situacije in okoliščine, ki ustvarjajo grožnje za neodvisnost.

2.1.2 Strokovnjaki morajo uporabiti pristop miselnega okvira, da:
- prepoznajo grožnje za neodvisnost;
- ovrednotijo pomembnost prepoznane grožnje;
- po potrebi uporabijo zaščitne ukrepe, da grožnje odpravijo ali jih zmanjšajo na sprejemljivo raven.

2.1.3 Kadar strokovnjaki ugotovijo, da ustrezni zaščitni ukrepi niso na voljo ali jih ni mogoče uporabiti za odpravo ali zmanjšanje grožnje na sprejemljivo raven, morajo odpraviti okoliščino ali razmerje, ki ustvarja grožnje, ali pa odkloniti ali odpovedati posel revidiranja ali dajanja zagotovil. Če strokovnjaki ne morejo odkloniti ali odpovedati posla, morajo pristojnim za upravljanje ustrezno razkriti oslabitev neodvisnost in tako razkritje vnesti v vsako poročilo, ki izhaja iz posla.

2.1.4 Pri uporabi tega miselnega okvira morajo strokovnjaki uporabiti strokovno presojo.

2.1.5 Pomemben vidik pri uporabi okvira je posvetovanje. Strokovnjak dajanja zagotovil in revidiranja IS naj po potrebi prosi za navodila:
- kolege v podjetju,
- vodstvo,
- pristojne za upravljanje,
- ustrezne strokovne organizacije.

2.1.6 Čeprav ni nobene zahteve, da morajo biti strokovnjaki za opravljanje nerevizijskih storitev ali vlog neodvisni, pa je nepristranskost pri njihovem izvajanju še vedno poklicna zahteva. Strokovnjaki morajo upoštevati uporabo tega miselnega okvira, da prepoznajo grožnje za nepristranskost, ovrednotijo pomembnost groženj in izvajajo ustrezne zaščitne ukrepe pri opravljanju nerevizijskih storitev ali vlog.

2.2 Grožnje in zaščitni ukrepi

2.2.1 Grožnje so lahko posledica zelo različnih razmerij in okoliščin. Kadar neko razmerje ali okoliščina ustvari grožnjo, bi lahko taka grožnja slabila ali pa bila zaznana, da slabi strokovno neodvisnost. Neka okoliščina ali razmerje lahko predstavlja več kot eno samo grožnjo za neodvisnost. Grožnje spadajo v eno kategorijo ali več od teh kategorij:
- **lastni interes** – grožnja, da bo finančni ali kakšen drug interes neprimerno vplival na strokovno presojo ali obnašanje;
- **samopregled** – grožnja, da strokovnjaki ne bodo ustrezno ovrednotili izidov prej opravljene presoje ali storitve, ki so jo opravili sami ali nekdo drug v funkciji revidiranja, na katero se bodo strokovnjaki oprli pri presoji v okviru izvajanja tekočega posla;
- **zagovarjanje** – grožnja, da bodo strokovnjaki do te mere uveljavljali stališče revidiranca, da bo s tem prizadeta njihova strokovna nepristranskost;
- **domačnost** – grožnja, da bo strokovnjak zaradi dolgega ali tesnega razmerja do revidiranca preveč razumevajoč do njegovih interesov ali preveč pripravljen sprejeti delo, stališča ali argumente revidiranca;
- **ustrahovanje** – grožnja, da dejanski ali zaznani pritiski, vključno s poskusi neprimernega vplivanja, odvrnejo strokovnjake od neoporečnega ravnanja in nepristranskosti;
- **pristranskost** – grožnja, da bodo strokovnjaki zaradi političnega, ideološkega, družbenega, psihološkega ali drugega prepričanja postali pristranski;
- **sodelovanje pri upravljanju** – grožnja, ki izhaja iz okoliščin, da strokovnjaki prevzemajo vlogo vodstva ali drugače opravljajo upravljavske funkcije za organizacijo, v kateri se izvaja posel revidiranja ali dajanja zagotovil.

2.2.2 Zaščitni ukrepi so kontrole, zasnovane za odpravo groženj za neodvisnost ali njihovo zmanjšanje na sprejemljivo raven. Po miselnem okviru uporabijo strokovnjaki zaščitne ukrepe za obvladovanje določenih dejstev in okoliščin, iz katerih izvirajo grožnje za neodvisnost. V nekaterih primerih utegne biti potrebnih več zaščitnih ukrepov za reševanje ene grožnje.

Primeri zaščitnih ukrepov, ki jih strokovnjaki lahko upoštevajo kot odgovor na prepoznane grožnje, so:
- struktura vodenja v podjetju in funkciji revidiranja, ki zagotavlja ustrezen nadzor in sporočanje glede storitev dajanja zagotovil in revidiranja IS, ki jih je treba opraviti;
- zagotavljanje, da strokovnjaki (in vodstvo revidiranja IS) poročajo ustrezni hierarhični ravni v podjetju, po možnosti pristojnim za upravljanje;
- notranji postopki v podjetju in funkciji revidiranja, ki zagotavljajo nepristransko izbiro pri dodeljevanju poslov, npr. ustrezne zahteve glede izobrazbe, usposabljanja in izkušenj, zahteve za nenehen strokovni razvoj;

2003 Strokovna neodvisnost *(nadaljevanje)*

2.2 Grožnje in zaščitni ukrepi (nadaljevanje)

2.2.2 *(nadalj.)*

- dodeljevanje vodstva in osebja izven funkcije revidiranja, na primer izposoja osebja iz neke druge funkcije, oddelka ali zunanje organizacije za nadomeščanje strokovnjakov;
- ustrezen sistem spodbud (nagrad in kazni), ki strokovnjake nagrajuje za kritično in nepristransko mišljenje ter kaznuje pristranskost ali vnaprejšnjo sodbo;
- redno kroženje strokovnjakov pri nalogah revidiranja IS, kar zmanjšuje stopnjo domačnosti in samopregleda;
- ustrezni postopki zaposlovanja, kot so poizvedbe glede prejšnjih zaposlitev in preverjanje, kar bi lahko povečalo verjetnost, da strokovnjaki niso obremenjeni s pristranskostjo ali lastnim interesom;
- odstranitev posameznika iz skupine za revidiranje IS, kadar njegovi interesi ali razmerja ogrožajo neodvisnost;
- ustrezne zahteve glede dokumentacije in poročanja, ki zagotavljajo, da je presoja strokovne neodvisnosti dokumentirana v delovnem gradivu in dosledno vključena v poročila in rezultate;
- določitev člana strokovnega osebja ali vodstva funkcije revidiranja, ki ni bil član skupine za revidiranje IS, da skrbno pregleda opravljeno delo;
- dodelitev neodvisnega strokovnjaka funkcije revidiranja ali iz drugih prej omenjenih virov, da opravi strokovni pregled ali deluje kot neodvisni opazovalec med načrtovanjem, delom na terenu in poročanjem;
- naročilo zunanjega pregleda poročil, sporočil ali informacij, ki so jih pripravili strokovnjaki, pri priznani tretji stranki, npr. pri splošno sprejetem organu za to področje ali neodvisnem specialistu;
- oddaja posla dajanja zagotovil in revidiranja IS zunanjemu izvajalcu storitev.

2.3 Obvladovanje groženj

2.3.1 Dejstva in okoliščine, ki ustvarjajo grožnje za neodvisnost, so lahko posledica dogodkov, kot so začetek nove revizije, dodelitev novega osebja reviziji v teku in sprejetje nerevizijske storitve pri revidirani organizaciji. Tudi mnogi drugi dogodki lahko povzročijo grožnje za neodvisnost. Kadar koli strokovnjaki pri poslu revidiranja ali dajanja zagotovil zvedo nove informacije o grožnji za neodvisnost, morajo ponovno ovrednotiti pomembnost te grožnje v skladu z miselnim okvirom.

2.3.2 Strokovnjaki naj bi ovrednotili grožnje:

- za neodvisnost na podlagi miselnega okvira, kadar lahko dejstva in okoliščine, v katerih strokovnjaki opravljajo svoje delo, ustvarjajo nove grožnje ali povečajo pomembnost obstoječih groženj za neodvisnost;
- posamično in vse skupaj, ker imajo grožnje lahko skupni učinek na strokovno neodvisnost;
- kakovostno in količinsko, kadar določajo pomembnost grožnje.

2.3.3 Funkcija revidiranja in strokovnjaki morajo ugotoviti, ali so prepoznane grožnje za neodvisnost na sprejemljivi ravni oziroma so bile odpravljene ali zmanjšane na sprejemljivo raven. Grožnja za neodvisnost ni sprejemljiva, če bi lahko:

- vplivala na zmožnost strokovnjaka, da izvaja posel revidiranja ali dajanja zagotovil brez vplivov, ki ogrožajo strokovno presojo, ali
- izpostavila strokovnjake, funkcijo revidiranja ali revizijsko organizacijo okoliščinam, zaradi katerih bi razumna in dobro obveščena tretja stranka sklepala, da so bile neoporečnost, nepristranskost ali <u>poklicna nezaupljivost</u> revizijske organizacije ali člana skupine za dajanje zagotovil in revidiranje IS ogrožene.

2.3.4 Kadar funkcija revidiranja in strokovnjaki prepoznajo grožnje za neodvisnost in na podlagi ovrednotenja teh groženj ugotovijo, da grožnje niso na sprejemljivi ravni, morajo:

- ugotoviti, ali so na voljo ustrezni zaščitni ukrepi in jih je mogoče uporabiti za odpravo groženj ali njihovo zmanjšanje na sprejemljivo raven;
- pri tem ugotavljanju uporabiti strokovna presojo in upoštevati, ali sta ohranjena <u>neodvisnost mišljenja</u> in <u>zaznana neodvisnost</u>;
- poiskati navodila ustreznih strank, kot je opisano v točki 2.1.5, da prepoznajo in uporabijo ustrezne zaščitne ukrepe.

2.3.5 Dokumentacija daje dokaze o presojah strokovnjakov pri oblikovanju sklepov glede skladnosti z zahtevami za neodvisnost.

2.3.6 Strokovnjaki morajo dokumentirati sklepe glede skladnosti z zahtevami za neodvisnost in glavno vsebino vseh razprav z vodstvom revizije in po potrebi s pristojnimi za upravljanje v podporo teh sklepov, med drugim:

- ukrepe, sprejete za proučitev narave neodvisnosti,
- dejansko naravo vprašanja neodvisnosti,
- seznam in opis groženj,
- sprejeti končni sklep,
- vzpostavljene zaščitne ukrepe za odpravo ali zmanjšanje groženj na sprejemljivo raven.

2003 Strokovna neodvisnost *(nadaljevanje)*

2.4 Nerevizijske storitve ali vloge

2.4.1 V mnogih podjetjih poslovodstvo, osebje IS in notranja revizija pričakujejo, da so strokovnjaki lahko vključeni v izvajanje nerevizijskih storitev ali vlog, kot so:
- določitev strategij IS v zvezi s področji, kot so tehnologija, aplikacije in viri,
- ocenjevanje, izbira in uvedba tehnologij,
- ocenjevanje, izbira, prilagajanje ter uvajanje aplikacij in rešitev IS tretjih strank,
- zasnova, razvoj in uvedba po meri izdelanih aplikacij in rešitev IS,
- vzpostavitev dobrih praks, usmeritev in postopkov v zvezi z različnimi funkcijami IT,
- zasnova, razvoj, preizkušanje in uvedba varnosti in kontrol IT,
- upravljanje projektov IT.

2.4.2 Izvajanje nerevizijskih storitev ali vlog na splošno vključuje sodelovanje pri pobudah in v projektnih skupinah IT v svetovalni ali posvetovalni vlogi, s polnim ali krajšim delovnim časom. Strokovnjaki dajanja zagotovil in revidiranja IS lahko izpolnjujejo nerevizijske naloge z izvajanjem aktivnosti, kot so:
- izvajanje začasne naloge s polnim delovnim časom ali posojanje osebja za dajanje zagotovil in revidiranje IS projektni skupini za IT;
- dodelitev 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 (ad hoc) delovanje v vlogi svetovalca ali pregledovalca posameznih projektov ali kontrol IT.

2.4.3 Izvajanje nerevizijskih storitev ali vlog lahko ogrozi strokovno neodvisnost mišljenja in zaznano neodvisnost, ki jo je zlasti težko premagati z zaščitnimi ukrepi, če je področje, na katerem so bile izvedene nerevizijske storitve ali vloge, že sedaj ali pa bo v prihodnosti postalo obravnavana zadeva posla revidiranja ali dajanja zagotovil. V taki situaciji utegne priti do zaznave, da sta zaradi opravljanja nerevizijskih storitev ali vlog oslabljeni neodvisnost in nepristranskost strokovnjakov.

2.4.4 Strokovnjaki, ki izvajajo nerevizijske storitve ali vloge, morajo z uporabo miselnega okvira oceniti, ali so nerevizijske storitve ali vloge oslabile njihovo neodvisnost, bodisi mišljenja ali zaznano, za sedanje ali prihodnje posle revidiranja ali dajanja zagotovil. To velja za posle, pri katerih je področje, na katerem se izvajajo nerevizijske storitve ali vloga, bistveno ali <u>pomembno</u> za obravnavano zadevo ali deležnike teh poslov. Po potrebi morajo strokovnjaki dobiti navodilo od kolegov in vodstva dajanja zagotovil in revidiranja IS in tudi od pristojnih za upravljanje, da ugotovijo, ali je mogoče izvesti ustrezne zaščitne ukrepe za primerno ublažitev kakršne koli dejanske ali zaznane grožnje za neodvisnost.

2.4.5 Preden začnejo izvajati nerevizijske storitve ali vloge, morajo strokovnjaki ugotoviti in dokumentirati razumevanje le-teh pri vodstvu revidiranja IS in/ali pristojnih za upravljanje, kot je primerno, glede na:
- cilje nerevizijskih storitev ali vlog,
- vrste nerevizijskih storitev ali vlog, ki jih je treba izvesti,
- sprejemanje zadolžitev v zvezi z nerevizijskimi storitvami ali vlogami s strani revidirane enote,
- strokovne zadolžitve, povezane z nerevizijskimi storitvami ali vlogami,
- kakršne koli omejitve nerevizijskih storitev ali vlog,
- kakršne koli omejitve obsega prihodnjih revizijskih storitev, ki jih strokovnjaki lahko izvajajo.

2.4.6 V primeru posla dajanja zagotovil ali revidiranja IS, pri katerem obstaja možnost za oslabljeno neodvisnost mišljenja ali zaznano neodvisnost zaradi opravljenih nerevizijskih storitev ali vlog, mora vodstvo dajanja zagotovil in revidiranja IS uvesti zaščitne ukrepe, kot so:
- skrbno spremljanje vodenja revizije,
- ocenjevanje vseh pomembnih znakov oslabitve neodvisnosti mišljenja ali zaznane neodvisnosti, ki izhajajo iz opravljenih nerevizijskih storitev ali vlog, in uvedba potrebnih zaščitnih ukrepov,
- seznanitev pristojnih za upravljanje o možni oslabitvi neodvisnosti mišljenja ali zaznane neodvisnosti in uvedenih zaščitnih ukrepih.

2003 Strokovna neodvisnost *(nadaljevanje)*

2.5 Nerevizijske storitve ali vloge, ki ne slabijo neodvisnosti

2.5.1 Aktivnosti, ki so rutinske in administrativne ali vključujejo na splošno manj pomembne zadeve, ne veljajo za upravljavske naloge in naj bi zato ne slabile neodvisnosti. Prav tako svetovanje in priporočila za pomoč poslovodstvu pri opravljanju njegovih zadolžitev ne velja za prevzemanje upravljavske odgovornosti.

2.5.2 Nerevizijska storitev ali vloga, ki prav tako ne bi oslabila neodvisnosti ali nepristranskosti, če se izvajajo ustrezni zaščitni ukrepi, je med drugim tudi rutinsko svetovanje o tveganju in kontrolah IT.

2.5.3 Da bi se izognili tveganju prevzemanja upravljavske odgovornosti pri izvajanju nerevizijskih storitev ali vlog na področju, ki je ali bi lahko postalo obravnavana zadeva posla revidiranja ali dajanja zagotovil, smejo strokovnjaki opravljati nerevizijske storitve ali vloge le, če so dobili ustrezna zagotovila, da poslovodstvo v zvezi z nerevizijskimi storitvami ali vlogami izvaja ali bo izvedlo:

- prevzem vseh upravljavskih zadolžitev,
- nadzor nad storitvami z imenovanjem osebe, po možnosti iz poslovodstva, ki ima za to primerne sposobnosti, znanje ali izkušnje,
- ovrednotenje ustreznosti in izidov opravljenih storitev,
- sprejetje odgovornosti za izide storitev.

Strokovnjaki morajo dokumentirati svoje premisleke o zmožnosti vodstva, da uspešno nadzoruje nerevizijske storitve ali vloge, ki jih je treba opraviti.

2.6 Nerevizijske storitve ali vloge, ki slabijo neodvisnost

2.6.1 Če bi morali strokovnjaki prevzemati poslovodne zadolžitve ali izvajati poslovodne aktivnosti, bi grožnje za neodvisnost lahko postale tako pomembne, da jih nobeni zaščitni ukrepi ne bi mogli zmanjšati na sprejemljivo raven. Ali je neka aktivnost poslovodna zadolžitev ali ne, je odvisno od okoliščin in zahteva strokovno presojo. Primeri aktivnosti, ki bi jih na splošno šteli za poslovodne zadolžitve, so med drugim:

- določanje politik in strateške usmeritve,
- usmerjanje in prevzemanje odgovornosti za ukrepanje zaposlenih v enoti,
- odobravanje poslov,
- odločanje o tem, katera priporočila funkcije revidiranja, notranje revizije, revizijske organizacije, podjetja ali drugih tretjih strank je treba izvesti,
- prevzemanje odgovornosti za zasnovo, uvedbo ali vzdrževanje notranje kontrole,
- sprejemanje odgovornosti za upravljanje projekta ali pobude za IT.

2.6.2 Poleg prevzemanja upravljavskih zadolžitev tudi za navedene nerevizijske storitve ali vloge v nadaljevanju velja, da slabijo neodvisnost in nepristranskost:

- pomembno vključevanje strokovnjakov v nadziranje ali izvajanje snovanja, razvijanja, preizkušanja, nameščanja, konfiguriranja ali upravljanja informacijskih sistemov, ki so pomembni ali bistveni za obravnavano zadevo posla revidiranja ali dajanja zagotovil;
- snovanje kontrol za informacijske sisteme, ki so pomembne ali bistvene za obravnavano zadevo posla revidiranja ali dajanja zagotovil;
- delo v upravljavski vlogi, v kateri so strokovnjaki zadolženi za samostojno ali skupno sprejemanje poslovodnih odločitev ali potrjevanje usmeritev in standardov;
- svetovanje, ki je glavna podlaga za poslovodne odločitve ali opravljanje poslovodnih funkcij.

2.7 Pomembnost neodvisnosti pri izvajanju nerevizijskih storitev ali vlog

2.7.1 Če ni prepovedi v drugih zunanjih standardih ali zakonodaji, ni nobene zahteve, da strokovnjaki dejansko so ali da so vsaj videti neodvisni pri izvajanju nalog v zvezi z opravljanjem nerevizijskih storitev ali vlog; še vedno pa ostaja nepristranskost poklicna zahteva. Zato morajo biti strokovnjaki pri izvajanju naloge v zvezi z nerevizijskimi storitvami ali vlogami nepristranski in strokovni.

2.7.2 Čeprav ni zahtevano, da morajo biti strokovnjaki pri opravljanju nerevizijske storitve ali vloge neodvisni, morajo strokovnjaki proučiti, ali bi bila njihova neodvisnost lahko oslabljena, če so dodeljeni izvajanju posla revidiranja ali dajanja zagotovil, pri katerem je področje, na katerem izvajajo ali so izvajali nerevizijske storitve ali vloge, pomembno za obravnavano zadevo posla. Kadar je tako možnost oslabitve mogoče predvideti (npr. kadar bo neodvisna revizija zahtevana pozneje in je na voljo samo en strokovnjak s potrebnim znanjem in izkušnjami za izvajanje tako nerevizijskih storitev ali vlog kot tudi poznejše revizije), mora strokovnjak zahtevati navodila od vodstva revizije in po potrebi pristojnih za upravljanje, preden sprejme ali opravlja nerevizijske storitve ali vloge.

2003 Strokovna neodvisnost *(nadaljevanje)*

2.7 Pomembnost neodvisnosti pri izvajanju nerevizijskih storitev ali vlog (nadaljevanje)

2.7.3 Odločanje o tem, ali morajo strokovnjaki izvajati nerevizijske storitve ali vloge, kadar je tekoči ali naslednji posel revidiranja ali dajanja zagotovil za področje, na katerem se izvajajo nerevizijske storitve ali vloge, načrtovan ali ga bo verjetno opravil isti strokovnjak, mora biti prepuščeno vodstvu revidiranja IS v dogovoru s pristojnimi za upravljanje. Vodstvo revizije IS mora pri odločanju uporabiti miselni okvir, na odločitev pa lahko vplivajo tudi naslednji dejavniki:

- strokovnjaki ne smejo revidirati svojega dela ali izvajati nerevizijskih storitev ali vlog za področja, za katera se ve, da so pomembna ali ki bodo verjetno pomembna za obravnavano zadevo poslov dajanja zagotovil ali revidiranja IS, v katere so ali bodo vključeni;
- ali so na voljo viri za ločeno izvajanje tako nerevizijskih nalog kot tudi neodvisne funkcije revidiranja in dajanja zagotovil;
- kako vodstvo IS in pristojni za upravljanje dojemajo vrednost ali pomembnost nerevizijskih storitev ali vlog v razmerju do posla revidiranja in dajanja zagotovil;
- raven tveganja za funkcijo revidiranja, povezano z nerevizijskimi storitvami ali vlogami;
- morebitni učinek odločitve na zahteve zunanjih revizorjev ali upravnih organov;
- določbe revizijske listine za IS.

2.8 Upravljanje dopustnosti nerevizijskih storitev ali vlog

2.8.1 V revizijski listini za IS mora biti določeno, ali je strokovnjakom dovoljeno vključevanje v opravljanje nerevizijskih storitev ali vlog, navedene morajo biti širše vrste, čas in obseg takih storitev ali vlog, tako bi bilo zagotovljeno, da ni oslabljena neodvisnost glede na sisteme, ki jih utegnejo revidirati. To bi lahko odpravilo ali zelo zmanjšalo potrebo po pridobitvi posebnih pooblastil za vsako nerevizijsko storitev ali vlogo za vsak primer posebej.

2.8.2 Strokovnjaki morajo dati sprejemljivo zagotovilo, da so naloge in pristojnosti posameznih nerevizijskih storitev ali vlog skladne z revizijsko listino. V primeru kakršnih koli odstopanj morajo biti ta izrecno navedena v opisu nalog in pristojnosti, odobriti pa jih morajo vodstvo dajanja zagotovil in revidiranja IS in/ali pristojni za upravljanje.

2.8.3 Kadar v revizijski listini nerevizijske storitve ali vloge niso natančno navedene ali kadar revizijske listine ni, morajo strokovnjaki o vrsti svojega vključevanja v nerevizijske storitve ali vloge poročati vodstvu dajanja zagotovil in revidiranja IS in pristojnim za upravljanje. Čas in obseg vključevanja strokovnjakov v nerevizijske storitve ali vloge morata biti vpisana v osebni opis nalog in pristojnosti, ki ga podpiše vodstvo funkcije, v okviru katere se bodo storitve ali vloge izvajale, odobriti pa ju morajo pristojni za upravljanje.

2.9 Poročanje

2.9.1 Kadar bi neodvisnost strokovnjakov glede na posel revidiranja ali dajanja zagotovil IS lahko bila dejansko ali dozdevno oslabljena ali če je oslabljena in so se pristojni za upravljanje odločili posel nadaljevati, morajo biti v poročilo o poslu dajanja zagotovil in revidiranja IS vključene zadostne informacije, da bi lahko uporabniki poročila razumeli naravo morebitne oslabitve. Informacije, o katerih razkritju v poročilu o poslu dajanja zagotovil in revidiranja IS bi morali strokovnjaki razmisliti, so med drugim:

- imena in položaj strokovnjakov, vključenih v posel revidiranja ali dajanja zagotovil IS, katerih neodvisnost je morda bila ali se morda zdi, da je bila oslabljena;
- analiza in opis grožnje za neodvisnost;
- zaščitni ukrepi, uvedeni za odpravo ali ublažitev različnih groženj za neodvisnost in nepristranskost med izvajanjem posla in v procesu poročanja o poslu;
- dejstvo, da je bila morebitna oslabitev neodvisnosti razkrita pristojnim za upravljanje, in njihova odobritev izvajanja ali nadaljevanja posla dajanja zagotovil in/ali nerevizijskih storitev ali vlog.

3. Povezava s standardi in procesi v COBIT 5

3.0 Uvod

To poglavje daje pregled ustreznih:
3.1 Povezav s standardi
3.2 Povezav s procesi v COBIT 5
3.3 Drugih navodil

Naštete so samo pomembne zahteve standardov.

2003 Strokovna neodvisnost *(nadaljevanje)*

3.1 Povezava s standardi

V tabeli je pregled:
- najpomembnejših standardov ISACA, ki jih neposredno podpira ta smernica;
- tistih zahtev standardov, ki so najpomembnejše za to smernico.

Opomba: Naštete so samo tiste zahteve standardov, ki so pomembne za to smernico.

Naslov standarda	Pomembne zahteve standarda
1001 Revizijska listina	Pri dajanju zagotovil in revidiranju IS mora biti revidiranje ustrezno dokumentirano v revizijski listini, pri čemer morajo biti navedeni namen, zadolžitev, pristojnost in odgovornost. Pri dajanju zagotovil in revidiranju IS mora biti revizijska listina usklajena in potrjena na ustrezni ravni v podjetju.
1002 Organizacijska neodvisnost	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	Strokovnjaki dajanja zagotovil in revidiranja IS morajo biti tako po mišljenju kot po zaznavi neodvisni in nepristranski v vseh zadevah, povezanih s posli revidiranja in dajanja zagotovil.
1005 Potrebna poklicna skrbnost	Strokovnjaki dajanja zagotovil in revidiranja IS morajo pri načrtovanju in izvajanju poslov ter poročanju o izidih ravnati s potrebno poklicno skrbnostjo, vključno z upoštevanjem veljavnih strokovnih standardov za revizijo.

3.2 Povezava s procesi v COBIT 5

V tabeli je pregled najpomembnejših:
- procesov v COBIT 5,
- namenov procesov v COBIT 5.

Posebne aktivnosti, ki se izvajajo kot del teh procesov, so v *COBIT 5: Omogočanje procesov*.

Proces v COBIT 5	Namen procesa
MEA02 Spremljajte, vrednotite in ocenjujte sistem notranjih kontrol.	Ključnim deležnikom omogočite pregled nad ustreznostjo sistema notranjih kontrol in s tem zagotovite zaupanje v delovanje, vero v doseganje ciljev podjetja in ustrezno razumevanje preostalega tveganja.
MEA03 Spremljajte, vrednotite in ocenjujte skladnost z zunanjimi zahtevami.	Zagotovite, da podjetje ravna v skladu z vsemi veljavnimi zunanjimi zahtevami.

3.3 Druga navodila

Pri izvajanju standardov in smernic naj strokovnjaki po potrebi poiščejo še druga navodila. Za dajanje zagotovil in revidiranje IS jih lahko pridobijo:
- od kolegov v podjetju in/ali zunaj njega, npr. prek strokovnih združenj ali strokovnih skupin na družbenih omrežjih,
- od vodstva,
- od organov upravljanja v podjetju, npr. od revizijske komisije.

2003 Strokovna neodvisnost *(nadaljevanje)*

4. Izrazi

Izraz	Pomen
Oslabitev	Stanje, ki povzroča slabost ali zmanjšano sposobnost za doseganje revizijskih ciljev. Oslabitev organizacijske neodvisnosti in nepristranskosti 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 nepristranskost ali zaznano nepristranskost. Grožnje za nepristranskost 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 so ogroženi poštenost, nepristranskost 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, nepristranskost in poklicno nezaupljivost.
Neoporečnost	Varovanje pred neustreznim spreminjanjem ali uničenjem informacij, kar vključuje tudi zagotavljanje nezatajljivosti in verodostojnosti informacij.
Pomembnost	Revizijski koncept, ki zadeva pomembnost informacije glede na njen vpliv ali učinek na pregledovano področje. Izraz relativne pomembnosti ali pomembnosti za neko določeno zadevo v kontekstu posla ali podjetja kot celote.
Nepristranskost	Zmožnost nepristranskega presojanja, izražanja mnenja in podajanja priporočil.
Strokovna presoja	Uporaba ustreznega znanja in izkušenj za ozaveščeno odločanje o ustreznem ukrepanju v okoliščinah posla dejanja zagotovil in revidiranja IS.
Poklicna nezaupljivost	Pristop, ki vključuje dvom in kritično ocenjevanje revizijskih dokazov. Vir: Ameriški inštitut preizkušenih javnih računovodij (AICPA) AU 230.07.

5. Datum uveljavitve

5.1 Datum uveljavitve Ta smernica velja za vse posle dajanja zagotovil in revidiranja IS, ki se začnejo 1. septembra 2014 ali pozneje.

2004 Upravičeno pričakovanje

Smernica je predstavljena v naslednjih poglavjih:
1. Namen smernice in povezava s standardi
2. Vsebina smernice
3. Povezava s standardi in procesi v COBIT 5
4. Izrazi
5. Datum uveljavitve

1. Namen smernice in povezava s standardi

1.0 Uvod

V tem poglavju so razjasnjeni:
1.1 Namen smernice
1.2 Povezava s standardi
1.3 Uporaba izrazov ‘revidiranje’ in ‘strokovnjaki’

1.1 Namen

1.1.1 Namen te smernice je pomagati strokovnjakom dajanja zagotovil in revidiranja IS pri uveljavljanju načela upravičenega pričakovanja pri izvajanju revizijskih poslov. Glavne značilnosti v zvezi s katerimi morajo imeti strokovnjaki upravičena pričakovanja, so, da:
- je revizijski posel mogoče dokončati v skladu s temi standardi in drugimi veljavnimi standardi ali predpisi in se bo zaključil s strokovnim mnenjem ali sklepom;
- bo obseg revizijskega posla omogočil izrek mnenja ali sklep o obravnavani zadevi;
- jim bo vodstvo zagotovilo ustrezne, pomembne in pravočasne informacije, potrebne za izvedbo revizijskega posla.

1.1.2 Ta smernica nadalje pomaga strokovnjakom dajanja zagotovil in revidiranja IS pri obravnavanju omejitev obsega in daje navodila glede sprejema sprememb v pogojih.

1.1.3 Strokovnjaki dajanja zagotovil in revidiranja IS morajo upoštevati to smernico pri določanju, kako izvajati standard, uporabiti strokovno presojo pri uporabi, utemeljiti vsako odstopanje in po potrebi poiskati dodatna navodila.

1.2 Povezava s standardi

1.2.1 Standard 1001 Revizijska listina
1.2.2 Standard 1004 Upravičeno pričakovanje

1.3 Uporaba izrazov

1.3.1 V nadaljnjem besedilu:
- se ‘dajanje zagotovil in revidiranje IS’ imenuje ‘revidiranje’;
- se ‘strokovnjaki dajanja zagotovil in revidiranja IS’ imenujejo ‘strokovnjaki’.

2. Vsebina smernice

2.0 Uvod

Poglavje o vsebini smernice je sestavljeno tako, da daje informacije o naslednjih ključnih temah posla dajanja zagotovil in revidiranja IS:
2.1 Standardi in predpisi
2.2 Obseg
2.3 Omejitve obsega
2.4 Informacije
2.5 Sprejemljivost spremembe v pogojih posla

2004 Upravičeno pričakovanje *(nadaljevanje)*

2.1 Standardi in predpisi

2.1.1 V revizijski listini bodo določeni standardi, po katerih se bodo ravnali funkcija revidiranja in strokovnjaki, kot je opisano v standardu 1001 Revizijska listina.

2.1.2 Strokovnjaki naj bi zbrali in ocenili vse veljavne standarde, navedene v revizijski listini, in predpise že pred revizijskim poslom in jih ponovno prebirali ves čas izvajanja posla, da preverijo, če lahko upravičeno pričakujejo, da lahko dokončajo revizijski posel v skladu s temi standardi in predpisi in da se bo revizijski posel zaključil s strokovnim mnenjem ali sklepom.

2.1.3 Če bi strokovnjaki ugotovili, da revizijskega posla ne morejo dokončati v skladu z enim ali več veljavnimi standardi in predpisi in ne bo mogoče izraziti strokovnega mnenja ali sklepa, naj bi:

- obvestili vodstvo dajanja zagotovil in revidiranja IS in pristojne za upravljanje o ugotovljeni vprašljivi skladnosti s standardi in predpisi,
- predlagali, da se spremenijo pogoji posla ali odklonili posel.

2.2 Obseg

2.2.1 Preden začnejo izvajati revizijski posel, naj bi strokovnjaki pregledali obseg revizijskega posla. Ugotovili naj bi, ali je obseg revizije jasno dokumentiran in omogoča pripravo strokovnega mnenja ali sklepa o obravnavani zadevi.

2.2.2 Obseg revizijskega posla naj bi bil jasno dokumentiran, tako da ne dopušča nobenih različnih tolmačenj glede področij (npr. procesi, aktivnosti, sistemi), ki so vključena v obseg posla. Pri nejasno opisanem obsegu strokovnjaki ne bodo mogli izoblikovati mnenja ali sklepa, ker ne bodo prepričani, ali so ocenjena vsa področja v obsegu posla.

2.2.3 Če bi strokovnjaki ugotovili, da obseg revizijskega posla ne omogoča izraziti strokovnega mnenja ali sklepa, naj bi:

- obvestili vodstvo dajanja zagotovil in revidiranja IS in pristojne za upravljanje o svojih ugotovitvah v zvezi z obsegom;
- predlagali spremembo v pogojih posla ali zavrnili predlagani revizijski posel.

2.3 Omejitve obsega

2.3.1 Določene omejitve obsega se lahko zgodijo pred ali med revizijskim poslom. Na te omejitve obsega lahko vplivajo različni dejavniki, kot so:

- ustrezne, pomembne in pravočasne informacije, potrebne za dokončanje revizijskega posla niso na voljo;
- (ključni) revidiranci niso na voljo;
- predvideni časovni okvir ne zadošča za dokončanje celotnega obsega revizijskega posla;
- poslovodstvo poskuša omejiti obseg revizijskega posla na izbrana področja;
- obseg revizijskega posla je premajhen ali prevelik, da bi lahko oblikovali sklep o obravnavani zadevi;
- stopnja decentralizacije otežuje oblikovanje sklepa o celoti obravnavane zadeve;
- razpoložljivost sprejemljivega števila ustrezno usposobljenih strokovnjakov za izvedbo revizijskega posla v sedanjem obsegu;
- struktura poročanja funkcije revidiranja, npr. če funkcija revidiranja ne poroča ustrezni ravni vodenja v podjetju, lahko dobi navodilo, naj ne oceni določenih elementov v obsegu posla.

2.3.2 Strokovnjaki naj bi proučili, ali jim te omejitve obsega še omogočajo upravičeno pričakovanje, da bo revizijski posel zaključen s strokovnim mnenjem ali sklepom. Če ugotovijo, da ta pogoj ne bo izpolnjen, naj ne bi sprejeli posla.

2.3.3 Če bi strokovnjaki sklepali, da še lahko upravičeno pričakujejo, da bo kljub omejitvam obsega posel lahko zaključen s strokovnim mnenjem ali sklepom, naj bi revizijski posel sprejeli ali ga nadaljevati. Omejitve obsega naj bi bile izrecno opisane v poročilu o poslu dajanja zagotovil in revidiranja IS.

2004 Upravičeno pričakovanje *(nadaljevanje)*

2.4 Informacije

2.4.1 V revizijski listini bo določena pravica dostopa do informacij, sistemov, zaposlenih in prostorov, pomembnih za izvajanje revizijskega posla, kot je opisano v standardu 1001 Revizijska listina.

2.4.2 Preden začnejo strokovnjaki izvajati revizijski posel, morajo ugotoviti in rešiti vse omejitve glede pravice dostopa do ustreznih, pomembnih in pravočasnih informacij za revizijski posel. Upravičeno naj bi pričakovali, da je njihova pravica dostopa do tega revizijskega posla v skladu z določbami v revizijski listini, ali da jim morebitna odstopanja od teh določb ne preprečujejo, da bi prišli do strokovnega mnenja ali sklepa o obravnavani zadevi.

2.4.3 Opravljanje posla revidiranja ali dajanja zagotovil bi lahko vključevalo tudi ocenjevanje aktivnosti, ki jih izvajata višje in izvršno vodstvo. Še pred izvajanjem revizijskega posla naj bi ocenili možnost, da bi do takega dogodka prišlo, kot tudi možnost, da bodo strokovnjakom oporekali potrebo za dostop do teh posameznikov ali s tem povezanih informacij. Pred izvajanjem revizijskega posla bi zato lahko bili potrebni ukrepi za zmanjšanje teh možnosti, ki so med drugim:

- zagotovitev, da revizijska listina daje ustrezne pristojnosti funkciji revidiranja in strokovnjakom,
- pridobitev izrecne pisne podpore pristojnih za upravljanje, npr. nadzornega sveta in revizijske komisije,
- navzočnost člana organa nadzora ali izvršnega vodstva, kadar se zahteva dostop do izvršnega vodstva ali poslovodstva.

2.4.4 Če bi strokovnjaki sklepali, da jim njihova pravica dostopa do informacij ne omogoča izraziti strokovnega mnenja ali sklepa, naj bi:

- obvestili vodstvo dajanja zagotovil in revidiranja IS in pristojne za upravljanje o ugotovljenih težavah glede pravice dostopa do ustreznih, pomembnih in pravočasnih informacij,
- predlagali spremembo v pogojih posla ali zavrnili predlagani revizijski posel.

2.5 Sprejemljivost spremembe v pogojih posla

2.5.1 Strokovnjaki naj ne bi sprejeli spremembe v pogojih revizijskega posla, kadar za to po njihovi strokovni presoji ni utemeljitve.

2.5.2 Če se od strokovnjakov pred koncem revizijskega posla zahteva, da sprejmejo spremembo v pogojih, ki znižuje raven zagotovila, naj bi na podlagi strokovne presoje ugotovili, ali je taka sprememba utemeljena.

2.5.3 Če se pogoji revizijskega posla spremenijo, naj bi to zapisali in uradno odobrili strokovnjaki in vodstvo dajanja zagotovil in revidiranja IS. Po dokončanju revizijskega posla naj bi bila taka sprememba v pogojih izrecno omenjena v poročilu o poslu dajanja zagotovil in revidiranja IS.

2.5.4 Če strokovnjaki ne sprejmejo spremembe v pogojih revizijskega posla in jim poslovodstvo ne dovoli nadaljevati prvotnega revizijskega posla, naj bi po posvetovanju z vodstvom revizije in dajanja zagotovil:

- odstopili od revizijskega posla,
- se v skladu s strokovno presojo odločili, ali je treba o okoliščinah poročati pristojnim za upravljanje, nadzornemu svetu ali celo nadzornikom.

---

3. Povezava s standardi in procesi v COBIT 5

3.0 Uvod

To poglavje daje pregled ustreznih:

3.1 Povezav s standardi
3.2 Povezav s procesi v COBIT 5
3.3 Drugih navodil

2004 Upravičeno pričakovanje *(nadaljevanje)*

3.1 Povezava s standardi

V tabeli je pregled:
- najpomembnejših standardov ISACA, ki jih neposredno podpira ta smernica;
- tistih zahtev standardov, ki so najpomembnejše za to smernico.

Opomba: Naštete so samo tiste zahteve standardov, ki so pomembne za to smernico.

Naslov standarda	Pomembne zahteve standarda
1001 Revizijska listina	Pri dajanju zagotovil in revidiranju IS mora biti revidiranje ustrezno dokumentirano v revizijski listini, pri čemer morajo biti navedeni namen, zadolžitev, pristojnost in odgovornost. Pri dajanju zagotovil in revidiranju IS mora biti revizijska listina usklajena in potrjena na ustrezni ravni v podjetju.
1004 Upravičeno pričakovanje	Strokovnjaki dajanja zagotovil in revidiranja IS morajo upravičeno pričakovati, da je posel lahko 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. Strokovnjaki dajanja zagotovil in revidiranja IS morajo upravičeno pričakovati, da je glede na obseg posla možno sklepati o obravnavani zadevi in obravnavati kakršne koli omejitve. Strokovnjaki dajanja zagotovil in revidiranja IS morajo upravičeno pričakovati, da se poslovodstvo zaveda obveznosti in zadolžitev pri zagotavljanju primernih, ustreznih in pravočasnih informacij, ki so potrebne za izvedbo posla.

3.2 Povezava s procesi v COBIT 5

V tabeli je pregled najpomembnejših:
- procesov v COBIT 5,
- namenov procesov v COBIT 5.

Posebne aktivnosti, ki se izvajajo kot del teh procesov, so v *COBIT 5: Omogočanje procesov*.

Proces v COBIT 5	Namen procesa
MEA02 Spremljajte, vrednotite in ocenjujte sistem notranjih kontrol.	Ključnim deležnikom omogočite pregled nad ustreznostjo sistema notranjih kontrol in s tem zagotovite zaupanje v delovanje, vero v doseganje ciljev podjetja in ustrezno razumevanje preostalega tveganja.
MEA03 Spremljajte, vrednotite in ocenjujte skladnost z zunanjimi zahtevami.	Zagotovite, da podjetje ravna v skladu z vsemi veljavnimi zunanjimi zahtevami.

3.3 Druga navodila

Pri izvajanju standardov in smernic naj strokovnjaki po potrebi poiščejo še druga navodila. Za dajanje zagotovil in revidiranje IS jih lahko pridobijo:
- od kolegov v podjetju in/ali zunaj njega, npr. prek strokovnih združenj ali strokovnih skupin na družbenih omrežjih,
- od vodstva,
- od organov upravljanja v podjetju, npr. od revizijske komisije,
- iz drugih navodil (npr. knjig, člankov, drugih smernic).

4. Izrazi

Izraz	Pomen
(Ga ni.)	

5. Datum uveljavitve

5.1 Datum uveljavitve Ta smernica velja za vse posle dajanja zagotovil in revidiranja IS, ki se začnejo 1. septembra 2014 ali pozneje.

2005 Potrebna poklicna skrbnost

Smernica je predstavljena v naslednjih poglavjih:
1. Namen smernice in povezava s standardi
2. Vsebina smernice
3. Povezava s standardi in procesi v COBIT 5
4. Izrazi
5. Datum uveljavitve

1. Namen smernice in povezava s standardi

1.0 Uvod

V tem poglavju so razjasnjeni:
1.1 Namen smernice
1.2 Povezava s standardi
1.3 Uporaba izrazov ‘revidiranje’ in ‘strokovnjaki’

1.1 Namen

1.1.1 Namen te smernice je pojasniti izraz ‘potrebna poklicna skrbnost’, kot se uporablja za neoporečno in skrbno izvajanje revizijskega posla v skladu s Kodeksom poklicne etike ISACA.

1.1.2 Ta smernica pojasnjuje, kako morajo strokovnjaki dajanja zagotovil in revidiranja IS uporabiti potrebno poklicno skrbnost pri načrtovanju in izvajanju revizijskega posla ter poročanju o njem.

1.1.3 Strokovnjaki dajanja zagotovil in revidiranja IS naj bi upoštevali to smernico pri odločanju, kako izvajati standard, uporabiti strokovno presojo pri uporabi, utemeljiti vsako odstopanje in po potrebi poiskati dodatna navodila.

1.2 Povezava s standardi

1.2.1 Standard 1002 Organizacijska neodvisnost
1.2.2 Standard 1003 Strokovna neodvisnost
1.2.3 Standard 1005 Potrebna poklicna skrbnost
1.2.4 Standard 1006 Strokovna usposobljenost
1.2.5 Standard 1205 Dokazi

1.3 Uporaba izrazov

1.3.1 V nadaljnjem besedilu:
- se ‘dajanje zagotovil in revidiranje IS’ imenuje ‘revidiranje’;
- se ‘strokovnjaki dajanja zagotovil in revidiranja IS’ imenujejo ‘strokovnjaki’.

2. Vsebina smernice

2.0 Uvod

Poglavje o vsebini smernice je sestavljeno tako, da daje informacije o naslednjih ključnih temah posla dajanja zagotovil in revidiranja IS:
2.1 Poklicna nezaupljivost in usposobljenost
2.2 Uporaba
2.3 Življenjski cikel posla
2.4 Komuniciranje
2.5 Upravljanje informacij

2005 Potrebna poklicna skrbnost *(nadaljevanje)*

2.1 Poklicna nezaupljivost in usposobljenost

2.1.1 Potrebna poklicna skrbnost velja za izvajanje strokovne presoje pri opravljanju prevzetega dela. Potrebna poklicna skrbnost pomeni, da naj bi se strokovnjaki lotili zadev, ki zahtevajo strokovno presojo, s poklicno nezaupljivostjo, prizadevnostjo, neoporečnostjo in skrbnostjo. Ta pristop naj bi ohranili ves čas izvajanja celotnega posla.

2.1.2 Strokovnjaki naj bi vzdrževali usposobljenost, neodvisnost in nepristransko mišljenje o vseh zadevah, povezanih z izvajanjem revizijskega posla. Pri obravnavanju zadev in sprejemanju sklepov morajo biti pošteni in nepristranski.

2.1.3 Ob izvajanju potrebne poklicne skrbnosti naj bi strokovnjaki upoštevali možnost, da bodo naleteli na neučinkovitost, zlorabe, napake in izločitve, nesposobnost, navzkrižja interesov ali prevare. Strokovnjaki naj bi bili pozorni tudi na posebne okoliščine ali aktivnosti, v katerih se take zadeve pojavljajo.

2.1.4 Če skrbijo za dobro obveščenost in se ravnajo po zadnjih dognanjih v strokovnih standardih, kažejo strokovnjaki sprejemljivo poznavanje in strokovno usposobljenost za doseganje ciljev dajanja zagotovil in revidiranja IS. Podrobna navodila lahko najdete v standardu 1006 Strokovna usposobljenost.

2.1.5 Strokovnjaki naj bi izvajali revizijski posel z vso skrbnostjo in se pri tem ravnali po strokovnih standardih ter zakonskih in drugih predpisanih zahtevah.

2.2 Uporaba

2.2.1 Potrebna poklicna skrbnost naj bi zajemala vse vidike revizije, kar med drugim vključuje ocenjevanje revizijskega tveganja, sprejetje revizijskih poslov, določitev obsega revizije, oblikovanje revizijskih ciljev, načrtovanje revizije, izvajanje revizije, dodeljevanje virov za revizijo, izbiranje revizijskih preizkusov, ovrednotenje izidov preizkusov, dokumentiranje revizije, sklepne ugotovitve revizije, poročanje in izročitev izidov revizije. Pri tem naj bi strokovnjaki določili ali ocenili:

- vrsto, raven, znanje in sposobnosti kadrov, potrebnih za doseganje ciljev dajanja zagotovil in revidiranja IS,
- pomembnost prepoznanih tveganj in njihov možni učinek na obravnavani predmet revizije,
- zadostnost, veljavnost in pomembnost zbranih revizijskih dokazov,
- usposobljenost, neoporečnost in sklepne ugotovitve drugih, na katerih delo se strokovnjaki opirajo.

2.2.2 Potrebna poklicna skrbnost tudi zahteva, da strokovnjaki opravljajo vse posle ob upoštevanju sprejemljivih zagotovil.

2.2.3 Strokovnjaki naj bi zakonito in pošteno delovali v interesu deležnikov, ob tem pa vzdrževali visoke standarde obnašanja in značaja in se ne bi smeli vpletati v dejanja, ki bi škodovala ugledu stroke.

2.3 Življenjski cikel posla

2.3.1 Strokovnjaki naj bi celovito in pravočasno načrtovali revizijski posel z vso potrebno poklicno skrbnostjo, da bi zagotovili razpoložljivost ustreznih virov in pravočasno dokončanje revizijskega posla. Strokovnjaki, dodeljeni projektu, naj bi imeli kot skupina potrebne veščine, znanje in ustrezne sposobnosti za izvajanje revizijskega posla.

2.3.2 Strokovnjaki naj bi izvajali revizijski posel s potrebno poklicno skrbnostjo, to je v skladu z ustreznimi strokovnimi standardi za zagotavljanje kakovosti in dokončanje revizije z izdanim sklepom ali mnenjem.

2.4 Komuniciranje

2.4.1 Opredeljene vloge in zadolžitve naj bi bile članom skupine sporočene pred začetkom projekta, tako da se bodo pri izvajanju revizijskega posla lahko ravnali po ustreznih strokovnih standardih.

2.4.2 Med izvajanjem revizijskega posla naj bi strokovnjaki primerno komunicirali z revidiranci in ustreznimi deležniki, da bi zagotovili njihovo sodelovanje.

2.4.3 Strokovnjaki naj bi svoje ugotovitve naslovili na revidiranca revizijskega posla.

2.4.4 Strokovnjaki naj bi vprašanja v zvezi z uporabo strokovnih standardov dokumentirali in sporočali ustreznim strankam, da bi jih skupaj rešili.

2.4.5 Strokovnjaki bi morali ravnati s potrebno poklicno skrbnostjo, kadar ustrezne stranke obveščajo o izidih opravljenega dela.

2.5 Pridobivanje in upravljanje informacij

2.5.1 Strokovnjaki naj bi upravičeno pričakovali, da poslovodstvo razume obveznosti in zadolžitve glede zagotavljanja ustreznih, pomembnih in pravočasnih informacij, potrebnih za izvajanje revizijskega posla.

2.5.2 Strokovnjaki naj bi sprejeli sprejemljive ukrepe za ohranjanje zasebnosti in zaupnosti informacij, pridobljenih med opravljanjem nalog, razen če razkritje zahteva z zakonom pooblaščeni organ. Take informacije se ne smejo uporabljati v osebno korist ali razkrivati neustreznim strankam.

2.5.3 Informacije je treba hraniti in jih pravilno uničiti v skladu z organizacijskimi usmeritvami in ustreznimi zakoni, pravili in predpisi.

2005 Potrebna poklicna skrbnost *(nadaljevanje)*

3. Povezava s standardi in procesi v COBIT 5

3.0 Uvod

To poglavje daje pregled ustreznih:
3.1 Povezav s standardi
3.2 Povezav s procesi v COBIT 5
3.3 Drugih navodil

3.1 Povezava s standardi

V tabeli je pregled:
- najpomembnejših standardov ISACA, ki jih neposredno podpira ta smernica;
- tistih zahtev standardov, ki so najpomembnejše za to smernico.

Opomba: Naštete so samo tiste zahteve standardov, ki so pomembne za to smernico.

Naslov standarda	Pomembne zahteve standarda
1002 Organizacijska neodvisnost	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	Strokovnjaki dajanja zagotovil in revidiranja IS morajo biti tako po mišljenju kot po zaznavi neodvisni in nepristranski v vseh zadevah, povezanih s posli revidiranja in dajanja zagotovil.
1005 Potrebna poklicna skrbnost	Strokovnjaki dajanja zagotovil in revidiranja IS morajo pri načrtovanju in izvajanju poslov ter poročanju o izidih ravnati s potrebno poklicno skrbnostjo, vključno z upoštevanjem veljavnih strokovnih standardov za revizijo.
1006 Strokovna usposobljenost	Strokovnjaki dajanja zagotovil in revidiranja IS morajo imeti 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. Strokovnjaki dajanja zagotovil in revidiranja IS morajo imeti s sodelavci pri nalogi ustrezno znanje o obravnavani zadevi. Strokovnjaki dajanja zagotovil in revidiranja IS morajo ohranjati strokovno usposobljenost z ustreznim nenehnim strokovnim izobraževanjem in usposabljanjem.
1205 Revizijski dokazi	Strokovnjaki dajanja zagotovil in revidiranja IS morajo pridobiti zadostne in ustrezne dokaze, da lahko sprejmejo primerne sklepe, s katerimi utemeljijo izide posla. Strokovnjaki dajanja zagotovil in revidiranja IS morajo ovrednotiti zadostnost dokazov, pridobljenih za utemeljitev sklepov in doseganje ciljev posla.

2005 Potrebna poklicna skrbnost *(nadaljevanje)*

3.2 Povezava s procesi v COBIT 5

V tabeli je pregled najpomembnejših:
- procesov v COBIT 5,
- namenov procesov v COBIT 5.

Posebne aktivnosti, ki se izvajajo kot del teh procesov, so v *COBIT 5: Omogočanje procesov*.

Proces v COBIT 5	Namen procesa
EDM01 Zagotovite postavitev in vzdrževanje okvira upravljanja.	Zagotovite dosleden pristop, povezan in usklajen z načinom upravljanja podjetja. Da bodo odločitve za IT sprejete v skladu s strategijami in cilji podjetja, zagotovite, da so procesi, povezani z IT, uspešno in pregledno nadzorovani, da je skladnost z zakonskimi in drugimi predpisanimi zahtevami potrjena in da so izpolnjene upravljavske zahteve za člane organa nadzora.
APO07 Upravljajte človeške vire.	Optimizirajte zmožnosti človeških virov za doseganje ciljev podjetja.
MEA02 Spremljajte, vrednotite in ocenjujte sistem notranjih kontrol.	Ključnim deležnikom omogočite pregled nad ustreznostjo sistema notranjih kontrol in s tem zagotovite zaupanje v delovanje, vero v doseganje ciljev podjetja in ustrezno razumevanje preostalega tveganja.
MEA03 Spremljajte, vrednotite in ocenjujte skladnost z zunanjimi zahtevami.	Zagotovite, da podjetje ravna v skladu z vsemi veljavnimi zunanjimi zahtevami.

3.3 Druga navodila

Pri izvajanju standardov in smernic naj strokovnjaki po potrebi poiščejo še druga navodila. Za dajanje zagotovil in revidiranje IS jih lahko pridobijo:
- od kolegov v podjetju in/ali zunaj njega, npr. prek strokovnih združenj ali strokovnih skupin na družbenih omrežjih,
- od vodstva,
- od organov upravljanja v podjetju, npr. od revizijske komisije,
- iz drugih navodil (npr. knjig, člankov, drugih smernic).

4. Izrazi

Izraz	Pomen
Strokovna usposobljenost	Dokazana raven zmožnosti s strokovnimi izkušnjami, pogosto povezana z dokazili o strokovnosti, ki so jih izdali strokovni organi v skladu s svojimi kodeksi prakse in standardi.
Strokovna presoja	Uporaba ustreznega znanja in izkušenj za ozaveščeno odločanje o ustreznem ukrepanju v okoliščinah posla dejanja zagotovil in revidiranja IS.
Poklicna nezaupljivost	Pristop, ki vključuje dvom in kritično ocenjevanje revizijskih dokazov. Vir: Ameriški inštitut preizkušenih javnih računovodij (AICPA) AU 230.07.

5. Datum uveljavitve

5.1 Datum uveljavitve

Ta smernica velja za vse posle dajanja zagotovil in revidiranja IS, ki se začnejo 1. septembra 2014 ali pozneje.

2006 Strokovna usposobljenost

Smernica je predstavljena v naslednjih poglavjih:
1. Namen smernice in povezava s standardi
2. Vsebina smernice
3. Povezava s standardi in procesi v COBIT 5
4. Izrazi
5. Datum uveljavitve

1. Namen smernice in povezava s standardi

1.0 Uvod

V tem poglavju so razjasnjeni:
1.1 Namen smernice
1.2 Povezava s standardi
1.3 Uporaba izrazov ‘revidiranje’ in ‘strokovnjaki’

1.1 Namen

1.1.1 Ta smernica daje navodila, ki strokovnjakom dajanja zagotovil in revidiranja IS pomagajo pridobiti potrebne veščine in znanje ter vzdrževati strokovno usposobljenost pri izvajanju revizijskih poslov.

1.1.2 Strokovnjaki dajanja zagotovil in revidiranja IS naj bi upoštevali to smernico pri odločanju, kako izvajati standard, uporabiti strokovno presojo pri njegovi uporabi, utemeljiti vsako odstopanje in po potrebi poiskati dodatna navodila.

1.2 Povezava s standardi

1.2.1 Standard 1005 Potrebna poklicna skrbnost
1.2.2 Standard 1006 Strokovna usposobljenost
1.2.3 Standard 1201 Načrtovanje posla
1.2.4 Standard 1203 Izvedba in nadzor

1.3 Uporaba izrazov

1.3.1 V nadaljnjem besedilu:
- se ‘dajanje zagotovil in revidiranje IS’ imenuje ‘revidiranje’;
- se ‘strokovnjaki dajanja zagotovil in revidiranja IS’ imenujejo ‘strokovnjaki’.

2. Vsebina smernice

2.0 Uvod

Poglavje o vsebini smernice je sestavljeno tako, da daje informacije o naslednjih ključnih temah posla dajanja zagotovil in revidiranja IS:
2.1 Strokovna usposobljenost
2.2 Ocenjevanje
2.3 Doseganje želene ravni usposobljenosti

2006 Strokovna usposobljenost *(nadaljevanje)*

2.1 Strokovna usposobljenost

2.1.1 Strokovna usposobljenost pomeni imeti veščine, znanje in izkušnje, pridobljene z ustrezno stopnjo izobrazbe in delovnimi izkušnjami, ki so potrebne za ustrezno izvedbo revizijskega posla.

2.1.2 Vodstvo dajanja zagotovil in revidiranja IS naj bi sporočilo, kakšna je želena in/ali pričakovana raven strokovne usposobljenosti na podlagi ustreznih meril uspešnosti za različne vloge in revizijske posle ter zagotovilo, da se taka merila uspešnosti redno pregledujejo in posodabljajo. Vodstvo dajanja zagotovil in revidiranja IS bi moralo dokumentirati zahtevano strokovno usposobljenost za različne ravni zahtevnosti dela, na primer z oblikovanjem matrike veščin, ki prikazuje zahtevano strokovno usposobljenost za različne ravni zahtevnosti dela.

2.1.3 Vodstvo dajanja zagotovil in revidiranja IS bi moralo dati sprejemljivo zagotovilo, da so na razpolago strokovno usposobljeni kadri, potrebni za izvedbo revizijskih poslov, opredeljenih v načrtu revidiranja IS, razpoložljivost takih strokovno usposobljenih kadrov pa naj bi bila potrjena in zagotovljena pred začetkom izvajanja revizijskega posla.

2.1.4 Vodstvo dajanja zagotovil in revidiranja IS je odgovorno za zagotavljanje, da so člani skupine strokovno usposobljeni izvesti revizijski posel. Ugotavljanje temeljnih strokovnih sposobnosti članov skupine bo pomagalo učinkovito izrabiti razpoložljive vire.

2.1.5 Strokovnjaki naj bi dali sprejemljivo zagotovilo, da imajo zahtevano raven strokovne usposobljenosti. Odgovorni bi morali biti za pridobivanje zahtevanih strokovnih in tehničnih veščin in znanja, da lahko opravijo vsako nalogo, ki so jo prevzeli.

2.1.6 Zahtevane veščine in znanje se razlikujejo glede na položaj in vlogo strokovnjakov pri revizijskem poslu. Zahteve za vodstvene veščine in znanje morajo biti sorazmerne s stopnjo odgovornosti.

2.1.7 Veščine in znanje vključujejo strokovno usposobljenost pri prepoznavanju in upravljanju tveganj in kontrol ter poznavanju revizijskih orodij in tehnik. Strokovnjaki naj bi imeli analitično in tehnično znanje ter obvladati veščine vodenja razgovorov, medosebnih odnosov in predstavitvene veščine.

2.1.8 Strokovnjaki naj bi prepoznali morebitne okoliščine ali odstopanja, ki so pomembna za revizijski posel, določili njihov vpliv in obveščali o njih.

2.1.9 Strokovnjaki naj bi bili sposobni prepoznati možne znake prevare.

2.1.10 Strokovnjaki naj bi imeli splošno temeljno poslovno znanje, npr. iz ekonomike, financ, računovodstva, informacijske tehnologije, tveganj, davkov in prava, da ne bi spregledali morebitnih vprašljivih zadev ali pomanjkljivosti.

2.1.11 Primerno je, da si strokovnjaki med člani skupine izmenjujejo in delijo izkušnje, sprejeto dobro prakso ter z delom pridobljene izkušnje in znanje za skupno boljšo strokovno usposobljenost virov. Strokovna usposobljenost članov skupine se izboljša tudi s srečanji za oblikovanje skupinskega duha, z delavnicami, s konferencami, seminarji, predavanji in drugimi načini medsebojnega delovanja.

2.1.12 Za zagotavljanje razpoložljivosti ustreznih veščin je treba oceniti tudi možnosti za pridobitev teh veščin. To vključuje pogodbeni najem določenih posebnih virov, zunanje izvajanje dela nalog dajanja zagotovil in revidiranja IS in/ali odlaganje revizijskega posla, dokler potrebne veščine niso na voljo.

2.1.13 Zunanje znanje je mogoče pridobiti z zunanjim izvajanjem dela posla. Sodelovanje med zunanjimi izvajalci in notranjimi strokovnjaki zagotavlja, da se razvijajo in vzdržujejo tudi notranje veščine in znanje.

2.1.14 Kadar je del revizijskega posla oddan v zunanje izvajanje ali je pridobljena strokovna pomoč, je treba dati sprejemljivo zagotovilo, da je agencija ali zunanji strokovnjak, ki prevzame delo v izvajanje, ustrezno strokovno usposobljen.

2.1.15 Kadar je pridobljena stalna strokovna pomoč, je treba strokovno usposobljenost takih zunanjih strokovnjakov redno meriti, spremljati in pregledovati po strokovnih standardih ali merilih uspešnosti.

2.2 Ocenjevanje

2.2.1 Strokovnjaki naj bi stalno spremljali svoje veščine in znanje, da bi vzdrževali ustrezno raven strokovne usposobljenosti. Vodstvo dajanja zagotovil in revidiranja IS naj bi redno ocenjevalo strokovno usposobljenost.

2.2.2 Ocenjevanje uspešnosti strokovnjakov je treba izvajati na pošten, pregleden, lahko razumljiv, nedvoumen, nepristranski način, ki velja za splošno sprejemljivo prakso v danem zaposlitvenem okolju.

2.2.3 Ocenjevalna merila in postopki naj bi bili jasno opredeljeni, lahko pa se razlikujejo glede na okoliščine, kot so zemljepisna lega, politično ozračje, vrsta naloge, kultura ipd.

2.2.4 Za skupino strokovnjakov bi bilo treba izvesti medfunkcijsko notranje ocenjevanje med skupinami ali posamezniki.

2.2.5 Za posameznega neodvisnega strokovnjaka pa bi bilo treba izvesti ocenjevanje med sodelavci, če je le mogoče. Če pregled med strokovnimi sodelavci ni mogoč, bi bilo treba izpeljati samoocenjevanje in ga dokumentirati.

2.2.6 Uspešnost dela strokovnjakov bi morala oceniti ustrezna raven vodstva.

2.2.7 Vrzeli, ugotovljene med ocenjevanjem, naj bi bile ustrezno obravnavane.

2006 Strokovna usposobljenost *(nadaljevanje)*

2.3 Doseganje želene ravni usposobljenosti

2.3.1 Vrzeli, ugotovljene na podlagi razlik med dejansko in pričakovano ravnijo strokovne usposobljenosti, je treba zapisati in proučiti. Če je za katerikoli vir ugotovljena pomembna pomanjkljivost, naj tega vira ne bi uporabili pri izvajanju revizijskega posla.

2.3.2 Pomembno je ugotoviti vzrok vrzeli in čim prej sprejeti ustrezne popravljalne ukrepe, kot so usposabljanje in stalno strokovno izobraževanje (angl. CPE – continuing professional education).

2.3.3 Usposabljanje, zahtevano za revizijski posel, je treba končati v razumnem roku in pred začetkom izvajanja revizijske aktivnosti.

2.3.4 Uspešnost usposabljanja je treba izmeriti po preteku primernega časa po končanem usposabljanju.

2.3.5 Dokumentacija o zahtevanih veščinah, na primer matrika veščin, kot jo je oblikovalo vodstvo dajanja zagotovil in revidiranja IS (glej točko 2.1.2), bo pomagala pri ugotavljanju vrzeli in potreb po usposabljanju. Taka matrika je lahko navzkrižna povezava z razpoložljivimi kadri ter njihovimi veščinami in znanjem.

2.3.6 Evidenco zagotovljenega usposabljanja skupaj s povratnimi informacijami o usposabljanju in njegovi uspešnosti je treba vzdrževati, proučevati in se nanjo sklicevati ob prihodnji uporabi.

2.3.7 Stalno strokovno izobraževanje (CPE) je sprejeta metodologija za vzdrževanje strokovne usposobljenosti in posodabljanje veščin in znanja. Strokovnjaki naj bi upoštevali zahteve usmeritev stalnega strokovnega izobraževanja, kot jih določijo ustrezne strokovne organizacije, v katere se povezujejo.

2.3.8 Programi stalnega strokovnega izobraževanja (CPE) naj pomagajo izpopolnjevati veščine in znanje, nanašajo pa naj se na strokovne in tehnične zahteve za dajanje zagotovil, varnost in upravljanje IS. Strokovne organizacije običajno predpišejo programe, ki so primerni za priznavanje stalnega strokovnega izobraževanja. Strokovnjaki naj bi se ravnali po normativih, ki jih predpišejo ustrezne strokovne organizacije.

2.3.9 Strokovne organizacije običajno predpišejo metodologijo za pridobitev točk stalnega strokovnega izobraževanje (CPE) in najmanjše število točk CPE, ki naj bi jih redno pridobivali njihovi člani. Strokovnjaki naj bi se ravnali po normativih, ki jih predpišejo ustrezne strokovne organizacije. Kadar se strokovnjaki združujejo v več strokovnih organizacij zaradi pridobivanja najmanjšega potrebnega števila kreditnih točk, lahko po svoji strokovni presoji skupno izkoristijo točke stalnega strokovnega izobraževanja (CPE) iz priznanih programov, če je le-to skladno s pravili oziroma smernicami, ki so jih opredelile ustrezne strokovne organizacije.

2.3.10 ISACA ima izdelano celovito usmeritev stalnega strokovnega izobraževanja (CPE), ki velja za njene člane in imetnike naziva CISA. Strokovnjaki z nazivom CISA se morajo glede stalnega strokovnega izobraževanja ravnati po usmeritvi ISACA. Podrobne informacije o tej usmeritvi so dostopne na spletni strani *www.isaca.org/CISAcpepolicy*.

2.3.11 Kot to predpisujejo ustrezne strokovne organizacije, vključno z ISACA, morajo strokovnjaki voditi primerno evidenco programov stalnega strokovnega izobraževanja, jih določen čas hraniti in po potrebi omogočiti njihov pregled.

3. Povezava s standardi in procesi v COBIT 5

3.0 Uvod

To poglavje daje pregled ustreznih:

3.1 Povezav s standardi
3.2 Povezav s procesi v COBIT 5
3.3 Drugih navodil

2006 Strokovna usposobljenost *(nadaljevanje)*

3.1 Povezava s standardi

V tabeli je pregled:
- najpomembnejših standardov ISACA, ki jih neposredno podpira ta smernica;
- tistih zahtev standardov, ki so najpomembnejše za to smernico.

Opomba: Naštete so samo tiste zahteve standardov, ki so pomembne za to smernico.

Naslov standarda	Pomembne zahteve standarda
1005 Potrebna poklicna skrbnost	Strokovnjaki dajanja zagotovil in revidiranja IS morajo pri načrtovanju in izvajanju poslov ter poročanju o izidih ravnati s potrebno poklicno skrbnostjo, vključno z upoštevanjem veljavnih strokovnih standardov za revizijo.
1006 Strokovna usposobljenost	Strokovnjaki dajanja zagotovil in revidiranja IS morajo imeti 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. Strokovnjaki dajanja zagotovil in revidiranja IS morajo imeti s sodelavci pri nalogi ustrezno znanje o obravnavani zadevi. Strokovnjaki dajanja zagotovil in revidiranja IS morajo ohranjati strokovno usposobljenost z ustreznim nenehnim strokovnim izobraževanjem in usposabljanjem.
1201 Načrtovanje posla	Strokovnjaki dajanja zagotovil in revidiranja IS morajo načrtovati vsak posel dajanja zagotovil in revidiranja IS z namenom, da obravnavajo: • 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 značilna za posel, • zahteve glede dokumentacije in poročanja. Strokovnjaki dajanja zagotovil in revidiranja IS morajo pripraviti in dokumentirati projektni načrt posla dajanja zagotovil ali revidiranja IS, ki opisuje: • vrsto posla, cilje, časovni načrt in zahteve glede virov, • časovno razporeditev in obseg revizijskih postopkov za izvedbo posla.
1203 Izvedba in nadzor	Za doseganje revizijskih ciljev in spoštovanje veljavnih strokovnih revizijskih standardov morajo strokovnjaki dajanja zagotovil in revidiranja IS nadzirati osebje, ki izvaja revizije IS in za katero so zadolženi. Strokovnjaki dajanja zagotovil in revidiranja IS lahko sprejmejo samo naloge, ki so v okviru njihovega strokovnega znanja in veščin, ali naloge, za katere upravičeno pričakujejo, da bodo veščine pridobili med izvajanjem posla ali da jih bodo opravili pod nadzorom.

3.2 Povezava s procesi v COBIT 5

V tabeli je pregled najpomembnejših:
- procesov v COBIT 5,
- namenov procesov v COBIT 5.

Posebne aktivnosti, ki se izvajajo kot del teh procesov, so v *COBIT 5: Omogočanje procesov*.

Proces v COBIT 5	Namen procesa
EDM04 Zagotovite optimizacijo virov.	Zagotovite, da so potrebe podjetja po virih optimalno izpolnjene, da so stroški IT optimizirani in da je večja verjetnost uresničevanja koristi in pripravljenosti za prihodnje spremembe.
APO07 Upravljajte človeške vire.	Optimizirajte zmožnosti človeških virov za doseganje ciljev podjetja.
MEA02 Spremljajte, vrednotite in ocenjujte sistem notranjih kontrol.	Ključnim deležnikom omogočite pregled nad ustreznostjo sistema notranjih kontrol in s tem zagotovite zaupanje v delovanje, vero v doseganje ciljev podjetja in ustrezno razumevanje preostalega tveganja.

2006 Strokovna usposobljenost *(nadaljevanje)*

3.3 Druga navodila Pri izvajanju standardov in smernic naj strokovnjaki po potrebi poiščejo še druga navodila. Za dajanje zagotovil in revidiranje IS jih lahko pridobijo:

- od kolegov v podjetju in/ali zunaj njega, npr. prek strokovnih združenj ali strokovnih skupin na družbenih omrežjih,
- od vodstva,
- od organov upravljanja v podjetju, npr. od revizijske komisije,
- iz drugih navodil (npr. knjig, člankov, drugih smernic).

4. Izrazi

Izraz	Pomen
Pomembnost	Revizijski koncept, ki zadeva pomembnost informacije glede na njen vpliv ali učinek na pregledovano področje. Izraz relativne pomembnosti ali pomembnosti za neko določeno zadevo v kontekstu posla ali podjetja kot celote.
Strokovna sposobnost	Dokazana raven zmožnosti skupaj s strokovnimi izkušnjami, pogosto povezana z dokazili o strokovnosti, ki so jih izdali strokovni organi v skladu s svojimi kodeksi prakse in standardi.
Strokovna presoja	Uporaba ustreznega znanja in izkušenj za ozaveščeno odločanje o ustreznem ukrepanju v okoliščinah posla dejanja zagotovil in revidiranja IS.
Strokovna usposobljenost	Spretnosti in izkušnje.

5. Datum uveljavitve

5.1 Datum uveljavitve Ta smernica velja za vse posle dajanja zagotovil in revidiranja IS, ki se začnejo 1. septembra 2014 ali pozneje.

2007 Trditve

Smernica je predstavljena v naslednjih poglavjih:
1. Namen smernice in povezava s standardi
2. Vsebina smernice
3. Povezava s standardi in procesi v COBIT 5
4. Izrazi
5. Datum uveljavitve

1. Namen smernice in povezava s standardi

1.0 Uvod

V tem poglavju so razjasnjeni:
1.1 Namen smernice
1.2 Povezava s standardi
1.3 Uporaba izrazov ‘revidiranje’ in ‘strokovnjaki’

1.1 Namen

1.1.1 Namen te smernice je podrobno obdelati različne trditve, usmerjati strokovnjake dajanja zagotovil in revidiranja IS pri zagotavljanju, da merila, na podlagi katerih je treba oceniti obravnavano zadevo, podpirajo te trditve, in dati navodila za oblikovanje sklepa in pripravljanje poročila o trditvah.

1.1.2 Strokovnjaki dajanja zagotovil in revidiranja IS naj bi upoštevali to smernico pri odločanju, kako izvajati standard, uporabiti strokovno presojo pri uporabi, utemeljiti vsako odstopanje in po potrebi poiskati dodatna navodila.

1.2 Povezava s standardi

1.2.1 Standard 1007 Trditve
1.2.2 Standard 1008 Merila
1.2.3 Standard 1204 Pomembnost
1.2.4 Standard 1206 Uporaba dela drugih strokovnjakov
1.2.5 Standard 1401 Poročanje

1.3 Uporaba izrazov

1.3.1 V nadaljnjem besedilu:
- se ‘dajanje zagotovil in revidiranje IS’ imenuje ‘revidiranje’;
- se ‘strokovnjaki dajanja zagotovil in revidiranja IS’ imenujejo ‘strokovnjaki’.

2. Vsebina smernice

2.0 Uvod

Poglavje o vsebini smernice je sestavljeno tako, da daje informacije o naslednjih ključnih temah posla dajanja zagotovil in revidiranja IS:
2.1 Trditve
2.2 Obravnavana zadeva in merila
2.3 Trditve, ki so jih navedle tretje stranke
2.4 Sklep in poročilo

2007 Trditve *(nadaljevanje)*

2.1 Trditve

2.1.1 Trditve so kakršne koli izjave ali skupek izjav o tem, ali obravnavana zadeva temelji na izbranih merilih ali je v skladu z njimi. Strokovnjaki naj bi upoštevali te trditve ves čas izvajanja revizijskega posla, pridobili zagotovilo o njihovi uresničitvi in to izrazili v revizijskem poročilu.

2.1.2 Pogoste trditve, ki naj bi se upoštevale, so med drugim:

- **zaupnost** – ohranjanje odobrenih omejitev za dostop in razkritje, vključno s sredstvi za zaščito zasebnosti in informacijami z lastninsko pravico;
- **popolnost** – vse aktivnosti, informacije in drugi podatki, ki jih je treba evidentirati, so dejansko tudi evidentirani; npr. vse spremembe sistema IT, predane v delovanje, so zapisane v aplikaciji za beleženje sprememb;
- **točnost** – zneski, datumi in drugi podatki, ki se nanašajo na evidentirane aktivnosti, so bili ustrezno zapisani; npr. podatki, povezani s predajo sprememb sistema IT v delovanje, so točno prikazani v zapisih sprememb v aplikaciji za beleženje sprememb;
- **neoporečnost** – informacije, dokazi in drugi prejeti podatki prihajajo iz zaupanja vrednih in zanesljivih virov, npr. zapise o spremembah, ki jih zahtevajo strokovnjaki, prejmejo od osebe, odgovorne za skladnost, to je iz zaupanja vrednega in zanesljivega vira v podjetju;
- **razpoložljivost** – informacije, dokazi in drugi podatki, potrebni za revizijski posel, obstajajo in so dostopni; npr. zahtevani zapisi o spremembah obstajajo in so takoj dostopni v aplikaciji za beleženje sprememb;
- **skladnost** – informacije, dokazi in drugi podatki so bili evidentirani v skladu z določili podjetja, s predpisanimi ali drugimi veljavnimi določbami; npr. zahtevana področja so v skladu z veljavnimi določbami vpisana v zapisih sprememb v aplikaciji za beleženje sprememb.

2.1.3 Poslovodstvo je odgovorno za opredelitev in odobritev obravnavane zadeve in z njo povezanih trditev. Strokovnjaki morajo zagotoviti, da vse trditve, ki jih je navedlo poslovodstvo, ustrezajo pričakovanjem dobro obveščenega bralca ali uporabnika v primerjavi z drugimi standardi uradnih določil.

2.1.4 Temeljni pogoj za sprejetje revizijskega posla je potrditev poslovodstva, da popolnoma razume svojo dolžnost, da strokovnjakom zagotovi vse zahtevane informacije v zvezi z obravnavano zadevo in trditvami. Če strokovnjaki menijo, da poslovodstvo te obveznosti ne bo moglo izpolniti, bi morali:

- obvestiti vodstvo dajanja zagotovil in revidiranja IS in pristojne za upravljanje o ugotovljeni zadevi,
- zavrniti predlagani revizijski posel.

2.1.5 Strokovnjaki naj bi pregledali izbrane trditve za revizijski posel in zagotovili, da so:

- **zadostne** – izpolnjujejo namen revizijskega posla, to je izdajo mnenja ali sklepa o obravnavani zadevi;
- **veljavne** – preizkusiti jih je mogoče glede na obravnavano zadevo;
- **ustrezne** – neposredno so povezane z obravnavano zadevo in prispevajo k izpolnitvi namena revizijskega posla.

2.2 Obravnavana zadeva in merila

2.2.1 Obravnavano zadevo revizijskega posla določijo poslovodstvo in pristojni za upravljanje. Običajno obravnavana zadeva revizijskega posla za IS ne bo tako točno opredeljena, kot je za finančne revizijske posle. Obravnavane zadeve poslov dajanja zagotovil in revidiranja IS se na primer lahko razlikujejo, od posameznega sistema in njegovih vmesnikov do procesa (ki zajema več sistemov in vmesnikov) ali celo do vseh operacij določenega oddelka, povezanih z IS.

2.2.2 Strokovnjaki naj bi ocenili obravnavano zadevo revizijskega posla na podlagi vnaprej določenih meril, da bi lahko izrazili mnenje ali sklep o obravnavani zadevi. Strokovnjaki naj bi ta merila ovrednotili in tako zagotovili, da res podpirajo zadevne trditve.

2.2.3 Posamezno merilo se lahko navezuje na več trditev. Po drugi strani pa lahko tudi eno samo trditev podpira več meril, ki dajejo delno zagotovilo za potrditev trditve.

2.2.4 Če bi strokovnjaki sklepali, da merila ne podpirajo popolnoma vseh ustreznih trditev, bi morali predlagati spremembo obstoječih meril ali dodatna merila. Vodstvo dajanja zagotovil in revidiranja IS pregleda in odobri ali zavrne nova ali spremenjena merila.

2.2.5 Poleg ocene, da merila popolnoma podpirajo zadevne trditve, naj bi strokovnjaki tudi presodili, ali je za merila mogoče opraviti nepristransko in merljivo analizo, kot je podrobneje opredeljeno v standardu 1008 Merila.

2007 Trditve *(nadaljevanje)*

2.3 Trditve, ki so jih navedle tretje stranke

2.3.1 Podjetja, ki oddajajo naloge v izvedbo tretjim strankam, bodo prejela poročila o kontrolnem okolju zunanjega izvajanja poslov. Poslovodstvo pregleda vsako poročilo, da ugotovi, ali:

- je poročilo izdala ustrezna neodvisna strokovna organizacija,
- je izdano revizijsko mnenje s pridržki ali brez pridržkov,
- obseg kontrolnih ciljev ustrezno zajema kontrole, ki jih podjetje zahteva,
- je pregledano obdobje v skladu s pričakovanji podjetja,
- so določene pomanjkljivosti kontrol (zaradi katerih poročilo sicer ni v celoti omejeno) za podjetje pomembne,
- so uporabljene trditve v skladu z zahtevanimi trditvami.

Vodstvo dajanja zagotovil in revidiranja IS naj bi dokumentiralo opravljeno analizo in ugotovljene sklepe. Strokovnjaki naj bi zagotovili, da so trditve preverjene in jih je poslovodstvo uradno potrdilo kot del revizijskega posla, opravljenega z zunanjim izvajanjem nalog. Standard 1206 Uporaba dela drugih strokovnjakov daje nadaljnja navodila o teh zadevah.

2.4 Sklep in poročilo

2.4.1 Po presoji obravnavane zadeve revizijskega posla na podlagi meril naj bi strokovnjaki oblikovali sklep o vsaki trditvi, in sicer na podlagi vseh ugotovitev po ustreznih merilih in svoje strokovne presoje.

2.4.2 Po oblikovanju sklepa naj bi strokovnjaki izdali posredno ali neposredno poročilo o obravnavani zadevi:

- **posredno poročilo** o trditvah o obravnavani zadevi, na primer o trditvi ‘popolnost’ za sestavino obravnavane zadeve: »Na podlagi našega preizkušanja uspešnosti delovanja so bile po našem mnenju spremembe sistema IT, predane v delovanje, v vseh pomembnih pogledih v skladu z izbranimi merili, v celoti evidentirane v aplikaciji za beleženje sprememb.«
- **neposredno poročilo** o obravnavani zadevi sami, na primer o celotni obravnavani zadevi: »Na podlagi našega preizkušanja so po našem mnenju spremembe sistema IT glede na izbrana merila v vseh pomembnih pogledih izvedene v skladu z zahtevanimi postopki upravljanja sprememb.«

3. Povezava s standardi in procesi v COBIT 5

3.0 Uvod

To poglavje daje pregled ustreznih:
3.1 Povezav s standardi
3.2 Povezav s procesi v COBIT 5
3.3 Drugih navodil

2007 Trditve *(nadaljevanje)*

3.1 Povezava s standardi

V tabeli je pregled:
- najpomembnejših standardov ISACA, ki jih neposredno podpira ta smernica;
- tistih zahtev standardov, ki so najpomembnejše za to smernico.

Opomba: Naštete so samo tiste zahteve standardov, ki so pomembne za to smernico.

Naslov standarda	Pomembne zahteve standarda
1007 Trditve	Strokovnjaki dajanja zagotovil in revidiranja IS morajo pregledati trditve, na podlagi katerih bodo presojali obravnavano zadevo, da bi ugotovili, ali je mogoče takšne trditve revidirati in ali so te trditve zadostne, veljavne in ustrezne.
1008 Merila	Strokovnjaki dajanja zagotovil in revidiranja IS morajo izbrati merila, po katerih se bo obravnavana zadeva presojala, ki so nepristranska, popolna, ustrezna, merljiva, razumljiva, splošno priznana, predpisana ter na voljo vsem bralcem in uporabnikom poročila.
1204 Pomembnost	Strokovnjaki dajanja zagotovil in revidiranja IS morajo v poročilu razkriti: • pomanjkanje kontrol ali neučinkovite kontrole, • pomembnost pomanjkljivosti kontrol, • verjetnost, da bodo te slabosti povzročile pomembno pomanjkljivost ali bistveno slabost.
1206 Uporaba dela drugih strokovnjakov	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.
1401 Poročanje	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.

3.2 Povezava s procesi v COBIT 5

V tabeli je pregled najpomembnejših:
- procesov v COBIT 5,
- namenov procesov v COBIT 5.

Posebne aktivnosti, ki se izvajajo kot del teh procesov, so v *COBIT 5: Omogočanje procesov*.

Proces v COBIT 5	Namen procesa
EDM01 Zagotovite vzpostavitev in vzdrževanje okvira upravljanja.	Zagotovite dosleden pristop, povezan in usklajen z načinom upravljanja podjetja. Da bodo odločitve za IT sprejete v skladu s strategijami in cilji podjetja, zagotovite, da so procesi, povezani z IT, uspešno in pregledno nadzorovani, da je skladnost z zakonskimi in drugimi predpisanimi zahtevami potrjena in da so izpolnjene upravljavske zahteve za člane organa nadzora.
MEA02 Spremljajte, vrednotite in ocenjujte sistem notranjih kontrol.	Ključnim deležnikom omogočite pregled nad ustreznostjo sistema notranjih kontrol in s tem zagotovite zaupanje v delovanje, vero v doseganje ciljev podjetja in ustrezno razumevanje preostalega tveganja.

3.3 Druga navodila

Pri izvajanju standardov in smernic naj strokovnjaki po potrebi poiščejo še druga navodila. Za dajanje zagotovil in revidiranje IS jih lahko pridobijo:
- od kolegov v podjetju in/ali zunaj njega, npr. prek strokovnih združenj ali strokovnih skupin na družbenih omrežjih,
- od vodstva,
- od organov upravljanja v podjetju, npr. od revizijske komisije,
- iz drugih navodil (npr. knjig, člankov, drugih smernic).

2007 Trditve *(nadaljevanje)*

4. Izrazi

Izraz	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.
Merila	Standardi in merila uspešnosti, ki se uporabljajo za merjenje in predstavitev obravnavane zadeve in na podlagi katerih revizor IS ovrednoti zadevo. Merila naj bi bila: • nepristranska – objektivna in brez predsodkov, • popolna – vključevala naj bi vse ustrezne dejavnike, ki vodijo do sklepa, • ustrezna – nanašala naj bi se na obravnavano zadevo, • merljiva – zagotavljala naj bi dosledno merjenje, • razumljiva. Pri poslih potrjevanja so to merila uspešnosti, s katerimi je mogoče preveriti pisne trditve poslovodstva glede obravnavane zadeve. Izvajalec pride do sklepa o obravnavani zadevi na podlagi primerjave z ustreznimi merili.
Strokovna presoja	Uporaba ustreznega znanja in izkušenj za ozaveščeno odločanje o ustreznem ukrepanju v okoliščinah posla dejanja zagotovil in revidiranja IS.
Obravnavana zadeva	Določene informacije, obdelane v poročilu in z njim povezanih postopkih revizorja IS, ki lahko vključujejo zadeve, kot so zasnova ali delovanje notranjih kontrol in skladnost s prakso ali standardi ali določenimi zakoni in predpisi o varovanju zasebnosti (področje dejavnosti).

5. Datum uveljavitve

5.1 Datum uveljavitve Ta smernica velja za vse posle dajanja zagotovil in revidiranja IS, ki se začnejo 1. septembra 2014 ali pozneje.

2008 Merila

Smernica je predstavljena v naslednjih poglavjih:
1. Namen smernice in povezava s standardi
2. Vsebina smernice
3. Povezava s standardi in procesi v COBIT 5
4. Izrazi
5. Datum uveljavitve

1. Namen smernice in povezava s standardi

1.0 Uvod

V tem poglavju so razjasnjeni:
1.1 Namen smernice
1.2 Povezava s standardi
1.3 Uporaba izrazov ‘revidiranje’ in ‘strokovnjaki’

1.1 Namen

1.1.1 Namen te smernice je pomagati strokovnjakom dajanja zagotovil in revidiranja IS pri izbiri meril, na podlagi katerih bo ocenjena obravnavana zadeva, ki so primerna, sprejemljiva in prihajajo iz pomembnega vira.

1.1.2 Strokovnjaki dajanja zagotovil in revidiranja IS naj bi upoštevali to smernico pri odločanju, kako izvajati standard, uporabiti strokovno presojo pri uporabi, utemeljiti vsako odstopanje in po potrebi poiskati dodatna navodila.

1.2 Povezava s standardi

1.2.1 Standard 1007 Trditve

1.2.2 Standard 1008 Merila

1.3 Uporaba izrazov

1.3.1 V nadaljnjem besedilu:
- se ‘dajanje zagotovil in revidiranje IS’ imenuje ‘revidiranje’;
- se ‘strokovnjaki dajanja zagotovil in revidiranja IS’ imenujejo ‘strokovnjaki’.

2. Vsebina smernice

2.0 Uvod

Poglavje o vsebini smernice je sestavljeno tako, da daje informacije o naslednjih ključnih temah posla dajanja zagotovil in revidiranja IS:
2.1 Izbira in uporaba meril
2.2 Primernost
2.3 Sprejemljivost
2.4 Vir
2.5 Sprememba meril med revizijskim poslom

2008 Merila *(nadaljevanje)*

2.1 Izbira in uporaba meril

2.1.1 Strokovnjaki morajo izbrati merila, po katerih se bo obravnavana zadeva presojala. Pri izbiri meril morajo strokovnjaki skrbno proučiti primernost, sprejemljivost in vir meril, kot je opisano v poglavjih 2.2, 2.3 in 2.4.

2.1.2 Strokovnjaki naj bi skrbno razmislili o izbiri meril. Upoštevanje lokalne zakonodaje in predpisov je pomembno in razumeti jih je treba kot obvezno zahtevo. Vsekakor pa velja, da mnogi revizijski posli vključujejo področja, kot so upravljanje sprememb, splošne kontrole IT in kontrole dostopa, ki jih zakonodaja ali drugi predpisi ne urejajo. Poleg tega so bile v določenih panogah, kot je na primer področje plačilnih kartic, vzpostavljene obvezne zahteve. Upoštevati je treba tudi pomembnost lokalnih in mednarodnih pravil o varstvu podatkov in predpisov o zasebnosti. Kadar zakonske zahteve temeljijo na načelih, naj bi strokovnjaki zagotovili, da izbrana merila ustrezajo ciljem revizije.

2.1.3 Uporaba primernih in sprejemljivih meril se zahteva zaradi zagotavljanja doslednega ocenjevanja obravnavane zadeve. Brez pravih meril bo vsak izoblikovan sklep ali mnenje mogoče napačno razumeti in ga bo bralec lahko tolmačil s svojega osebnega stališča.

2.1.4 Strokovnjaki bi se morali vzdržati ovrednotenja obravnavane zadeve na podlagi lastnih pričakovanj, izkušenj ali presoj, ker to ne bi bila primerna in sprejemljiva merila.

2.1.5 Kadar merila niso takoj na voljo, so nepopolna ali bi jih bilo mogoče različno tolmačiti, bi morali strokovnjaki vključiti opis in vse druge potrebne informacije in tako zagotoviti, da je poročilo pošteno, nepristransko in razumljivo, in je jasen miselni okvir, v katerem so merila uporabljena.

2.1.6 Strokovno presojo je treba uporabiti pri zagotavljanju, da bo uporaba meril omogočila pripravo poštenega in nepristranskega mnenja ali sklepa, ki bralca ali uporabnika ne bo zavajal. Znano pa je, da poslovodstvo lahko določi merila, ki ne izpolnjujejo vseh zahtev.

2.2 Primernost

2.2.1 Strokovnjaki naj bi ocenili primernost in ustreznost meril, uporabljenih za presojo obravnavane zadeve. Merilo 'lokalni zakon določa, da morajo pri posredovanju podatkov o poslih vsi osebni podatki stranke vedno ostati zasebni', se na primer uporablja za razjasnitev naslednjih značilnosti meril:

- **nepristranskost** – merila naj bi bila brez pristranskosti, ki bi negativno vplivala na ugotovitve in sklepe strokovnjakov in zavajala uporabnika revizijskega poročila, češ da je merilo nepristransko zato, ker ga je potrdila lokalna zakonodaja;
- **popolnost** – merila naj bi bila dovolj popolna, tako da so pri izvajanju revizijskega posla prepoznana in uporabljena vsa merila, ki bi lahko vplivala na sklepe strokovnjakov o obravnavani zadevi. Doseči je treba popolnost vseh uporabljenih meril glede na cilje revizijskega posla;
- **ustreznost** – merila naj bi bila ustrezna za obravnavano zadevo in naj bi prispevala k ugotovitvam in sklepom, ki izpolnjujejo cilje revizijskega posla. Ustreznost meril je lahko odvisna od vsebine; celo za isto obravnavano zadevo so merila lahko različna glede na cilje in okoliščine revizijskega posla; merilo je na primer ustrezno, ker so podatki o transakcijah vključeni v obseg tega revizijskega posla;
- **merljivost** – merila naj bi dovoljevala konsistentno merjenje obravnavane zadeve in pripravo dosledno enakih sklepov, kadar jih uporabljajo različni strokovnjaki v podobnih okoliščinah; merilo je na primer merljivo, ker je vse prenose podatkov o poslu z nezaščitenimi osebnimi podatki mogoče enotno prepoznati in jih konsistentno izmeriti;
- **razumljivost** – merila naj bi bila jasno sporočena, tako da jih predvideni uporabniki ne bi mogli bistveno različno razlagati; merilo je na primer razumljivo, ker je bilo za ta člen zakona izdanih že več sodnih odločb, ki pomagajo jasno razumeti izvajanje v praksi in tolmačenje zakona.

2.3 Sprejemljivost

2.3.1 Na sprejemljivost meril vpliva razpoložljivost revizijskega poročila uporabnikom, tako da uporabniki razumejo podlago za dajanje zagotovil in pomembnost ugotovitev in sklepov. Viri lahko vključujejo merila, ki so:

- **priznana** – dovolj splošno priznana, tako da njihova uporaba za predvidene uporabnike ni vprašljiva;
- **predpisana** – odražajo predpisane določbe na zadevnem področju in so ustrezna za obravnavano zadevo; predpisane določbe so lahko izdale strokovne organizacije, panožne skupine, vlada in upravni organi;
- **javno dostopna** – taka merila so med drugim standardi, ki so jih pripravile strokovne računovodske in revizijske organizacije, kot so ISACA, Mednarodna zveza računovodskih strokovnjakov (IFAC) in drugi priznani vladni ali strokovni organi;
- **na voljo vsem uporabnikom** – če merila niso javno dostopna, jih je treba sporočiti vsem uporabnikom prek trditev, ki predstavljajo del revizijskega poročila. Trditve vključujejo izjave o obravnavani zadevi, ki izpolnjujejo zahteve 'primernih meril', tako da jih je mogoče revidirati, kot je opisano v standardu 1007 Trditve.

2.3.2 Strokovnjaki naj bi zagotovili, da so merila, uporabljena v revizijskem poslu:

- **sprejeta zunaj organizacije** – priznana, predpisana in javno dostopna;
- **potrjena zunaj organizacije** – merila, ki jih je pripravilo poslovodstvo (za določen revizijski posel) ne veljajo za priznana, predpisana in javno dostopna. Pred njihovo uporabo mora taka merila preveriti in potrditi priznana neodvisna tretja stranka, da se zagotovi, da poslovodstvo prek njih ne vsiljuje želenega izida revizijskega posla.

2008 Merila *(nadaljevanje)*

2.4 Vir

2.4.1 Poleg primernost in razpoložljivosti je treba pri izbiri meril za dajanje zagotovil IS upoštevati tudi vir glede na njihovo uporabo in verjetne prejemnike. Pri obravnavanju vladnih predpisov na primer utegnejo biti najustreznejša merila, ki temeljijo na trditvah, pripravljenih v zakonodaji in predpisih, ki veljajo za obravnavano zadevo. V drugih primerih pa so lahko ustrezna merila panožnih ali trgovinskih združenj. Možni viri meril, navedeni po vrstnem redu upoštevanja, so:

- **merila, ki jih določa ISACA** – javno dostopna merila in standardi, ki so jih pregledali in s potrebno poklicno skrbnostjo preverili mednarodno priznani strokovnjaki s področja upravljanja, 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 poseben pravni pomen. Pogosto je treba pravna določila preoblikovati v trditve. Poleg tega lahko tolmačenje zakonodaje podajo samo člani pravne stroke;
- **merila, ki jih določajo organizacije, ki ne sledijo predpisanim postopkom** – ta vključujejo ustrezna merila, ki so jih pripravile druge organizacije, ki ne sledijo predpisanim postopkom skrbnega pregleda ter niso predmet javnega posvetovanja in razprave;
- **merila, razvita posebej za revizijski posel** – merila, pripravljena posebej za revizijski posel, so sicer lahko ustrezna, vendar je treba posebej paziti, da se zagotovi, da so ta merila res primerna in zlasti nepristranska, popolna in merljiva. Merila, pripravljena posebej za revizijski posel, imajo obliko trditev. Običajno so pripravljena tako, da upoštevajo potrebe določenega uporabnika. Kot uveljavljena merila za ocenjevanje uspešnosti sistema notranje kontrole je na primer mogoče uporabiti različne okvire; določen uporabnik pa utegne pripraviti skupek meril, ki ustrezajo določenim potrebam, na primer hierarhiji odobrenih potrditev. Strokovnjaki bi morali v revizijskem poročilu jasno navesti, da so bila nekatera merila razvita posebej za ta revizijski posel. Razmisliti bi morali, ali bi tako razvita merila lahko zavedla predvidenega uporabnika, po potrebi naj bi dali še več informacij o merilih. Ker je ta merila pripravilo poslovodstvo, je zanje treba pridobiti zunanjo potrditev in to navesti v poročilu, kot je opisano v točki 2.3.2.

2.5 Sprememba meril med revizijskim poslom

2.5.1 Ko revizija napreduje, so dodatne informacije in spoznanja o obravnavani zadevi lahko razlog za spremembo izbranih meril:

- nekatera merila morda ne bodo več potrebna za doseganje cilja revizije. V takih okoliščinah revizijsko delo, povezano z merili, ni več potrebno;
- za doseganje cilja revizije pa utegnejo biti potrebna še dodatna merila. V takih okoliščinah bodo dodatna merila izbrana in opravljeno bo tudi revizijsko delo, povezano s temi merili.

3. Povezava s standardi in procesi v COBIT 5

3.0 Uvod

To poglavje daje pregled ustreznih:
3.1 Povezav s standardi
3.2 Povezav s procesi v COBIT 5
3.3 Drugih navodil

3.1 Povezava s standardi

V tabeli je pregled:

- najpomembnejših standardov ISACA, ki jih neposredno podpira ta smernica;
- tistih zahtev standardov, ki so najpomembnejše za to smernico.

Opomba: Naštete so samo tiste zahteve standardov, ki so pomembne za to smernico.

Naslov standarda	Pomembne zahteve standarda
1007 Trditve	Strokovnjaki dajanja zagotovil in revidiranja IS morajo pregledati trditve, na podlagi katerih bodo presojali obravnavano zadevo, da bi ugotovili, ali je mogoče takšne trditve revidirati in ali so te trditve zadostne, veljavne in ustrezne.
1008 Merila	Strokovnjaki dajanja zagotovil in revidiranja IS morajo izbrati merila, po katerih se bo obravnavana zadeva presojala, ki so nepristranska, popolna, ustrezna, merljiva, razumljiva, splošno priznana, predpisana ter na voljo vsem bralcem in uporabnikom poročila.

2008 Merila *(nadaljevanje)*

3.2 Povezava s procesi v COBIT 5

V tabeli je pregled najpomembnejših:
- procesov v COBIT 5,
- namenov procesov v COBIT 5.

Posebne aktivnosti, ki se izvajajo kot del teh procesov, so v *COBIT 5: Omogočanje procesov*.

Proces v COBIT 5	Namen procesa
EDM01 Zagotovite vzpostavitev in vzdrževanje okvira upravljanja.	Zagotovite dosleden pristop, povezan in usklajen z načinom upravljanja podjetja. Da bodo odločitve za IT sprejete v skladu s strategijami in cilji podjetja, zagotovite, da so procesi, povezani z IT, uspešno in pregledno nadzorovani, da je skladnost z zakonskimi in drugimi predpisanimi zahtevami potrjena in da so izpolnjene upravljavske zahteve za člane organa nadzora.
MEA02 Spremljajte, vrednotite in ocenjujte sistem notranjih kontrol.	Ključnim deležnikom omogočite pregled nad ustreznostjo sistema notranjih kontrol in s tem zagotovite zaupanje v delovanje, vero v doseganje ciljev podjetja in ustrezno razumevanje preostalega tveganja.

3.3 Druga navodila

Pri izvajanju standardov in smernic naj strokovnjaki po potrebi poiščejo še druga navodila. Za dajanje zagotovil in revidiranje IS jih lahko pridobijo:
- od kolegov v podjetju in/ali zunaj njega, npr. prek strokovnih združenj ali strokovnih skupin na družbenih omrežjih,
- od vodstva,
- od organov upravljanja v organizaciji, npr. od revizijske komisije,
- iz drugih navodil (npr. knjig, člankov, drugih smernic).

4. Izrazi

Izraz	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.
Merila	Standardi in merila uspešnosti, ki se uporabljajo za merjenje in predstavitev obravnavane zadeve in na podlagi katerih revizor IS ovrednoti zadevo. Merila naj bi bila: • nepristranska – objektivna in brez predsodkov, • popolna – vključevala naj bi vse ustrezne dejavnike, ki vodijo do sklepa, • ustrezna – nanašala naj bi se na obravnavano zadevo, • merljiva – zagotavljala naj bi dosledno merjenje, • razumljiva. Pri poslih potrjevanja so to merila uspešnosti, s katerimi je mogoče preveriti pisne trditve poslovodstva glede obravnavane zadeve. Izvajalec pride do sklepa o obravnavani zadevi na podlagi primerjave z ustreznimi merili.
Strokovna presoja	Uporaba ustreznega znanja in izkušenj za ozaveščeno odločanje o ustreznem ukrepanju v okoliščinah posla dejanja zagotovil in revidiranja IS.
Obravnavana zadeva	Določene informacije, obdelane v poročilu in z njim povezanih postopkih revizorja IS, ki lahko vključujejo zadeve, kot so zasnova ali delovanje notranjih kontrol in skladnost s prakso ali standardi ali določenimi zakoni in predpisi o varovanju zasebnosti (področje dejavnosti).

5. Datum uveljavitve

5.1 Datum uveljavitve

Ta smernica velja za vse posle dajanja zagotovil in revidiranja IS, ki se začnejo 1. septembra 2014 ali pozneje.

Izvedbene smernice

Izvedbene smernice so:
2201 Načrtovanje posla
2202 Ocenjevanje tveganja pri revizijskem načrtovanju
2203 Izvedba in nadzor
2204 Pomembnost
2205 Dokazi
2206 Uporaba dela drugih strokovnjakov
2207 Nepravilnosti in nezakonita dejanja
2208 Vzorčenje

Smernice so tukaj vključene v celoti. Za povezave s posameznimi standardi obiščite *www.isaca.org/standard*.

2201 Načrtovanje posla

Smernica je predstavljena v naslednjih poglavjih:
1. Namen smernice in povezava s standardi
2. Vsebina smernice
3. Povezava s standardi in procesi v COBIT 5
4. Izrazi
5. Datum uveljavitve

1. Namen smernice in povezava s standardi

1.0 Uvod

V tem poglavju so razjasnjeni:
1.1 Namen smernice
1.2 Povezava s standardi
1.3 Uporaba izrazov ‘revidiranje’ in ‘strokovnjaki’

1.1 Namen

1.1.1 Ta smernica daje navodila strokovnjakom dajanja zagotovil in revidiranja IS. Ustrezno načrtovanje jim pomaga zagotoviti, da bo primerna pozornost namenjena pomembnim področjem revizije, da bodo morebitne težave pravočasno prepoznane in rešene ter da bo revizijski posel pravilno, uspešno in učinkovito organiziran, voden in izveden.

1.1.2 Strokovnjaki dajanja zagotovil in revidiranja IS naj bi upoštevali to smernico pri določanju, kako izvajati standard, uporabiti strokovno presojo pri uporabi, utemeljiti vsako odstopanje in po potrebi poiskati dodatna navodila.

1.2 Povezava s standardi

1.2.1 Standard 1201 Načrtovanje posla
1.2.2 Standard 1202 Ocenjevanje tveganja pri revizijskem načrtovanju
1.2.3 Standard 1203 Izvedba in nadzor
1.2.4 Standard 1204 Pomembnost

1.3 Uporaba izrazov

1.3.1 V nadaljnjem besedilu:
- se ‘dajanje zagotovil in revidiranje IS’ imenuje ‘revidiranje’;
- se ‘strokovnjaki dajanja zagotovil in revidiranja IS’ imenujejo ‘strokovnjaki’.

2. Vsebina smernice

2.0 Uvod

Poglavje o vsebini smernice je sestavljeno tako, da daje informacije o naslednjih ključnih temah posla dajanja zagotovil in revidiranja IS:
2.1 Revizijski načrt za IS
2.2 Cilji
2.3 Obseg in poznavanje poslovanja
2.4 Na tveganjih temelječ pristop
2.5 Dokumentiranje projektnega načrta revizijskega posla
2.6 Spremembe med potekom revizije

2201 Načrtovanje posla *(nadaljevanje)*

2.1 Revizijski načrt za IS

2.1.1 Za funkcijo revidiranja je treba najmanj enkrat na leto pripraviti in posodobiti celovit revizijski načrt za IS na podlagi tveganj. Opredeliti je treba tudi večletni pogled naprej (za tri do pet let) in ga vključiti v letni načrt. Večletni in letni načrti naj bodo okvir za aktivnosti dajanja zagotovil in revidiranja IS in so namenjeni obravnavanju zadolžitev, določenih z revizijsko listino.

2.1.2 Revizijski načrt za IS naj bi bil pripravljen tako, da je skladen z vsemi ustreznimi zunanjimi zahtevami in veljavnimi standardi ISACA.

2.1.3 Vsak revizijski posel naj bi se skliceval na revizijski načrt za IS ali pa vseboval posebno pooblastilo, cilje in druge pomembne vidike dela, ki ga je treba opraviti.

2.2 Cilji

2.2.1 Strokovnjaki naj bi opredelili cilje revizijskega posla in jih dokumentirali v projektnem načrtu revizijskega posla, tako da jih bodo uspešno izvedli. Cilje posla je treba določiti zato, da bodo obravnavana tveganja povezana s pregledovano dejavnostjo.

2.2.2 Strokovnjaki naj bi pripravili projektni načrt revizijskega posla, v katerem so upoštevani cilji revizijskega posla. Ti cilji lahko vplivajo na revizijski posel, npr. na potrebne vire, časovni načrt in izdelke.

2.3 Obseg in poznavanje poslovanja

2.3.1 Pred začetkom revizijskega posla je treba delo strokovnjakov ustrezno načrtovati, da se dosežejo revizijski cilji. V okviru načrtovalnega procesa naj bi strokovnjaki spoznali podjetje in njegove procese. To jim bo pomagalo določiti pomembnost virov, ki se pregledujejo, saj so ti povezani s cilji podjetja. Na ta način se strokovnjaki lahko osredotočijo na področja, ki so najobčutljivejša za prevare ali netočna ravnanja. Določili naj bi obseg revizijskega dela in izvedli tudi predhodno oceno notranjih kontrol nad funkcijo, ki jo pregledujejo.

2.3.2 Strokovnjaki naj bi spoznali vse vrste zaposlenih, dogodkov, poslov in ravnanj, ki lahko pomembno vplivajo na določeno podjetje, funkcijo, proces ali podatke, ki so predmet revizijskega posla. Poznavanje podjetja naj vključuje poslovna in finančna tveganja, s katerimi se podjetje sooča, kakor tudi razmere na trgu podjetja ter obseg zunanjega izvajanja del, ki ga podjetje uporablja za doseganje svojih ciljev. Strokovnjaki naj te informacije uporabijo pri prepoznavanju morebitnih težav, oblikovanju ciljev in obsega dela, pri izvajanju dela in preiskovanju ukrepov poslovodstva, na katere bi morali biti pozorni.

2.4 Na tveganjih temelječ pristop

2.4.1 Strokovnjaki naj bi pripravili projektni načrt revizijskega posla, da bi zmanjšali revizijsko tveganje na sprejemljivo raven.

2.4.2 Ocenjevanje tveganja je potrebno za sprejemljivo zagotovilo, da bodo vse pomembne postavke ustrezno obdelane med izvajanjem revizijskega posla in bodo strokovnjaki lahko prišli do sklepa. S to oceno naj bi prepoznali področja, na katerih so pomembne težave zelo verjetne.

2.4.3 Oceno tveganj in razvrstitev prepoznanih tveganj po pomembnosti za pregledovano področje in za okolje IS v podjetju je treba izvesti v potrebnem obsegu.

2.4.4 V postopku načrtovanja naj strokovnjaki praviloma določijo ravni pomembnosti načrtovanja, tako da bo revizijsko delo zadoščalo za dosego revizijskih ciljev in bodo revizijski viri učinkovito uporabljeni. Pri pregledu obstoječega sistema naj bi na primer strokovnjaki pri načrtovanju revizijskega posla za delo, ki ga je treba opraviti, ovrednotili pomembnost različnih sestavin sistema. Pri določanju pomembnosti je treba upoštevati tako kakovostne kot tudi količinske vidike.

2.4.5 Pred začetkom revizijskega posla in med izvajanjem revizije naj bi strokovnjaki upoštevali skladnost z veljavnimi zakoni in strokovnimi revizijskimi standardi.

2.4.6 Kadar strokovnjaki ocenjujejo notranje kontrole, da ugotovijo, koliko se lahko zanesejo na kontrolne postopke v podporo informacijam, ki so jih zbrali kot del širše revizije (kakršna je na primer revizija računovodskih informacij iz prejšnjih obdobij), naj bi praviloma predhodno ocenili kontrole in na podlagi teh ocen pripravili projektni načrt revizijskega posla.

2201 Načrtovanje posla *(nadaljevanje)*

2.5 Dokumentiranje projektnega načrta revizijskega posla

2.5.1 Delovno gradivo strokovnjakov bi moralo vključevati projektni načrt revizijskega posla.

2.5.2 Jasna opredelitev projekta je zelo pomemben dejavnik uspeha, ki zagotavlja uspešnost in učinkovitost projekta. Projektni načrt revizijskega posla naj v opisu nalog in pristojnosti vključuje postavke, kot so:

- Področja, ki jih je treba revidirati;
- vrsta načrtovanega dela;
- visokoravenski cilji in obseg dela;
- razgovori za ugotavljanje dejstev, ki jih je treba opraviti;
- pomembne informacije, ki jih je treba pridobiti;
- postopki za preverjanje ali potrditev pridobljenih informacij in njihova uporaba za revizijske dokaze;
- splošne teme, kot so na primer:
  - proračun,
  - razpoložljivost in dodelitev virov,
  - predvideni datumi,
  - vrsta poročila,
  - predvideni prejemniki,
  - izidi;
- posebne teme, kot so na primer:
  - določitev orodij, potrebnih za zbiranje dokazov, izvajanje preizkusov in pripravo/povzetek informacij za poročanje,
  - merila za presojo, ki jih bo treba uporabiti,
  - zahteve poročanja in razpošiljanje;
- drugi splošni vidiki dela, kadar je to primerno.

2.5.3 Projektni načrt naj vključuje zahteve, povezane s časovnim načrtom revizijskega posla, kot so obravnavano obdobje in različni končni datumi, da bo revizijski posel izveden v dogovorjenem roku. To vključuje tudi proračunske izdatke.

2.5.4 Strokovnjaki naj bi zagotovili popolno pokritost potrebne strokovne usposobljenosti virov revizijskega posla. Sestavili naj bi skupino za revizijski posel, ki ima prave veščine, znanje in izkušnje za uspešno dokončanje revizijskega posla. Strokovnjaki naj bi tudi poskrbeli, da bodo članom skupine za revidiranje IS dodeljene različne vloge in zadolžitve, ki najbolje ustrezajo njihovi strokovni usposobljenosti. Več informacij o tem najdete v Standardu 1203 Izvedba in nadzor.

2.5.5 V projektnem načrtu revizijskega posla naj bi bili našteti vsi izdelki, povezani z revizijskim poslom.

2.5.6 Projektni načrt revizijskega posla in vse njegove kasnejše spremembe naj bi odobrilo vodstvo dajanja zagotovil in revidiranja IS.

2.5.7 Po odobritvi vodstva dajanja zagotovil in revidiranja IS je treba dele projektnega načrta revizijskega posla (npr. obseg, časovni načrt, zahteve glede dokumentacije, razpored razgovorov) pravočasno sporočiti revidirancem, da bodo poskrbeli za ustrezen in popoln dostop do potrebne dokumentacije in virov ter njihovo razpoložljivost.

2.6 Spremembe med potekom revizije

2.6.1 Med potekom revizijskega posla je treba projektni načrt revizijskega posla po potrebi posodabljati in spreminjati.

2.6.2 Načrtovanje revizijskega posla je nenehen in ponavljajoč se proces. Zaradi nepričakovanih dogodkov, spremenjenih razmer ali pridobljenih revizijskih dokazov morajo strokovnjaki prilagoditi načrtovane vrsto, čas in obseg nadaljnjih revizijskih postopkov.

2.6.3 Revizijski načrt naj bi upošteval možnost nepričakovanih dogodkov, ki pomenijo tveganje za podjetje. Zato naj bi projektni načrt revizijskega posla omogočal prednostno obravnavo takih dogodkov v postopkih revidiranja in dajanja zagotovil na podlagi tveganj.

---

3. Povezava s standardi in procesi v COBIT 5

3.0 Uvod

To poglavje daje pregled ustreznih:

3.1 Povezav s standardi
3.2 Povezav s procesi v COBIT 5
3.3 Drugih navodil

2201 Načrtovanje posla *(nadaljevanje)*

3.1 Povezava s standardi

V tabeli je pregled:
- najpomembnejših standardov ISACA, ki jih neposredno podpira ta smernica;
- tistih zahtev standardov, ki so najpomembnejše za to smernico.

Opomba: Naštete so samo tiste zahteve standardov, ki so pomembne za to smernico.

Naslov standarda	Pomembne zahteve standarda
1201 Načrtovanje posla	Strokovnjaki dajanja zagotovil in revidiranja IS morajo načrtovati vsak posel dajanja zagotovil in revidiranja IS z namenom, da obravnavajo: • 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 značilna za posel, • zahteve glede dokumentacije in poročanja. Strokovnjaki dajanja zagotovil in revidiranja IS morajo pripraviti in dokumentirati projektni načrt posla dajanja zagotovil ali 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	Pri dajanju zagotovil in revidiranju IS morata biti za pripravo celotnega načrta revidiranja IS in določitev prednosti za učinkovito dodelitev virov za revizijo IS uporabljena ustrezen pristop in pripadajoča metodologija za oceno tveganja. Strokovnjaki dajanja zagotovil in revidiranja IS morajo pri načrtovanju posameznih poslov prepoznati in oceniti tveganje, ki se nanaša na področje pregleda.
1203 Izvedba in nadzor	Strokovnjaki dajanja zagotovil in revidiranja IS morajo delo opraviti skladno z odobrenim načrtom revidiranja IS in v dogovorjenih rokih, da zajamejo prepoznana tveganja.
1204 Pomembnost	Strokovnjaki dajanja zagotovil in revidiranja IS morajo pri načrtovanju posla upoštevati morebitne slabosti ali pomanjkanje kontrol in pretehtati, ali bi bila posledica teh slabosti ali pomanjkanja kontrol lahko pomembna pomanjkljivost ali bistvena slabost.

3.2 Povezava s procesi v COBIT 5

V tabeli je pregled najpomembnejših:
- procesov v COBIT 5,
- namenov procesov v COBIT 5.

Posebne aktivnosti, ki se izvajajo kot del teh procesov, so v *COBIT 5: Omogočanje procesov*.

Proces v COBIT 5	Namen procesa
MAE01 Spremljajte, vrednotite in ocenjujte uspešnost in skladnost.	Zagotovite preglednost izvajanja in skladnost ter spodbujajte doseganje ciljev.
MEA02 Spremljajte, vrednotite in ocenjujte sistem notranjih kontrol.	Ključnim deležnikom omogočite pregled nad ustreznostjo sistema notranjih kontrol in s tem zagotovite zaupanje v delovanje, vero v doseganje ciljev podjetja in ustrezno razumevanje preostalega tveganja.
MEA03 Spremljajte, vrednotite in ocenjujte skladnost z zunanjimi zahtevami.	Zagotovite, da podjetje ravna v skladu z vsemi veljavnimi zunanjimi zahtevami.

2201 Načrtovanje posla *(nadaljevanje)*

3.3 Druga navodila Pri izvajanju standardov in smernic naj strokovnjaki po potrebi poiščejo še druga navodila. Za dajanje zagotovil in revidiranje IS jih lahko pridobijo:

- od kolegov v podjetju in/ali zunaj njega, npr. prek strokovnih združenj ali strokovnih skupin na družbenih omrežjih,
- od vodstva,
- od organov upravljanja v organizaciji, npr. od revizijske komisije,
- iz drugih navodil (npr. knjig, člankov, drugih smernic).

4. Izrazi

Izraz	Pomen
Revizijski načrt	1. Načrt, ki vsebuje vrsto, čas in obseg revizijskih postopkov, ki jih morajo opraviti člani skupine za posel, da pridobijo zadostne in ustrezne revizijske dokaze za oblikovanje mnenja. Opomba vključuje področja, ki jih je treba revidirati, vrsto načrtovanega dela, visokoravenske cilje in obseg dela ter teme, kot so proračun, dodelitev virov, predvideni datumi, vrsta poročila in predvideni prejemniki ter drugi splošni vidiki dela. 2. Opis revizijskega dela na visoki ravni, ki ga je treba opraviti v določenem roku.
Revizijsko tveganje	Tveganje za sprejem nepravilnega sklepa na podlagi ugotovitev revizije zajema tri sestavine revizijskega tveganja: • tveganje pri kontroliranju, • tveganje pri odkrivanju, • tveganje pri delovanju.
Pomembnost	Revizijski koncept, ki zadeva pomembnost informacije glede na njen vpliv ali učinek na pregledovano področje. Izraz relativne pomembnosti ali pomembnosti za neko določeno zadevo v kontekstu posla ali 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.

5. Datum uveljavitve

5.0 Datum uveljavitve Ta smernica velja za vse posle dajanja zagotovil in revidiranja IS, ki se začnejo 1. septembra 2014 ali pozneje.

2202 Ocenjevanje tveganja pri revizijskem načrtovanju

Smernica je predstavljena v naslednjih poglavjih:
1. Namen smernice in povezava s standardi
2. Vsebina smernice
3. Povezava s standardi in procesi v COBIT 5
4. Izrazi
5. Datum uveljavitve

1. Namen smernice in povezava s standardi

1.0 Uvod

V tem poglavju so razjasnjeni:
1.1 Namen smernice
1.2 Povezava s standardi
1.3 Uporaba izrazov ‘revidiranje’ in ‘strokovnjaki’

1.1 Namen

1.1.1 Stopnja revizijskega dela, potrebnega za izpolnitev cilja revizije, je subjektivna odločitev strokovnjakov dajanja zagotovil in revidiranja IS. Namen te smernice je zmanjšati tveganje, da pride do nepravilnega sklepa na podlagi ugotovitev revizije, in zmanjšati obstoj napak na pregledovanem področju.

1.1.2 Smernica daje navodila pri uporabi pristopa za oceno tveganja, da se pripravi:
- revizijski načrt za IS, ki zajema vse letne revizijske posle,
- projektni načrt revizijskega posla, ki se osredotoča na določen revizijski posel.

1.1.3 Smernica navaja podrobnosti različnih vrst tveganj, s katerimi se srečujejo strokovnjaki dajanja zagotovil in revidiranja IS.

1.1.4 Strokovnjaki dajanja zagotovil in revidiranja IS naj bi upoštevali to smernico pri določanju, kako izvajati standard, uporabiti strokovno presojo pri uporabi, utemeljiti vsako odstopanje in po potrebi poiskati dodatna navodila.

1.2 Povezava s standardi

1.2.1 Standard 1201 Načrtovanje posla
1.2.2 Standard 1202 Ocenjevanje tveganja pri načrtovanju
1.2.3 Standard 1203 Izvedba in nadzor
1.2.4 Standard 1204 Pomembnost
1.2.5 Standard 1207 Nepravilnosti in nezakonita dejanja

1.3 Uporaba izrazov

1.3.1 V nadaljnjem besedilu:
- se ‘dajanje zagotovil in revidiranje IS’ imenuje ‘revidiranje’;
- se ‘strokovnjaki dajanja zagotovil in revidiranja IS’ imenujejo ‘strokovnjaki’.

2. Vsebina smernice

2.0 Uvod

Poglavje o vsebini smernice je sestavljeno tako, da daje informacije o naslednjih ključnih temah posla dajanja zagotovil in revidiranja IS:
2.1 Ocena tveganja revizijskega načrta za IS
2.2 Metodologija za ocenjevanje tveganja
2.3 Ocena tveganja posameznih revizijskih poslov
2.4 Revizijsko tveganje
2.5 Tveganje pri delovanju
2.6 Tveganje pri kontroliranju
2.7 Tveganje pri odkrivanju

2202 Ocenjevanje tveganja pri revizijskem načrtovanju *(nadaljevanje)*

2.1 Ocena tveganja revizijskega načrta za IS

2.1.1 Pri pripravi celovitega revizijskega načrta za IS je treba uporabiti primeren pristop za ocenjevanje tveganj. Ocenjevanje tveganj je treba izvesti in dokumentirati najmanj enkrat letno, kar omogoča lažjo pripravo revizijskega načrta za IS. Ta naj upošteva strateške načrte in cilje organizacije ter okvir in pobude za upravljanje tveganj podjetja.

2.1.2 Za pravilno in popolno oceno tveganja, ki je povezano s celotnim obsegom področja revizije IS, naj bi strokovnjaki pri pripravi revizijskega načrta za IS upoštevali naslednje:
- popolno pokritost vseh področij v obsegu revidiranja IS, kar predstavlja vse mogoče revizijske aktivnosti,
- zanesljivost in primernost ocene tveganja, ki jo je dalo poslovodstvo,
- postopke poslovodstva za nadziranje in proučevanje morebitnega tveganja ali drugih zadev in poročanje o njih,
- pokrivanje tveganja v povezanih dejavnostih, pomembnih za pregledovane dejavnosti.

2.1.3 Uporabljeni pristop za ocenjevanje tveganj naj bi pomagal pri prednostnem in časovnem razporejanju dela pri dajanju zagotovil in revidiranju IS. Podpiral naj bi izbiro področij in postavk, ki so za revizijo zanimivi, in proces odločanja pri zasnovi in izvajanju določenih poslov revidiranja IS.

2.1.4 Strokovnjaki naj bi zagotovili, da so uporabljeni pristop za ocenjevanje tveganj odobrili pristojni za upravljanje in je bil razposlan različnim deležnikom posla.

2.1.5 Strokovnjaki naj bi uporabili ocene tveganj za opredelitev količine in utemeljitev zneska virov za revizijo IS, potrebnih za dokončanje revizijskega načrta za IS, in zahtev za posebne posle.

2.1.6 Na podlagi ocene tveganj/-a, naj bi strokovnjaki pripravili revizijski načrt za IS, ki predstavlja okvir za aktivnosti dajanja zagotovil in revidiranja IS. Ta načrt naj:
- upošteva zahteve in aktivnosti dajanja zagotovil in revidiranja, ki niso povezane z IS,
- bo posodobljen najmanj enkrat na leto,
- odobrijo pristojni za upravljanje,
- obravnava zadolžitve, določene z revizijsko listino.

Več informacij lahko najdete v Standardu 1201 Načrtovanje posla.

2.2 Metodologija za ocenjevanje tveganja

2.2.1 Strokovnjaki naj upoštevajo ustrezno metodologijo za ocenjevanje tveganj, da zagotovijo popolno in natančno pokritost revizijskih poslov v revizijskem načrtu za IS.

2.2.2 Strokovnjaki naj v metodologijo vključijo vsaj analizo tveganj za podjetje, ki so povezana z razpoložljivostjo sistema, celovitostjo podatkov in zaupnostjo poslovnih informacij.

2.2.3 Na voljo je veliko metodologij za ocenjevanje tveganj, ki podpirajo proces ocenjevanja tveganj. Zajemajo vse od preprostih razvrstitev v velika, srednja in majhna tveganja na podlagi presoje strokovnjakov do bolj količinskih in znanstvenih izračunov, ki dajejo številčno oceno tveganja, in drugih, ki so kombinacija navedenih. Strokovnjaki naj upoštevajo raven zapletenosti in podrobnosti, ustrezne za podjetje ali enote, ki jih revidirajo. Posebna navodila za ocenjevanje tveganj lahko najdete tudi v publikaciji ISACA *COBIT 5 for Risk*.

2.2.4 Vse metodologije za ocenjevanje tveganj se na določeni točki v procesu (npr. pri dodeljevanju pomembnosti različnim parametrom) opirajo na subjektivne presoje. Strokovnjaki bi morali vedeti, katere subjektivne odločitve so potrebne pri uporabi določene metodologije, in pretehtati, ali take presoje lahko ustrezno opredelijo in jih preverijo, da dosežejo primerno raven natančnosti.

2.2.5 Pri odločanju o najustreznejši metodologiji za ocenjevanje tveganj naj bi strokovnjaki upoštevali 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 kolikšni 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 revizij,
- pripravljenost pristojnih za upravljanje na področju revizije IS, da sprejmejo to metodologijo kot sredstvo za določanje vrste in ravni opravljenega revizijskega dela.

2.2.6 Od nobene metodologije za ocenjevanje tveganj ni mogoče pričakovati, da bo ustrezna v vseh okoliščinah. Okoliščine, ki vplivajo na revizije, se sčasoma lahko spremenijo. Zato naj bi strokovnjaki občasno ponovno ocenili ustreznost izbrane metodologije za ocenjevanje tveganj.

2202 Ocenjevanje tveganja pri revizijskem načrtovanju *(nadaljevanje)*

2.2. Metodologija za ocenjevanje tveganja (nadaljevanje)

2.2.7 Strokovnjaki naj bi pri pripravi celovitega revizijskega načrta za IS in pri načrtovanju posebnih revizijskih poslov uporabili izbrane tehnike ocenjevanja tveganj. Ocenjevanje tveganj v povezavi z drugimi revizijskimi tehnikami je treba upoštevati pri načrtovalnih odločitvah, kot so:

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

2.2.8 Izidi sprejete metodologije za ocenjevanje tveganj bi morali biti konsistentni, veljavni, primerljivi in ponovljivi. Ocene tveganj, pridobljene s to metodologijo, bi morale biti konsistentne (za celo obdobje), veljavne, primerljive (s prejšnjimi/poznejšimi ocenami, dobljenimi po isti metodologiji ocenjevanja) in ponovljive (podoben splet dejstev in uporaba iste metodologije ocenjevanja bosta dala podoben izid).

2.3 Ocena tveganja posameznih revizijskih poslov

2.3.1 Pri načrtovanju posameznega posla naj bi strokovnjaki prepoznali in ocenili tveganje, ki se nanaša na področje pregleda. Izidi te ocene tveganja naj bi se odražali v ciljih revizijskega posla. Med ocenjevanjem tveganja naj strokovnjaki upoštevajo:

- izide prejšnjih revizijskih poslov, pregledov in ugotovitev, vključno z vsemi popravljalnimi aktivnostmi,
- vseobsegajoči proces ocenjevanja tveganj v podjetju,
- verjetnost pojava določenega tveganja,
- vpliv določenega tveganja (v denarni ali drugi obliki vrednosti), če se pojavi.

2.3.2 Strokovnjaki naj bi pred ocenjevanjem tveganja zagotovili, da popolnoma razumejo dejavnosti področja. Deležnike in druge ustrezne stranke naj zaprosijo za pripombe in predloge, kar je potrebno, da pravilno določijo in proučijo vpliv možnega tveganja na revizijske posle.

2.3.3 Cilj ocenjevanja tveganj je zmanjšati revizijsko tveganje na sprejemljivo nizko raven in prepoznati tiste dele dejavnosti, na katere se mora revizija bolj usmeriti. To je treba opraviti z ustrezno oceno obravnavane zadeve IS in s tem povezanih kontrol pri načrtovanju in izvajanju revizije.

2.3.4 Pri načrtovanju določenega postopka dajanja zagotovil in revidiranja IS naj bi se strokovnjaki zavedali dejstva, da so pri nižje postavljenem pragu pomembnosti revizijska pričakovanja natančnejša in bo revizijsko tveganje večje.

2.3.5 Pri načrtovanju določenega postopka dajanja zagotovil in revidiranja IS morajo strokovnjaki upoštevati možnost nezakonitih dejanj, zaradi katerih bo treba spremeniti vrsto, čas in obseg obstoječih postopkov. Več informacij lahko najdete v Standardu 1207 Nepravilnosti in nezakonita dejanja in v Smernici 2207.

2.3.6 Kadar je revizijsko tveganje visoko ali je prag pomembnosti nižji, naj bi strokovnjaki bodisi razširili obseg ali vrsto revizijskih preizkusov bodisi povečali oz. razširili preizkušanje podatkov, da bi pridobili dodatna zagotovila.

2.4 Revizijsko tveganje

2.4.1 Revizijsko tveganje se nanaša na tveganje, da pride do nepravilnega sklepa na podlagi ugotovitev revizije. Tri sestavine revizijskega tveganja so:

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

2.4.2 Strokovnjaki naj bi proučili vsako od sestavin tveganja, da bi določili celovito raven tveganja. To vključuje tveganje obravnavane zadeve, ki vključuje tveganje pri delovanju in tveganje pri kontroliranju; skupaj s tveganjem pri odkrivanju potem predstavlja revizijsko tveganje. Nadaljnjo obravnavo različnih sestavin revizijskega tveganja lahko najdete v poglavjih 2.5 do 2.7.

2.5 Tveganje pri delovanju

2.5.1 Tveganje pri delovanju je dovzetnost revizijskega področja za napako na način, ki utegne biti pri delovanju posamično ali z drugimi napakami pomemben ob predpostavki, da ni bilo nobenih ustreznih notranjih kontrol. Tveganje pri delovanju, povezano z operacijskimi sistemi brez ustreznih kontrol, je na primer običajno veliko, ker bi spremembe podatkov ali programov ali celo njihovo razkritje zaradi slabosti pri varnosti operacijskega sistema lahko povzročili napačne poslovodne informacije ali slabšo konkurenčno prednost. Nasprotno pa je tveganje pri delovanju, povezano z varnostjo za nepovezan osebni računalnik brez kontrol, običajno nizko, če ustrezna analiza pokaže, da se ne uporablja za poslovno kritične namene.

2.5.2 Tveganje pri delovanju je za večino revizijskih področij IS veliko, ker morebitni učinki napak običajno segajo na več poslovnih sistemov in uporabnikov.

2202 Ocenjevanje tveganja pri revizijskem načrtovanju *(nadaljevanje)*

2.6 Tveganje pri kontroliranju

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

2.6.2 Strokovnjaki naj tveganje pri kontroliranju ocenijo kot veliko, razen če so ustrezne notranje kontrole:
- ugotovljene,
- ocenjene kot uspešne,
- preizkušene in dokazano ustrezno delujejo.

2.6.3 Strokovnjaki naj upoštevajo tako vseobsegajoče kot tudi podrobne kontrole IS:
- Vseobsegajoče kontrole IS so podsklop splošnih kontrol; to so tiste splošne kontrole, ki so usmerjene v upravljanje in spremljanje okolja IS. Zato vplivajo na vse aktivnosti, povezane z IS. Vpliv vseobsegajočih kontrol IS na delo strokovnjakov ni omejen na zanesljivost aplikativnih kontrol v sistemih poslovnega procesa. Vplivajo tudi na zanesljivost podrobnih kontrol IS, npr. nad razvojem aplikacijskega programa, uvajanjem sistemov, administracijo varnosti in postopki varnostnega kopiranja. Šibke vseobsegajoče kontrole IS in slabo upravljanje in spremljanje okolja IS morajo strokovnjake opozoriti na možnost velikega tveganja, da utegnejo biti kontrole, zasnovane za delovanje na podrobni ravni, neuspešne.
- Podrobne kontrole IS sestavljajo aplikativne kontrole in tiste splošne kontrole, ki niso vključene v vseobsegajoče kontrole IS. Po okviru COBIT so to kontrole nabave, uvajanja, dobave in podpore sistemov in storitev IS.

2.6.4 Tveganje, ki bi ga strokovnjaki morali upoštevati, so omejitve in pomanjkljivosti v podrobnih kontrolah IS, ki so posledica neustreznih vseobsegajočih kontrol IS.

2.7 Tveganje pri odkrivanju

2.7.1 Tveganje pri odkrivanju je tveganje, da strokovnjaki s postopki preizkušanja podatkov ne bodo odkrili 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 veliko, ker med revizijo dnevniki za celotno obdobje revizije niso na voljo. Tveganje pri odkrivanju, povezano z ugotavljanjem, da ni načrtov za obnovo po katastrofi, je običajno majhno, ker je njihov obstoj lahko preveriti.

2.7.2 Pri določanju ravni potrebnega preizkušanja podatkov morajo strokovnjaki upoštevati:
- oceno tveganja pri delovanju,
- sklepe glede tveganja pri kontroliranju po preizkušanju skladnosti.

2.7.3 Višje kot sta ocenjena tveganje pri delovanju in tveganje pri kontroliranju, več revizijskih dokazov morajo strokovnjaki običajno pridobiti pri izvajanju revizijskih postopkov preizkušanja podatkov.

2202 Ocenjevanje tveganja pri revizijskem načrtovanju *(nadaljevanje)*

3. Povezava s standardi in procesi v COBIT 5

3.0 Uvod

To poglavje daje pregled ustreznih:
3.1 Povezav s standardi
3.2 Povezav s procesi v COBIT 5
3.3 Drugih navodil

3.1 Povezava s standardi

V tabeli je pregled:
- najpomembnejših standardov ISACA, ki jih neposredno podpira ta smernica;
- tistih zahtev standardov, ki so najpomembnejše za to smernico.

Opomba: Naštete so samo tiste zahteve standardov, ki so pomembne za to smernico.

Naslov standarda	Pomembne zahteve standarda
1201 Načrtovanje posla	Strokovnjaki dajanja zagotovil in revidiranja IS morajo načrtovati vsak posel dajanja zagotovil in revidiranja IS z namenom, da obravnavajo: • 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 značilna za posel, • zahteve glede dokumentacije in poročanja.
1202 Ocenjevanje tveganja pri načrtovanju	Pri dajanju zagotovil in revidiranju IS morata biti za pripravo celotnega načrta revidiranja IS in določitev prednosti za učinkovito dodelitev virov za revizijo IS uporabljena ustrezen pristop in pripadajoča metodologija za oceno tveganja. Strokovnjaki dajanja zagotovil in revidiranja IS morajo pri načrtovanju posameznih poslov prepoznati in oceniti tveganje, ki se nanaša na področje pregleda. Strokovnjaki dajanja zagotovil in revidiranja IS morajo proučiti tveganja, povezana z obravnavano zadevo, revizijsko tveganje in vpliv na izpostavljenost podjetja.
1203 Izvedba in nadzor	Strokovnjaki dajanja zagotovil in revidiranja IS morajo delo opraviti skladno z odobrenim načrtom revidiranja IS in v dogovorjenih rokih, da zajamejo prepoznana tveganja.
1204 Pomembnost	Strokovnjaki dajanja zagotovil in revidiranja IS morajo pri načrtovanju posla upoštevati morebitne slabosti ali pomanjkanje kontrol in pretehtati, ali bi bila posledica teh slabosti ali pomanjkanja kontrol lahko pomembna pomanjkljivost ali bistvena slabost. 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. Strokovnjaki dajanja zagotovil in revidiranja IS morajo upoštevati skupni učinek manjših pomanjkljivosti ali slabosti kontrol in možnost, da se pomanjkanje kontrol prevede v pomembno pomanjkljivost ali bistveno slabost. Strokovnjaki dajanja zagotovil in revidiranja IS morajo v poročilu razkriti: • pomanjkanje kontrol ali neučinkovite kontrole, • pomembnost pomanjkljivosti kontrol, • verjetnost, da bodo te slabosti povzročile pomembno pomanjkljivost ali bistveno slabost.
1207 Nepravilnosti in nezakonita dejanja	Strokovnjaki dajanja zagotovil in revidiranja IS morajo med izvajanjem posla upoštevati tveganja nepravilnosti in nezakonitih dejanj.

2202 Ocenjevanje tveganja pri revizijskem načrtovanju *(nadaljevanje)*

3.2 Povezava s procesi v COBIT 5

V tabeli je pregled najpomembnejših:
- procesov v COBIT 5,
- namenov procesov v COBIT 5.

Posebne aktivnosti, ki se izvajajo kot del teh procesov, so v *COBIT 5: Omogočanje procesov*.

Proces v COBIT 5	Namen procesa
EDM01 Zagotovite vzpostavitev in vzdrževanje okvira upravljanja.	Zagotovite dosleden pristop, povezan in usklajen z načinom upravljanja podjetja. Da bodo odločitve za IT sprejete v skladu s strategijami in cilji podjetja, zagotovite, da so procesi, povezani z IT, uspešno in pregledno nadzorovani, da je skladnost z zakonskimi in drugimi predpisanimi zahtevami potrjena in da so izpolnjene upravljavske zahteve za člane organa nadzora.
EDM03 Zagotovite optimizacijo tveganja.	Zagotovite, da tveganje, povezano z IT v podjetju, ne preseže pripravljenosti za prevzemanje tveganj in sprejemljivega tveganja, da je vpliv tveganja IT na vrednost podjetja prepoznan in obvladovan ter da so možnosti za neskladnost s predpisi čim manjše.
APO12 Upravljajte tveganje.	Združite upravljanje tveganja, povezanega z IT, s celotnim obvladovanjem tveganja v podjetju (ERM) in izravnajte stroške in koristi upravljanja tveganja, povezanega z IT v podjetju.
MEA02 Spremljajte, vrednotite in ocenjujte sistem notranjih kontrol.	Ključnim deležnikom omogočite pregled nad ustreznostjo sistema notranjih kontrol in s tem zagotovite zaupanje v delovanje, vero v doseganje ciljev podjetja in ustrezno razumevanje preostalega tveganja.
MEA03 Spremljajte, vrednotite in ocenjujte skladnost z zunanjimi zahtevami.	Zagotovite, da podjetje ravna v skladu z vsemi veljavnimi zunanjimi zahtevami.

3.3 Druga navodila

Pri izvajanju standardov in smernic naj strokovnjaki po potrebi poiščejo še druga navodila. Za dajanje zagotovil in revidiranje IS jih lahko pridobijo:
- od kolegov v podjetju in/ali zunaj njega, npr. prek strokovnih združenj ali strokovnih skupin na družbenih omrežjih,
- od vodstva,
- od organov upravljanja v organizaciji, npr. od revizijske komisije,
- iz drugih navodil (npr. knjig, člankov, drugih smernic).

2202 Ocenjevanje tveganja pri revizijskem načrtovanju *(nadaljevanje)*

4. Izrazi

Izraz	Pomen
Revizijska listina	Dokument, ki ga odobrijo pristojni za upravljanje in opredeljuje namen, pristojnost in zadolžitve notranje revizije za dajanje zagotovil in revidiranja IS. Revizijska listina naj bi: • vzpostavila položaj notranje revizije za dajanje zagotovil in revidiranja IS v podjetju, • odobrila dostop do zapisov, osebja ter prostorov in opreme, ki so pomembni za opravljanje poslov dajanja zagotovil in revidiranja IS, • določila obseg aktivnosti revidiranja.
Revizijsko tveganje	Tveganje za sprejem nepravilnega sklepa na podlagi ugotovitev revizije zajema tri sestavine revizijskega tveganja: • tveganje pri kontroliranju, • tveganje pri odkrivanju, • tveganje pri delovanju.
Tveganje pri kontroliranju	Tveganje, da obstaja pomembna napaka, ki je sistem notranjih kontrol ne more pravočasno preprečiti ali odkriti. Glej tveganje pri delovanju.
Podrobne kontrole IS	Kontrole nad nabavo, uvajanjem, dobavo in podporo sistemov in storitev IS, ki jih sestavljajo aplikativne kontrole in tiste splošne kontrole, ki niso vključene v vseobsegajoče kontrole.
Tveganje pri odkrivanju	Tveganje, da strokovnjak dajanja zagotovil ali revidiranja IS s postopki preizkušanja podatkov ne bo odkril napake, ki bi posamično ali v povezavi z drugimi napakami lahko bila pomembna. Glej revizijsko tveganje.
Tveganje pri delovanju	Raven tveganja ali izpostavljenosti brez upoštevanja dejanj, ki jih je poslovodstvo izvedlo ali bi jih lahko izvedlo (npr. uvajanje kontrol). Glej tveganje pri kontroliranju.
Pomembnost	Revizijski koncept, ki zadeva pomembnost informacije glede na njen vpliv ali učinek na pregledovano področje. Izraz relativne pomembnosti ali pomembnosti za neko določeno zadevo v kontekstu posla ali 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.
Vseobsegajoče kontrole IS	Splošne kontrole, ki so zasnovane za upravljanje in spremljanje okolja IS in zato vplivajo na vse aktivnosti, povezane z IS.
Preizkušanje podatkov	Pridobivanje revizijskih dokazov o popolnosti, točnosti ali obstoju aktivnosti ali transakcij v obdobju revidiranja.

5. Datum uveljavitve

5.1 Datum uveljavitve Ta smernica velja za vse posle dajanja zagotovil in revidiranja IS, ki se začnejo 1. septembra 2014 ali pozneje.

2203 Izvedba in nadzor

Smernica je predstavljena v naslednjih poglavjih:
1. Namen smernice in povezava s standardi
2. Vsebina smernice
3. Povezava s standardi in procesi v COBIT 5
4. Izrazi
5. Datum uveljavitve

1. Namen smernice in povezava s standardi

1.0 Uvod

V tem poglavju so razjasnjeni:
1.1 Namen smernice
1.2 Povezava s standardi
1.3 Uporaba izrazov ‘revidiranje’ in ‘strokovnjaki’

1.1 Namen

1.1.1 Ta smernica daje strokovnjakom dajanja zagotovil in revidiranja IS navodila pri izvajanju revizijskega posla in nadziranju članov skupine za revidiranje IS. Vključuje:
- izvajanje revizijskega posla,
- vloge in zadolžitve, zahtevano znanje in veščine za izvajanje revizijskih poslov,
- ključne vidike nadzora,
- zbiranje dokazov,
- dokumentiranje opravljenega dela,
- oblikovanje ugotovitev in sklepov.

1.1.2 Strokovnjaki dajanja zagotovil in revidiranja IS naj bi upoštevali to smernico pri odločanju, kako izvajati standard, uporabiti strokovno presojo pri uporabi, utemeljiti vsako odstopanje in po potrebi poiskati dodatna navodila.

1.2 Povezava s standardi

1.2.1 Standard 1005 Potrebna poklicna skrbnost
1.2.2 Standard 1006 Strokovna usposobljenost
1.2.3 Standard 1201 Načrtovanje posla
1.2.4 Standard 1203 Izvedba in nadzor
1.2.5 Standard 1205 Dokazi
1.2.6 Standard 1401 Poročanje

1.3 Uporaba izrazov

1.3.1 V nadaljnjem besedilu:
- se ‘dajanje zagotovil in revidiranje IS’ imenuje ‘revidiranje’;
- se ‘strokovnjaki dajanja zagotovil in revidiranja IS’ imenujejo ‘strokovnjaki’.

2. Vsebina smernice

2.0 Uvod

Poglavje o vsebini smernice je sestavljeno tako, da daje informacije o naslednjih ključnih temah posla dajanja zagotovil in revidiranja IS:
2.1 Izvajanje dela
2.2 Vloge in zadolžitve, znanje in veščine
2.3 Nadzor
2.4 Dokazi
2.5 Dokumentiranje
2.6 Ugotovitve in sklepi

2203 Izvedba in nadzor *(nadaljevanje)*

2.1 Izvajanje dela

2.1.1 Strokovnjaki naj bi vsak revizijski posel načrtovali in izvajali v skladu odobrenim revizijskim načrtom za IS. Oblikovanje projektnega načrta revizijskega posla, kot je podrobno opisano v Standardu 1201 Načrtovanje posla, omogoča strokovnjakom, da razumejo vse elemente in obseg ter zahtevane veščine in znanje za izvedbo revizijskega posla v dogovorjenem roku in pri tem pokrijejo vsa prepoznana tveganja.

2.1.2 Glavne naloge pri izvajanju revizijskega posla so med drugim:

- **načrtovanje in ocenjevanje tveganj** – strokovnjaki naj bi te aktivnosti izvajali v skladu s standardoma 1201 Načrtovanje posla in 1202 Ocenjevanje tveganja pri načrtovanju;
- **prepoznavanje kontrol** – na podlagi obsega, ciljev revizije in glavnih področij tveganja, ugotovljenih v revizijskem načrtu IS, naj strokovnjaki ugotovijo kontrole v obsegu revizijskega posla;
- **ocena kontrol in zbiranje dokazov** – strokovnjaki naj kontrole v obsegu posla ocenijo z zbiranjem in preiskovanjem informacij in dokazov o uspešnosti zasnove in uspešnosti delovanja kontrol, kot je opisano v standardu 1205 Dokazi;
- **dokumentiranje opravljenega dela in opredelitev ugotovitev** – strokovnjaki naj dokumentirajo opravljeno delo, zapišejo zbrane informacije in dokaze ter dokumentirajo vse prepoznane ugotovitve;
- **potrjevanje ugotovitev in nadaljnje spremljanje popravljalnih ukrepov** – strokovnjaki naj svoje ugotovitve potrdijo pri revidirancu. Če revidiranec izvede popravljalne ukrepe za ugotovitve še pred koncem revizijskega posla, naj strokovnjaki sprejete ukrepe vključijo v dokumentacijo (in sklepe), vendar naj bi vedno omenili tudi prvotne ugotovitve;
- **oblikovanje sklepov in poročanje** – strokovnjaki naj oblikujejo sklepe in poročajo o vplivu ugotovitev na doseganje revizijskih ciljev, kot je podrobno opisano v standardu 1401 Poročanje. Ni dovolj, da se osredotočijo samo na ugotovitve glede kontrol brez presoje vpliva na cilje revizije.

2.2 Vloge in zadolžitve, znanje in veščine

2.2.1 Strokovnjaki, odgovorni za revizijski posel, naj bi določili in upravljali vloge in zadolžitve članov skupine za revidiranje IS ves čas izvajanja posla, pri čemer naj obravnavajo vsaj:

- oblikovanje metodologije in pristopa,
- pripravo programov revizijskega dela,
- opredelitev vlog pri izvajanju in pregledu,
- reševanje vprašanj, skrbi in težav, ko se pojavijo,
- dokumentiranje in pojasnjevanje ugotovitev,
- pisanje poročila.

2.2.2 Na podlagi potreb posla naj bi odgovorni strokovnjaki upoštevali zahtevano strokovno usposobljenost za določen revizijski posel. Sestaviti bi morali skupino za posel, v kateri so združeni veščine, znanje in izkušnje za uspešno dokončanje revizijskega posla. Strokovnjaki naj bi zagotovili, da bodo članom skupine za revidiranje IS dodelili tiste vloge in zadolžitve, ki se najbolje ujemajo z njihovimi sposobnostmi.

2.2.3 Strokovnjaki lahko sprejmejo samo vloge, zadolžitve in sorodne naloge, ki so v okviru njihovega znanja in veščin. Glede na čas in stroške usposabljanja strokovnjaki morda niso mogli pridobiti vseh potrebnih znanj in veščin pred začetkom revizijskega posla; zato je strokovnjakom dovoljeno sprejeti vloge, zadolžitve in sorodne naloge, če upravičeno pričakujejo, da bodo med izvajanjem revizijskega posla sprejeti ustrezni ukrepi za zagotavljanje uspešnega dokončanja posla. Tako upravičeno pričakovanje omogočajo naslednji ukrepi:

- **učenje na delovnem mestu** – v nekaterih okoliščinah bodo strokovnjaki lahko pridobili potrebne veščine in znanje med izvajanjem revizijskega posla;
- **nadzor** – odgovorni strokovnjaki bi lahko organizirali ustrezno nadziranje članov skupine za revidiranje IS, kar bi jim omogočilo, da pod nadzorom uspešno opravijo nalogo;
- **zunanji viri** – odgovorni strokovnjaki bi lahko razmislili tudi o najemanju zunanjih strokovnjakov za tista področja revizijskega posla, na katerih nimajo ustreznega notranjega znanja in veščin. Odgovorni strokovnjak naj razmisli o krepitvi razvoja članov notranje skupine za revidiranje IS tako, da ti tesno sodelujejo z zunanjimi strokovnjaki; tako se zagotovi prenos znanja in veščin v skupino.

2.2.4 Navodila o pridobivanju, vzdrževanju in spremljanju zahtevane usposobljenosti so podrobno navedena v standardu 1006 Strokovna usposobljenost.

2203 Izvedba in nadzor *(nadaljevanje)*

2.3 Nadzor

2.3.1 Vsako nalogo, ki jo med revizijskim poslom izvedejo člani skupine za revidiranje IS, naj bi nadzorovali strokovnjaki, zadolženi za nadzor nad njimi, da se zagotovi izpolnitev revizijskih ciljev in veljavnih strokovnih revizijskih standardov. Obseg potrebnega nadzora bo v veliki meri odvisen od veščin, znanja in izkušenj strokovnjakov, ki izvajajo pregledovane naloge, in od zapletenosti revizijskega posla.

2.3.2 Nadzor je proces, ki je navzoč v vseh fazah revizijskega posla in vključuje:
- zagotavljanje, da imajo člani skupine za revidiranje IS veščine, znanje in izkušnje za uspešno dokončanje revizijskega posla;
- zagotavljanje, da sta sestavljena in odobrena ustrezen projektni načrt revizijskega posla in program revizijskega dela;
- pregledovanje delovnega gradiva revizijskega posla;
- zagotavljanje, da je obveščanje revidirancev in drugih pomembnih deležnikov o revizijskem poslu točno, jasno, zgoščeno, nepristransko, konstruktivno in pravočasno;
- zagotavljanje, da je odobreni program dela revizijskega posla na koncu revizijskega posla izpolnjen, razen če niso bile vnaprej utemeljene in odobrene spremembe, in da so cilji revizijskega posla izpolnjeni;
- zagotavljanje priložnosti članom skupine za revidiranje IS, da razvijejo svoje veščine in znanje.

2.3.3 Pregledovanje delovnega gradiva revizijskega posla je potrebno za zagotovitev, da so vsi potrebni revizijski postopki izvedeni, da so zbrani dokazi zadostni in ustrezni in da ugotovitve ustrezno podpirajo cilje posla in sklep ali mnenje. Glede na namen pregleda bi tega morali izvajati člani skupine za revidiranje IS, ki so zadolženi za nadzor nad strokovnjaki, ki so pripravili delovno gradivo revizijskega posla.

2.3.4 Med pregledovanjem si morajo pregledovalci zapisovati vprašanja. Ko strokovnjaki odgovorijo na zastavljena vprašanja ali jih rešijo, je treba zagotoviti, da se shranijo zadostni in ustrezni dokazi o tem, da so bila vprašanja zastavljena, obravnavana in odgovorjena.

2.3.5 Ustrezne dokaze pregleda je treba dokumentirati in jih shraniti. Možnosti za dokumentiranje dokazov o izvajanju pregleda so med drugim, da se:
- vsako delovno gradivo revizijskega posla po pregledu podpiše in datira,
- izpolni kontrolni seznam pregleda delovnega gradiva revizijskega posla,
- pripravi podpisana listina, na kateri se navede delovno gradivo revizijskega posla, ki je pregledano, in podrobno opišejo vrsta, čas, obseg in izid pregleda.

Vse te možnosti so veljavne tako v elektronski obliki kot na papirju.

2.3.6 Nadzor omogoča razvoj in ocenjevanje strokovnjakov. Pregledovalci imajo posebne pravice pregleda opravljenega dela drugih članov skupine za revidiranje, kar jim omogoča podrobno in ustrezno ocenitev uspešnosti pri delu. Pregledovalci naj bi opozorili na področja potrebnega izpopolnjevanja in svetovali, kako izboljšati veščine in znanje.

2.4 Dokazi

2.4.1 Strokovnjaki naj bi pridobili dokaze, ki so zadostni in ustrezni za oblikovanje mnenja ali podporo sklepom in doseganje revizijskih ciljev. Ali so dokazi zadostni in ustrezni, je treba ugotavljati na podlagi pomembnosti cilja revizije in napora, potrebnega za pridobitev dokazov.

2.4.2 Strokovnjaki naj bi pridobili dodatne dokaze, če bi presodili, da pridobljeni dokazi ne izpolnjujejo meril zadostnosti in ustreznosti za oblikovanje mnenja ali podporo sklepom in doseganje revizijskih ciljev.

2.4.3 Strokovnjaki naj bi izbrali najustreznejši postopek za zbiranje dokazov glede na obravnavano zadevo revizije.

2.4.4 Strokovnjaki naj bi upoštevali vir in naravo pridobljenih dokazov, da ovrednotijo njihovo zanesljivost in ocenijo, ali je potrebno nadaljnje preverjanje.

2.4.5 Strokovnjaki naj dokaze ustrezno analizirajo in razložijo, da z njimi podprejo revizijske ugotovitve in oblikujejo sklepe. Prejete dokaze in informacije naj primerjajo s pričakovanji, ki so jih sami prepoznali ali izoblikovali. Zavedati pa bi se morali možnosti:
- nepričakovanih razlik,
- da razlik ne bo tam, kjer so bile pričakovane,
- morebitnih napak,
- prevar ali nezakonitih dejanj,
- neskladnosti z zakoni ali predpisi,
- neobičajnih ali enkratnih aktivnosti.

2.4.6 Če ugotovijo odstopanja od pričakovanj, naj bi strokovnjaki vprašali poslovodstvo o razlogih za razliko. Če je pojasnilo poslovodstva v skladu s strokovno presojo ustrezno, morajo strokovnjaki spremeniti svoja pričakovanja in ponovno analizirati dokaze in informacije.

2.4.7 Pomembna odstopanja, ki jih revidiranec ne more ustrezno pojasniti, naj bodo vključena med revizijske ugotovitve in sporočena izvršnemu vodstvu ali pristojnim za upravljanje. Odvisno od okoliščin bi strokovnjaki lahko priporočili ustrezno ukrepanje.

2.4.8 Podrobna navodila o različnih vrstah dokazov, postopkov za zbiranje dokazov, uporabnih virih, načinih ocenjevanja dokazov itd. lahko najdete v standardu 1205 Dokazi.

2203 Izvedba in nadzor *(nadaljevanje)*

2.5 Dokumentiranje

2.5.1 Strokovnjaki naj bi pravočasno pripravili zadostno, primerno in ustrezno dokumentacijo, ki daje podlago za sklep in vsebuje dokaze izvedenega pregleda. Zadostna, primerna in ustrezna dokumentacija naj bi omogočala, da razsodna in obveščena oseba, ki prej ni bila povezana z revizijskim poslom, ponovno izvede naloge, ki so bile opravljene med izvajanjem revizijskega posla, in pride do enakega sklepa. Dokumentacija naj vključuje:

- cilje revizijskega posla in obseg dela,
- projektni načrt revizijskega posla,
- program revizijskega dela,
- izvedene faze revizije,
- zbrane dokaze,
- sklepe in priporočila.

2.5.2 Dokumentacija pomaga pri načrtovanju, izvajanju in pregledovanju revizijskih poslov, ker:

- opredeli, kdo izmed članov skupine za revidiranje IS je izvedel posamezno revizijsko nalogo in kakšna je njegova vloga pri pripravi in pregledu dokumentacije,
- evidentira potrebne dokaze,
- podpira točnost, popolnost in veljavnost opravljenega dela,
- zagotavlja podporo za sprejete sklepe,
- omogoča lažje pregledovanje,
- dokumentira, ali so bili cilji posla doseženi,
- daje podlago programom za izboljšanje kakovosti.

2.5.3 Običajno naj bi strokovnjaki določili predhodni program pregleda še pred začetkom dela. Ta program revizije je treba dokumentirati tako, da strokovnjakom dovoljuje dokumentiranje dokončanega revizijskega dela in pregled dela, ki ga bo treba še opraviti. Med potekom dela naj strokovnjaki ocenijo ustreznost revizijskega programa na podlagi informacij, zbranih med izvajanjem revizijskega posla. Če strokovnjaki ugotovijo, da načrtovani postopki niso zadostni, naj ustrezno spremenijo revizijski program.

2.5.4 Izvedbene in nadzorne aktivnosti je treba dokumentirati v delovnem gradivu revizijskega posla. Zasnova in vsebina delovnega gradiva revizijskega posla se spreminjata glede na okoliščine določenega revizijskega posla. Vsekakor pa bi moralo vodstvo dajanja zagotovil in revidiranja IS podrobno določiti omejeno število standardnih predlog delovnega gradiva za različne vrste revizijskih poslov. Standardno delovno gradivo izboljšuje učinkovitost revizijskega posla in omogoča lažji nadzor. Vodstvo dajanja zagotovil in revidiranja IS naj določi tudi nosilce podatkov, ki se uporabljajo, ter postopke za skladiščenje in hranjenje delovnega gradiva.

2.5.5 Strokovnjaki naj bi zagotovili, da je dokumentacija opravljenega dela pravočasno dokončana. Vse informacije in dokaze, potrebne za oblikovanje sklepa ali mnenja, je treba pridobiti pred datumom izdaje revizijskega poročila. Delovno gradivo revizijskega posla naj bi imelo datum, ko je bilo gradivo pripravljeno in pregledano.

2.5.6 Delovno gradivo revizijskega posla je last podjetja. Vodstvo dajanja zagotovil in revidiranja IS nadzira delovno gradivo in zagotavlja dostop pooblaščenemu osebju. Zaprosila zunanjih revizorjev za dostop do delovnega gradiva revizijskega posla morajo odobriti izvršno vodstvo in pristojni za upravljanje. Zaprosila za dostop zunanjih strank, ki niso zunanji revizorji, naj bi odobrili izvršno vodstvo in pristojni za upravljanje po nasvetu pravnega svetovalca.

2.6 Ugotovitve in sklepi

2.6.1 Strokovnjaki naj analizirajo zbrane dokaze in informacije, kot je opisano v točki 2.4.5. Pomembna odstopanja od pričakovanj bi se morala odraziti v ugotovitvah. Strokovnjaki naj bi te ugotovitve potrdili pri revidirancu, potrdili pa naj bi tudi vpliv teh ugotovitev na druge vidike kontrolnega okolja.

2.6.2 Strokovnjaki lahko predlagajo popravljalne ukrepe, vendar jih sami ne bodo nikoli izvajali. Če revidiranec izvede popravljalne ukrepe, ki izboljšajo prvotno ugotovitev, še pred koncem revizijskega posla, morajo strokovnjaki sprejete popravljalne ukrepe vključiti v dokumentacijo.

2.6.3 Strokovnjaki naj bi sprejeli sklepe o prepoznanih ugotovitvah in ocenili njihov vpliv na revizijske cilje. Sklepi naj bi bili izoblikovani za prvotne ugotovitve. Če so bili izvedeni popravljalni ukrepi, se lahko oblikuje dodatek k sklepu, v katerem je pojasnjen popravljalni ukrep in njegov vpliv na prvotni sklep.

2.6.4 Vsi izoblikovani sklepi in izjava, ali so bili cilji revizije doseženi ali ne, naj bi bili dokumentirani v poročilu revizijskega posla. Podrobna navodila o poročanju lahko najdete v standardu 1401 Poročanje in smernici 2401 Poročanje.

2203 Izvedba in nadzor *(nadaljevanje)*

3. Povezava s standardi in procesi v COBIT 5

3.0 Uvod

To poglavje daje pregled ustreznih:
3.1 Povezav s standardi
3.2 Povezav s procesi v COBIT 5
3.3 Drugih navodil

3.1 Povezava s standardi

V tabeli je pregled:
- najpomembnejših standardov ISACA, ki jih neposredno podpira ta smernica;
- tistih zahtev standardov, ki so najpomembnejše za to smernico.

Opomba: Naštete so samo tiste zahteve standardov, ki so pomembne za to smernico.

Naslov standarda	Pomembne zahteve standarda
1005 Potrebna poklicna skrbnost	Strokovnjaki dajanja zagotovil in revidiranja IS morajo pri načrtovanju in izvajanju poslov ter poročanju o izidih ravnati s potrebno poklicno skrbnostjo, vključno z upoštevanjem veljavnih strokovnih standardov za revizijo.
1006 Strokovna usposobljenost	Strokovnjaki dajanja zagotovil in revidiranja IS morajo imeti 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. Strokovnjaki dajanja zagotovil in revidiranja IS morajo imeti s sodelavci pri nalogi ustrezno znanje o obravnavani zadevi.
1201 Načrtovanje posla	Strokovnjaki dajanja zagotovil in revidiranja IS morajo načrtovati vsak posel dajanja zagotovil in revidiranja IS z namenom, da obravnavajo: • 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 značilna za posel, • zahteve glede dokumentacije in poročanja. Strokovnjaki dajanja zagotovil in revidiranja IS morajo pripraviti in dokumentirati projektni načrt posla dajanja zagotovil ali revidiranja IS, ki opisuje: • vrsto posla, cilje, časovni načrt in zahteve glede virov, • časovno razporeditev in obseg revizijskih postopkov za izvedbo posla.
1203 Izvedba in nadzor	Strokovnjaki dajanja zagotovil in revidiranja IS morajo delo opraviti skladno z odobrenim načrtom revidiranja IS in v dogovorjenih rokih, da zajamejo prepoznana tveganja. Za doseganje revizijskih ciljev in spoštovanje veljavnih strokovnih revizijskih standardov morajo strokovnjaki dajanja zagotovil in revidiranja IS nadzirati osebje, ki izvaja revizije IS in za katero so zadolženi. Strokovnjaki dajanja zagotovil in revidiranja IS lahko sprejmejo samo naloge, ki so v okviru njihovega strokovnega znanja in veščin, ali naloge, za katere upravičeno pričakujejo, da bodo veščine pridobili med izvajanjem posla ali da jih bodo opravili pod nadzorom. 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. Strokovnjaki dajanja zagotovil in revidiranja IS morajo revizijski postopek dokumentirati z opisi revizijskega dela in revizijskimi dokazi, ki podpirajo ugotovitve in sklepe. Strokovnjaki dajanja zagotovil in revidiranja IS morajo prepoznavati in sklepati na podlagi ugotovitev.

2203 Izvedba in nadzor *(nadaljevanje)*

3.1 Povezava s standardi (nadaljevanje)

Naslov standarda	Pomembne zahteve standarda
1205 Dokazi	Strokovnjaki dajanja zagotovil in revidiranja IS morajo pridobiti zadostne in ustrezne dokaze, da lahko sprejmejo primerne sklepe, s katerimi utemeljijo izide posla. Strokovnjaki dajanja zagotovil in revidiranja IS morajo ovrednotiti zadostnost dokazov, pridobljenih za utemeljitev sklepov in doseganje ciljev posla.
1401 Poročanje	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. Strokovnjaki dajanja zagotovil in revidiranja IS morajo zagotoviti, da so ugotovitve v revizijskem poročilu podprte z zadostnimi in ustreznimi revizijskimi dokazi.

3.2 Povezava s procesi v COBIT 5

V tabeli je pregled najpomembnejših:
- procesov v COBIT 5,
- namenov procesov v COBIT 5.

Posebne aktivnosti, ki se izvajajo kot del teh procesov, so v *COBIT 5: Omogočanje procesov*.

Proces v COBIT 5	Namen procesa
APO07 Upravljajte človeške vire.	Optimizirajte zmožnosti človeških virov za doseganje ciljev podjetja.
APO08 Upravljajte razmerja.	Ustvarjajte izboljšane izide, povečujte zaupanje, vero v IT in uspešno rabo virov.
MEA02 Spremljajte, vrednotite in ocenjujte sistem notranjih kontrol.	Ključnim deležnikom omogočite pregled nad ustreznostjo sistema notranjih kontrol in s tem zagotovite zaupanje v delovanje, vero v doseganje ciljev podjetja in ustrezno razumevanje preostalega tveganja.

3.3 Druga navodila

Pri izvajanju standardov in smernic naj strokovnjaki po potrebi poiščejo še druga navodila. Za dajanje zagotovil in revidiranje IS jih lahko pridobijo:
- od kolegov v podjetju in/ali zunaj njega, npr. prek strokovnih združenj ali strokovnih skupin na družbenih omrežjih,
- od vodstva,
- od organov upravljanja v organizaciji, npr. od revizijske komisije,
- iz drugih navodil (npr. knjig, člankov, drugih smernic).

2203 Izvedba in nadzor *(nadaljevanje)*

4. Izrazi

Izraz	Pomen
Kontrolno okolje	Stališča in delovanje organa nadzora in (poslo)vodstva v zvezi s pomembnostjo kontroliranja v organizaciji. Kontrolno okolje zagotavlja red in organiziranost za doseganje temeljnih ciljev ureditve notranjega kontroliranja in nadzora. Kontrolno okolje sestavljajo: • neoporečnost in etične vrednote, • filozofija poslovodenja in slog delovanja, • organizacijski ustroj, • dodelitev pristojnosti in nalog, • usmeritve in običaji pri ravnanju z ljudmi, • sposobnost zaposlenih. Vir: Mednarodni standardi strokovnega ravnanja pri notranjem revidiranju, 2010.
Uspešnost zasnove	Če kontrole v družbi delujejo tako, kot so predpisale osebe, ki imajo potrebne pristojnosti in usposobljenost za uspešno izvajanje nadzora, zadovoljujejo kontrolne cilje družbe in lahko uspešno preprečujejo ali odkrivajo napake ali prevare, ki bi bile lahko razlog za pomembno napačne navedbe v računovodskih izkazih, velja, da so uspešno zasnovane. Vir: PCAOB, Standard revidiranja št. 5, 2007.
Uspešnost delovanja	Če kontrole delujejo tako, kot so jih zasnovale osebe, ki imajo potrebne pristojnosti in usposobljenost za uspešno izvajanje nadzora, velja, da kontrole uspešno delujejo. Vir: PCAOB, Standard revidiranja št. 5, 2007.

5. Datum uveljavitve

5.1 Datum uveljavitve Ta smernica velja za vse posle dajanja zagotovil in revidiranja IS, ki se začnejo 1. septembra 2014 ali pozneje.

2204 Pomembnost

Smernica je predstavljena v naslednjih poglavjih:
1. Namen smernice in povezava s standardi
2. Vsebina smernice
3. Povezava s standardi in procesi v COBIT 5
4. Izrazi
5. Datum uveljavitve

1. Namen smernice in povezava s standardi

1.0 Uvod

V tem poglavju so razjasnjeni:
1.1 Namen smernice
1.2 Povezava s standardi
1.3 Uporaba izrazov ‘revidiranje’ in ‘strokovnjaki’

1.1 Namen

1.1.1 Namen te smernice je jasno opredeliti pojem ‘pomembnost’ za strokovnjake dajanja zagotovil in revidiranja IS in jasno opozoriti na razliko s pojmom pomembnosti, kot ga uporabljajo strokovnjaki za finančno revizijo in dajanje zagotovil.

1.1.2 Smernica pomaga strokovnjakom dajanja zagotovil in revidiranja IS pri presoji pomembnosti obravnavane zadeve in preiskovanju pomembnosti v odnosu do kontrol in zadev, o katerih je treba poročati.

1.1.3 Strokovnjaki dajanja zagotovil in revidiranja IS naj bi upoštevali to smernico pri odločanju, kako izvajati standard, uporabiti strokovno presojo pri uporabi, utemeljiti vsako odstopanje in po potrebi poiskati dodatna navodila.

1.2 Povezava s standardi

1.2.1 Standard 1201 Načrtovanje posla
1.2.2 Standard 1202 Ocenjevanje tveganja in načrtovanje
1.2.3 Standard 1204 Pomembnost
1.2.4 Standard 1207 Nepravilnosti in nezakonita dejanja

1.3 Uporaba izrazov

1.3.1 V nadaljnjem besedilu:
- se ‘dajanje zagotovil in revidiranje IS’ imenuje ‘revidiranje’;
- se ‘strokovnjaki dajanja zagotovil in revidiranja IS’ imenujejo ‘strokovnjaki’.

2. Vsebina smernice

2.0 Uvod

Poglavje o vsebini smernice je sestavljeno tako, da daje informacije o naslednjih ključnih temah posla dajanja zagotovil in revidiranja IS:
2.1 Razlika med posli revidiranja IS in finančnimi revizijskimi posli
2.2 Presoja pomembnosti obravnavane zadeve
2.3 Pomembnost in kontrole
2.4 Pomembnost in zadeve, o katerih je treba poročati

2.1 Razlika med posli revidiranja IS in finančnimi revizijskimi posli

2.1.1 Strokovnjaki IS potrebujejo za merjenje pomembnosti drugačno merilo kot tisti, ki opravljajo finančne revizijske posle. Finančni strokovnjaki običajno merijo denarno izraženo pomembnost, ker je tudi vse, kar revidirajo, merjeno in vključeno v poročila v denarni vrednosti. Strokovnjaki za revidiranje IS običajno revidirajo nefinančne postavke, npr. kontrole pri razvoju programov, kontrole sprememb v programu, fizične kontrole dostopa, logične kontrole dostopa in kontrole delovanja računalnikov v celi vrsti različnih sistemov. Zato utegnejo strokovnjaki potrebovati navodilo, kako naj ocenjujejo pomembnost, da bodo uspešno načrtovali revizijske posle, kako naj usmerijo svoje napore na področja z velikim tveganjem in kako naj ocenijo težo ugotovljenih napak ali slabosti.

2204 Pomembnost *(nadaljevanje)*

2.2 Presoja pomembnosti obravnavane zadeve

2.2.1 Ocena glede pomembnosti je stvar strokovne presoje. Vključuje premislek o učinku in/ali morebitnem učinku na zmožnost podjetja, da izpolni poslovne cilje, če je morda prišlo do napak, opustitev, nepravilnosti in nezakonitih dejanj zaradi slabosti pri delovanju kontrol na pregledovanem področju. Kadar se cilj revizije nanaša na sisteme ali operacije, s katerimi se obdelujejo finančne transakcije, je treba pri revidiranju upoštevati merila pomembnosti, ki jih uporabljajo finančni strokovnjaki.

2.2.2 Za ocenjevanje pomembnosti naj bi strokovnjaki razvrstili informacijska sredstva glede na:
- zaupnost, razpoložljivost in celovitost,
- pravila za kontrolo dostopa pri upravljanju pooblastil,
- stopnjo kritičnosti in tveganje za poslovanje,
- skladnost z zakoni in predpisi.

Pri ocenjevanju je treba upoštevati tudi:
- vrsto obdelanih in shranjenih podatkov in informacij,
- strojno opremo IS,
- arhitekturo in programsko opremo IS (aplikacije in operacijski sistemi),
- infrastrukturo omrežja IS,
- delovanje IS,
- produkcijsko, razvojno in testno okolje,
- veljavne zakone in druge predpise.

2.2.3 Podrobnejši primeri dejavnikov, ki bi jih lahko upoštevali pri ocenjevanju pomembnosti, so:
- kritičnost poslovnih procesov, podprtih s sistemom ali postopki,
- kritičnost informacijskih podatkovnih baz, podprtih s sistemom ali postopki,
- število in vrsta razvitih aplikacij,
- število uporabnikov informacijskega sistema,
- število vodij in direktorjev, ki delajo z informacijskim sistemom, razvrščenih po pooblastilih,
- kritičnost omrežnih komunikacij, podprtih s sistemom ali postopki,
- stroški sistema ali delovanja (strojna oprema, programska oprema, osebje, storitve tretjih strank, režijski stroški ali kakršna koli 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 pri delu, nepotrebni visoki stroški proizvodnje, veliko izgub itd.),
- stroški izgube kritičnih in pomembnih informacij v smislu denarja in časa za njihovo ponovno pridobitev, pa tudi izguba ugleda in dobrega imena,
- število dostopov/transakcij/poizvedb, obdelanih v obdobju,
- vrsta, čas in obseg pripravljenih poročil in vzdrževanih datotek,
- vrsta in količine obdelanega materiala (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 glede zdravja in varstva pri delu in okoljskih zahtev,
- določene opredelitve ali premisleki o pomembnosti, ki jih zagotavljajo zakonodajni ali regulativni organi,
- prenos operacij IT na tretjo stranko, kar povzroči pomembno spremembo predpisanih zahtev glede skladnosti, npr. zasebnost in varstvo osebnih podatkov, pravila o nadzoru trgovanja, finančne zahteve.

2.2.4 Znak večje pomembnosti obravnavanega področja je treba uporabiti za ustrezno zmanjšanje revizijskega tveganja bodisi z razširjenim preizkušanjem kontrol (za zmanjšanje tveganja pri kontroliranju) in/ali z razširitvijo postopkov vsebinskega preizkušanja podatkov (za zmanjšanje tveganja pri odkrivanju).

2.2.5 Strokovnjaki naj ponovno ocenijo opredeljeno pomembnost, kadar zaznajo spremembe v določenih okoliščinah ali pridobijo dodatne informacije, ki bi lahko vplivale na pomembnost sistemov ali operacij. Najpogostejše situacije, v katerih bi se to lahko zgodilo, so med drugim:
- pomembnost je bila na začetku opredeljena na podlagi ocen ali po predhodnih informacijah, ki so bistveno drugačne od dejanskega stanja;
- dogodki ali spremenjene razmere v času po prvotni določitvi pomembnosti bistveno vplivajo na zmožnost podjetja, da izpolni svoje poslovne cilje.

2204 Pomembnost *(nadaljevanje)*

2.3 Pomembnost in kontrole

2.3.1 Za dosego revizijskih ciljev naj bi strokovnjaki prepoznali pomembne kontrolne cilje in na podlagi ravni sprejemljivega tveganja določili, kaj je treba pregledati. Za določen kontrolni cilj je posamezna kontrola ali skupina kontrol pomembna, če brez takih kontrol ne bi bilo mogoče dati sprejemljivega zagotovila, da bo kontrolni cilj dosežen.

2.3.2 Strokovnjaki naj bi upoštevali pomembnost, kadar določajo vrsto, čas in obseg revizijskih postopkov, ki jih je treba uporabiti za preizkušanje kontrole ali skupine kontrol. Da se zmanjša revizijsko tveganje, je za pomembne kontrole potrebno temeljitejše, pogostejše in obsežnejše preizkušanje kot za manj pomembne kontrole.

2.3.3 Pri presoji pomembnosti naj bi strokovnjaki upoštevali:
- raven napak, ki je še sprejemljiva za poslovodstvo, strokovnjake, ustrezne regulativne agencije in druge deležnike,
- možnost, da skupni učinek več majhnih napak ali slabosti postane pomemben.

2.3.4 Pred začetkom dela na terenu v okviru revizijskega posla naj strokovnjaki poskusijo od ustreznih deležnikov pridobiti pisno potrditev, da je bila razkrita vsaka pomembna slabost, za katero deležniki v podjetju vedo.

2.3.5 Kadar strokovnjaki odkrijejo pomanjkljivosti kontrol, morajo oceniti njihov učinek na celotno revizijsko mnenje ali sklep. Pri oceni tega učinka naj strokovnjaki upoštevajo različne vidike pojavljanja pomanjkljivosti kontrol, vključno z:
- velikostjo,
- vrsto,
- posebnimi okoliščinami.

2.3.6 Pri preizkušanju pomembnih kontrol naj strokovnjaki ocenijo učinek nadomestnih kontrol na zmanjševanje tveganja, povezanega z odkrito pomanjkljivostjo kontrol. Pomanjkljivosti kontrol je treba razvrstiti kot:
- pomembno slabost, kadar so nadomestne kontrole neuspešne,
- bistveno pomanjkljivost, kadar so nadomestne kontrole delno uspešne,
- posledično pomanjkljivost, kadar nadomestne kontrole zmanjšajo tveganje na sprejemljivo raven.

2.3.7 Več napak ali neuspešnih kontrol ima lahko skupni učinek, ki bi ga strokovnjaki morali upoštevati pri določanju celovite pomembnosti pomanjkljivosti kontrol.

2.3.8 Strokovnjaki naj bi ugotovili, ali je katera od splošnih pomanjkljivosti kontrol IT pomembna. Pomembnost takih pomanjkljivih splošnih kontrol IT je treba ovrednotiti glede na njihov učinek na aplikativne kontrole in ugotoviti, ali so neuspešne 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 na podlagi uporabljene aplikacije pomembno napačen in je razlog za to v nezadostnih kontrolah upravljanja sprememb v tabelah davčnih stopenj, potem sta pomembno šibki tako kontrola, ki temelji na aplikaciji (izračun), kot tudi splošna kontrola (upravljanje sprememb).

2.3.9 Strokovnjaki naj bi ovrednotili pomanjkljivost splošne kontrole IT v zvezi z njenim učinkom na aplikativne kontrole in vse skupaj ocenili glede na druge pomanjkljivosti kontrol. Primer: odločitev poslovodstva, da ne popravi pomanjkljivosti splošne kontrole IT in s tem povezanega vpliva na kontrolno okolje, bi na primer lahko postala pomembna, ko bi skupaj z drugimi pomanjkljivostmi kontrol vplivala na kontrolno okolje.

2.3.10 Strokovnjaki naj bi se tudi zavedali, da opustitev odprave pomanjkljivost lahko postane pomembna, na primer potem, ko so bili poslovodstvo in pristojni za upravljanje opozorjeni na pomanjkljivost.

2.3.11 Pomanjkljivosti kontrol so vedno pomembne na področjih, na katerih so bile namerno opuščene zaradi prevare ali nezakonitih dejanj.

2.4 Pomembnost in zadeve, o katerih je treba poročati

2.4.1 Pri določanju ugotovitev, sklepov in priporočil, o katerih je treba poročati, morajo strokovnjaki upoštevati tako pomembnost vsake ugotovljene napake kot tudi pomembnost napak, do katerih bi lahko prišlo zaradi slabosti v delovanju kontrol.

2.4.2 Kadar revizijski posel uporabi poslovodstvo za to, da pridobi izjavo o zagotovilu delovanja kontrol IS, izdano mnenje o ustreznosti kontrol brez pridržkov pomeni, da so vzpostavljene kontrole v skladu s splošno sprejeto kontrolno prakso za doseganje kontrolnih ciljev brez kakršnih koli pomembnih slabosti v delovanju kontrol.

2.4.3 Velja, da je slabost v delovanju kontrol pomembna, zato je treba o njej poročati, če zaradi odsotnosti kontrol ni mogoče dati sprejemljivega zagotovila, da bo kontrolni cilj dosežen. Če so z delom pri revizijskem poslu ugotovljene pomembne slabosti kontrol, morajo strokovnjaki razmisliti o izdaji mnenja s pridržki ali odklonilnega mnenja o cilju revizije.

2.4.4 Glede na cilje revizijskega posla naj strokovnjaki razmislijo o tem, da poslovodstvu poročajo tudi o nepomembnih slabostih, zlasti kadar so stroški za okrepitev kontrol majhni. Poleg tega bi strokovnjaki lahko tudi svetovali o rešitvah za odpravo ugotovljenih slabosti.

2204 Pomembnost *(nadaljevanje)*

3. Povezava s standardi in procesi v COBIT 5

3.0 Uvod

To poglavje daje pregled ustreznih:
3.1 Povezav s standardi
3.2 Povezav s procesi v COBIT 5
3.3 Drugih navodil

3.1 Povezava s standardi

V tabeli je pregled:
- najpomembnejših standardov ISACA, ki jih neposredno podpira ta smernica;
- tistih zahtev standardov, ki so najpomembnejše za to smernico.

Opomba: Naštete so samo tiste zahteve standardov, ki so pomembne za to smernico.

Naslov standarda	Pomembne zahteve standarda
1201 Načrtovanje posla	Strokovnjaki dajanja zagotovil in revidiranja IS morajo pripraviti in dokumentirati projektni načrt posla dajanja zagotovil ali 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	Strokovnjaki dajanja zagotovil in revidiranja IS morajo pri načrtovanju posameznih poslov prepoznati in oceniti tveganje, ki se nanaša na področje pregleda. Strokovnjaki dajanja zagotovil in revidiranja IS morajo proučiti tveganja, povezana z obravnavano zadevo, revizijsko tveganje in vpliv na izpostavljenost podjetja.
1204 Pomembnost	Strokovnjaki dajanja zagotovil in revidiranja IS morajo pri načrtovanju posla upoštevati morebitne slabosti ali pomanjkanje kontrol in pretehtati, ali bi bila posledica teh slabosti ali pomanjkanja kontrol lahko pomembna pomanjkljivost ali bistvena slabost. 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. Strokovnjaki dajanja zagotovil in revidiranja IS morajo upoštevati skupni učinek manjših pomanjkljivosti ali slabosti kontrol in možnost, da se pomanjkanje kontrol prevede v pomembno pomanjkljivost ali bistveno slabost. Strokovnjaki dajanja zagotovil in revidiranja IS morajo v poročilu razkriti: • pomanjkanje kontrol ali neučinkovite kontrole, • pomembnost pomanjkljivosti kontrol, • verjetnost, da bodo te slabosti povzročile pomembno pomanjkljivost ali bistveno slabost.
1207 Nepravilnosti in nezakonita dejanja	Strokovnjaki dajanja zagotovil in revidiranja IS morajo med izvajanjem posla upoštevati tveganja nepravilnosti in nezakonitih dejanj. Strokovnjaki dajanja zagotovil in revidiranja IS morajo med izvajanjem posla ohranjati poklicno nezaupljivost. Strokovnjaki dajanja zagotovil in revidiranja IS morajo dokumentirati in primerni stranki pravočasno sporočiti vsako pomembno nepravilnost ali nezakonito dejanje.

2204 Pomembnost *(nadaljevanje)*

3.2 Povezava s procesi v COBIT 5

V tabeli je pregled najpomembnejših:
- procesov v COBIT 5,
- namenov procesov v COBIT 5.

Posebne aktivnosti, ki se izvajajo kot del teh procesov, so vsebovane v *COBIT 5: Omogočanje procesov*.

Proces v COBIT 5	Namen procesa
EDM03 Zagotovite optimizacijo tveganja.	Zagotovite, da tveganje, povezano z IT v podjetju, ne preseže pripravljenosti za prevzemanje tveganj in sprejemljivega tveganja, da je vpliv tveganja IT na vrednost podjetja prepoznan in obvladovan ter da so možnosti za neskladnost s predpisi čim manjše.
MEA02 Spremljajte, vrednotite in ocenjujte sistem notranjih kontrol.	Ključnim deležnikom omogočite pregled nad ustreznostjo sistema notranjih kontrol in s tem zagotovite zaupanje v delovanje, vero v doseganje ciljev podjetja in ustrezno razumevanje preostalega tveganja.

3.3 Druga navodila

Pri izvajanju standardov in smernic naj strokovnjaki po potrebi poiščejo še druga navodila. Za dajanje zagotovil in revidiranje jih lahko pridobijo:
- od kolegov v podjetju in/ali zunaj njega, npr. prek strokovnih združenj ali strokovnih skupin na družbenih omrežjih,
- od vodstva,
- od organov upravljanja v organizaciji, npr. od revizijske komisije,
- iz drugih navodil (npr. knjig, člankov, drugih smernic).

4. Izrazi

Izraz	Pomen
Revizijsko tveganje	Tveganje, da pride do nepravilnega sklepa na podlagi ugotovitev revizije. Tri sestavine 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 je bistvena, če zaradi pomanjkanja kontrol ni mogoče dati 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 nujno. 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.
Pomembnost	Revizijski koncept, ki zadeva pomembnost informacije glede na njen vpliv ali učinek na pregledovano področje. Izraz relativne pomembnosti ali pomembnosti za neko določeno zadevo v kontekstu posla ali podjetja kot celote.
Pomembna pomanjkljivost	Pomanjkljivost ali kombinacija pomanjkljivosti pri notranjem kontroliranju, ki je manj huda od bistvene slabosti, vendar dovolj pomembna, da zasluži pozornost odgovornih za nadzor. Opomba: Bistvena slabost je pomembna pomanjkljivost ali kombinacija pomembnih pomanjkljivosti, katerih posledica je več kot majhna verjetnost neželenega dogodka ali dogodkov, ki niso bili preprečeni ali odkriti.

5. Datum uveljavitve

5.1 Datum uveljavitve Ta smernica velja za vse posle dajanja zagotovil in revidiranja IS, ki se začnejo 1. septembra 2014 ali pozneje.

2205 Dokazi

Smernica je predstavljena v naslednjih poglavjih:
1. Namen smernice in povezava s standardi
2. Vsebina smernice
3. Povezava s standardi in procesi v COBIT 5
4. Izrazi
5. Datum uveljavitve

1. Namen smernice in povezava s standardi

1.0 Uvod

V tem poglavju so razjasnjeni:
1.1 Namen smernice
1.2 Povezava s standardi
1.3 Uporaba izrazov ‘revidiranje’ in ‘strokovnjaki’

1.1 Namen

1.1.1 Namen te smernice je dati navodila strokovnjakom dajanja zagotovil in revidiranja IS pri pridobivanju zadostnih in ustreznih dokazov, ovrednotenju prejetih dokazov in pripravi ustrezne revizijske dokumentacije.

1.1.2 Strokovnjaki dajanja zagotovil in revidiranja IS naj bi upoštevali to smernico pri odločanju, kako izvajati standard, uporabiti strokovno presojo pri uporabi, utemeljiti vsako odstopanje in po potrebi poiskati dodatna navodila.

1.2 Povezava s standardi

1.2.1 Standard 1203 Izvedba in nadzor
1.2.2 Standard 1205 Dokazi
1.2.3 Standard 1206 Uporaba dela drugih strokovnjakov

1.3 Uporaba izrazov

1.3.1 V nadaljnjem besedilu:
- se ‘dajanje zagotovil in revidiranje IS’ imenuje ‘revidiranje’;
- se ‘strokovnjaki dajanja zagotovil in revidiranja IS’ imenujejo ‘strokovnjaki’.

2. Vsebina smernice

2.0 Uvod

Poglavje o vsebini smernice je sestavljeno tako, da daje informacije o naslednjih ključnih temah posla dajanja zagotovil in revidiranja IS:
2.1 Vrste dokazov
2.2 Pridobivanje dokazov
2.3 Ocenjevanje dokazov
2.4 Priprava revizijske dokumentacije

2.1 Vrste dokazov

2.1.1 Pri načrtovanju in izvajanju posla, naj bi strokovnjaki upoštevali vrste dokazov, ki jih je treba zbrati, njihovo uporabo za dosego ciljev posla in njihove različne ravni zanesljivosti. Med različnimi vrstami dokazov, katerih uporabo morajo strokovnjaki upoštevati, so:
- opazovani procesi in obstoj fizičnih predmetov,
- dokumentarni dokazi,
- navedbe,
- analiza.

2.1.2 Opazovani procesi in obstoj fizičnih predmetov lahko vključujejo opazovanja dejavnosti, premoženja in funkcij IS, kot so:
- delujoči sistem spremljanja omrežne varnosti,
- zaloga nosilcev podatkov v dislociranem skladišču.

2.1.3 Dokumentarni dokazi, zapisani na papirju ali drugih nosilcih podatkov, lahko vključujejo:
- pisne usmeritve in postopke,
- izide izvlečkov podatkov,
- zapise transakcij,
- izpise programov,
- druge dokumente in zapise, izdelane med rednim poslovanjem.

2205 Dokazi *(nadaljevanje)*

2.1 Vrste dokazov (nadaljevanje)

2.1.4 Pisne in ustne navedbe revidirancev lahko vključujejo:
- pisno izjavo poslovodstva, npr. navedbe o obstoju in uspešnosti notranjih kontrol ali načrte za uvedbo novega finančnega sistema,
- ustno predstavitev zadev, kot so način delovanja postopka ali načrti poslovodstva o nadaljnjem ukrepanju v zvezi s programom osveščanja o varnosti.

2.1.5 Tudi izide analiziranja informacij s primerjavami, simulacijami, izračuni in sklepanjem je mogoče uporabiti kot dokaze. Na primer:
- primerjalno analizo uspešnosti delovanja IS glede na druga podjetja ali prejšnja obdobja,
- primerjavo pogostnosti napak med aplikacijami, transakcijami in uporabniki,
- uspešnost delovanja postopkov ali kontrol.

2.2 Pridobivanje dokazov

2.2.1 Strokovnjak naj bi pridobil zadostne in ustrezne dokaze, da bi lahko sprejel primerne revizijske sklepe. Taki dokazi so med drugim:
- izvedeni postopki,
- izidi izvedenih postopkov,
- izvorni dokumenti (v elektronski ali papirni obliki), zapisi in potrditvene informacije, uporabljene v podporo pri revizijskem poslu,
- dokumentacija, da je bilo delo izvedeno v skladu z veljavnimi zakoni, predpisi in usmeritvami.

2.2.2 Če so pridobljeni dokazi v obliki ustnih navedb bistveni za revizijsko mnenje ali sklep, naj strokovnjaki proučijo možnost, da pridobijo potrditev teh navedb v pisni ali elektronski obliki (npr. po e-pošti). Strokovnjaki naj razmislijo tudi o drugih možnih dokazih za potrditev teh navedb, da zagotovijo njihovo zanesljivost.

2.2.3 Pri zbiranju dokazov naj strokovnjak upošteva:
- čas, stopnjo napora in stroškov za pridobitev dokazov v primerjavi z njihovo zadostnostjo za zmanjšanje revizijskega tveganja;
- pomembnost ocenjevane zadeve in revizijskega postopka, za katerega je dokaz potreben, pri doseganju revizijskih ciljev in zmanjševanju revizijskega tveganja;
- da elektronskih dokazov po določenem času morda ne bo več mogoče v celoti ali delno ponovno pridobiti.

2.2.4 Postopki, uporabljeni za zbiranje dokazov, se razlikujejo glede pregledovanega informacijskega sistema, časa, obsega in ciljev revizije ter strokovne presoje. Dokazi so lahko zbrani z ročnimi revizijskimi postopki, računalniško podprtimi revizijskimi tehnikami (CAAT) ali s kombinacijo obojih. Strokovnjaki naj bi izbrali najustreznejši postopek glede na cilj revizije IS. Upoštevati je treba naslednje postopke:
- **poizvedovanje in potrditev** – postopek iskanja informacij pri izkušenih ljudeh, ki dobro poznajo obravnavano zadevo. Izkušene osebe niso nujno člani pregledovanega podjetja. Ta postopek lahko vključuje vse od uradne pisne poizvedbe do neformalnih ustnih poizvedb;
- **opazovanje** – opazovanje postopka ali procesa, ki ga izvajajo posamezniki, ki so običajno zadolženi za njihovo izvajanje, ali opazovanje fizičnih predmetov, kot so objekti in naprave, računalniška strojna oprema ali nastavitve ali konfiguracije informacijskega sistema. Ta vrsta dokazov je omejena na čas, v katerem je potekalo opazovanje. Strokovnjaki morajo upoštevati, da opazovanje izvajanja nekega procesa ali postopka lahko vpliva na način njegovega izvajanja;
- **preiskovanje** – preiskovanje notranjih ali zunanjih dokumentov in zapisov. Postavke, ki jih je treba preiskati, so lahko predložene v papirni ali elektronski obliki. Preiskovanje lahko vključuje tudi preiskovanje fizičnih sredstev;
- **analitični postopki** – ocenjevanje (finančnih ali nefinančnih) podatkov s preiskovanjem možnih razmerij med samimi podatki ali med podatki in drugimi pomembnimi informacijami. To vključuje tudi preiskovanje nihanj, trendov in nekonsistentnih razmerij;
- **ponovno izračunavanje** – postopek preverjanja aritmetične in matematične točnosti dokumentov ali zapisov. Izvaja se lahko ročno ali z računalniško podprtimi revizijskimi tehnikami (CAAT);
- **ponovno izvajanje** – neodvisno izvajanje postopkov in/ali kontrol, ki jih je prvotno izvedel informacijski sistem ali podjetja samo;
- **drugi splošno sprejeti načini** – drugi splošno sprejeti postopki, po katerih lahko delajo strokovnjaki pri zbiranju zadostnih in ustreznih dokazov. Strokovnjaki na primer lahko izvajajo socialni inženiring, delujejo kot skrivnostni obiskovalci ali preizkušajo etične vdore.

2.2.5 Pri zbiranju dokazov naj bi strokovnjaki upoštevali neodvisnost in strokovnost dajalca revizijskih dokazov. Potrditveni revizijski dokazi neodvisne tretje stranke so na primer lahko zanesljivejši od revizijskih dokazov, pridobljenih od pregledovanega podjetja. Fizični revizijski dokazi so na splošno zanesljivejši od navedb posameznika.

2.2.6 Če obstaja možnost, da bodo zbrani dokazi postali del pravnega postopka, naj se strokovnjaki posvetujejo z ustreznim pravnim svetovalcem, da ugotovijo, ali so kakršne koli posebne zahteve, ki vplivajo na to, kako je treba dokaze zbrati, predstaviti in razkriti.

2205 Dokazi *(nadaljevanje)*

2.2 Pridobivanje dokazov

2.2.7 Kadar strokovnjaki ne morejo pridobiti zadostnih revizijskih dokazov, na primer kadar posamezniki ali poslovodstvo nočejo dati zadostnih in ustreznih dokazov, potrebnih za dosego ciljev revizije IS, bi morali strokovnjaki tako okoliščino razkriti vodstvu revizije in po potrebi pristojnim za upravljanje. Strokovnjaki morajo to dejstvo razkriti tudi v skladu z ustaljenimi postopki revizijske organizacije. Omejitve glede obsega revizije in doseganja revizijskih ciljev bi morale biti razkrite v sporočilih o revizijskih izidih.

2.2.8 Strokovnjaki naj bi hranili dokaze tudi po končanem revizijskem delu in s tem zagotoviti, da so dokazi:
- razpoložljivi za čas in v obliki, ki sta skladna z usmeritvami revizijske organizacije in ustreznimi strokovnimi standardi, zakoni in predpisi;
- zaščiteni pred nedovoljenim razkritjem ali spremembo ves čas njihove priprave in hrambe,
- na koncu obdobja hrambe pravilno uničeni.

2.3 Ocenjevanje dokazov

2.3.1 Dokazi so zadostni in ustrezni, kadar zagotavljajo sprejemljivo podlago za podporo ugotovitvam ali sklepom glede revizijskih ciljev. Če dokazi po presoji strokovnjakov ne izpolnjujejo teh meril, naj bi strokovnjaki pridobili dodatne dokaze ali izvedli dodatne postopke, da bi se zmanjšale omejitve ali negotovosti, povezane z dokazi. Izpis programov na primer morda ni ustrezen dokaz, dokler niso zbrani drugi dokazi, ki potrjujejo, da izpis predstavlja dejanski program, uporabljen v proizvodnem procesu.

2.3.2 Pri ocenjevanju zanesljivosti dokazov, pridobljenih med revizijo, naj bi strokovnjaki upoštevali značilnosti in lastnosti dokazov, kot so izvor, vrsta (pisni, ustni, vidni ali elektronski), verodostojnost (opremljeni z digitalnimi ali ročnimi podpisi, datumskim žigom z uro) in povezave med potrditvenimi dokazi iz več različnih virov. Na splošno se zanesljivost dokazov razvršča od malo do zelo zanesljivih na podlagi postopkov, uporabljenih za pridobivanje dokazov, kot so:
- poizvedovanje in potrditev,
- opazovanje,
- preiskovanje,
- analitični postopki,
- ponovno izračunavanje,
- ponovno izvajanje.

Za vsakega od naštetih postopkov velja, da je zanesljivost dokazov na splošno večja, če so dokazi:
- pridobljeni v pisni obliki, ne iz ustnih navedb,
- pridobljeni neposredno od strokovnjakov, ne pa posredno od revidirane enote,
- pridobljeni iz neodvisnih virov,
- potrjeni od neodvisne stranke,
- hranjeni pri neodvisni stranki.

2.3.3 Strokovnjaki naj bi pri določanju vrste, časa in obsega vsebinskega preizkušanja podatkov in preizkušanja njihove skladnosti, če je to primerno, upoštevali čas obstoja ali razpoložljivosti informacij. 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.

2.3.4 Če je revizijo opravila neodvisna tretja stranka, naj bi strokovnjaki proučili, ali je bilo izvedeno preizkušanje kontrol, pomembnih za predmet revizije, in ali se je na izide tega preizkušanja mogoče zanesti.

2.3.5 Strokovnjaki naj bi pridobili dokaze, ki so zadostni in ustrezni, da usposobljeni neodvisni stranki omogočajo ponovno izvesti preizkuse in priti do enakih izidov in sklepov.

2.4 Priprava revizijske dokumentacije

2.4.1 Med izvajanjem revizije naj bi strokovnjaki pripravili dokumentacijo pridobljenih dokazov, da bo shranjena in na razpolago za vnaprej določeno obdobje in v obliki, ki je v skladu z usmeritvami podjetja in zadevnimi strokovnimi standardi, zakoni in predpisi.

2.4.2 Dokazi, pridobljeni med izvajanjem revizije, naj bi bili ustrezno ugotovljeni, navzkrižno preverjeni in katalogizirani, tako da je mogoče lažje ugotoviti celovito zadostnost in ustreznost dokazov, ki dajejo sprejemljivo podlago za ugotovitve in sklepe glede na revizijske cilje in da jih lahko drugi člani skupine za revidiranje IS ali neodvisna stranka enostavno obnovijo.

2.4.3 Strokovnjaki naj bi zagotovili, da je dokumentacija dokazov zaščitena pred nepooblaščenim dostopom, razkritjem ali spreminjanjem ves čas priprave in hrambe.

2.4.4 Strokovnjaki naj bi na koncu določenega obdobja hrambe dokazno dokumentacijo uničili.

2205 Dokazi *(nadaljevanje)*

3. Povezava s standardi in procesi v COBIT 5

3.0 Uvod

To poglavje daje pregled ustreznih:
3.1 Povezav s standardi
3.2 Povezav s procesi v COBIT 5
3.3 Drugih navodil

3.1 Povezava s standardi

V tabeli je pregled:
- najpomembnejših standardov ISACA, ki jih neposredno podpira ta smernica;
- tistih zahtev standardov, ki so najpomembnejše za to smernico.

Opomba: Naštete so samo tiste zahteve standardov, ki so pomembne za to smernico.

Naslov standarda	Pomembne zahteve standarda
1203 Izvedba in nadzor	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. Strokovnjaki dajanja zagotovil in revidiranja IS morajo revizijski postopek dokumentirati z opisi revizijskega dela in revizijskimi dokazi, ki podpirajo ugotovitve in sklepe.
1205 Dokazi	Strokovnjaki dajanja zagotovil in revidiranja IS morajo pridobiti zadostne in ustrezne dokaze, da lahko sprejmejo primerne sklepe, s katerimi utemeljijo izide posla. Strokovnjaki dajanja zagotovil in revidiranja IS morajo ovrednotiti zadostnost dokazov, pridobljenih za utemeljitev sklepov in doseganje ciljev posla.
1206 Uporaba dela drugih strokovnjakov	Strokovnjaki dajanja zagotovil in revidiranja IS morajo izvesti dodatne preizkusne postopke za pridobitev zadostnih in ustreznih dokazov v okoliščinah, v katerih delo drugih strokovnjakov ne zagotavlja zadostnih ali ustreznih dokazov.

3.2 Povezava s procesi v COBIT 5

V tabeli je pregled najpomembnejših:
- procesov v COBIT 5,
- namenov procesov v COBIT 5.

Posebne aktivnosti, ki se izvajajo kot del teh procesov, so v *COBIT 5: Omogočanje procesov*.

Proces v COBIT 5	Namen procesa
MEA02 Spremljajte, vrednotite in ocenjujte sistem notranjih kontrol.	Ključnim deležnikom omogočite pregled nad ustreznostjo sistema notranjih kontrol in s tem zagotovite zaupanje v delovanje, vero v doseganje ciljev podjetja in ustrezno razumevanje preostalega tveganja.

3.3 Druga navodila

Pri izvajanju standardov in smernic naj strokovnjaki po potrebi poiščejo še druga navodila. Za dajanje zagotovil in revidiranje IS jih lahko pridobijo:
- od kolegov v podjetju,
- od vodstva,
- od organov upravljanja v podjetju, npr. od revizijske komisije,
- od strokovnih organizacij ali strokovnih medijskih skupin,
- iz drugih strokovnih navodil (npr. knjig, člankov, drugih smernic).

2205 Dokazi *(nadaljevanje)*

4. Izrazi

Izraz	Pomen
Ustrezni dokazi	Merilo kakovosti dokazov.
Navedba	Podpisana ali ustna izjava, ki jo poslovodstvo izroči strokovnjakom in v kateri poslovodstvo izjavi, da je ali bo neko sedanje ali prihodnje dejstvo (npr. proces, sistem, postopek, usmeritev) po najboljšem vedenju poslovodstva v določenem stanju.
Zadostni dokazi	Merilo količine dokazov; zadostni dokazi podpirajo vsa pomembna vprašanja za cilj in obseg revizije. Glej Dokaze.

5. Datum uveljavitve

5.1 Datum uveljavitve Ta smernica velja za vse posle dajanja zagotovil in revidiranja IS, ki se začnejo 1. septembra 2014 ali pozneje.

2206 Uporaba dela drugih strokovnjakov

Smernica je predstavljena v naslednjih poglavjih:
1. Namen smernice in povezava s standardi
2. Vsebina smernice
3. Povezava s standardi in procesi v COBIT 5
4. Izrazi
5. Datum uveljavitve

1. Namen smernice in povezava s standardi

1.0 Uvod

V tem poglavju so razjasnjeni:
1.1 Namen smernice
1.2 Povezava s standardi
1.3 Uporaba izrazov ‘revidiranje’ in ‘strokovnjaki’

1.1 Namen

1.1.1 Ta smernica daje navodila strokovnjakom dajanja zagotovil in revidiranja IS, kadar proučujejo možnost uporabe dela drugih strokovnjakov. Smernica jim pomaga pri presoji ustreznosti strokovnjakov, pregledovanju in ocenjevanju dela drugih strokovnjakov, presoji potrebe po izvajanju dodatnih preizkusnih postopkov in pri izražanju mnenja za revizijski posel, pri katerem upoštevajo opravljeno delo drugih strokovnjakov.

1.1.2 Strokovnjaki dajanja zagotovil in revidiranja IS naj bi upoštevali to smernico pri odločanju, kako izvajati standard, uporabiti strokovno presojo pri uporabi, utemeljiti vsako odstopanje in po potrebi poiskati dodatna navodila.

1.2 Povezava s standardi

1.2.1 Standard 1007 Trditve
1.2.2 Standard 1203 Izvedba in nadzor
1.2.3 Standard 1206 Uporaba dela drugih strokovnjakov

1.3 Uporaba izrazov

1.3.1 V nadaljnjem besedilu:
- se ‘dajanje zagotovil in revidiranje IS’ imenuje ‘revidiranje’;
- se ‘strokovnjaki dajanja zagotovil in revidiranja IS’ imenujejo ‘strokovnjaki’.

2. Vsebina smernice

2.0 Uvod

Poglavje o vsebini smernice je sestavljeno tako, da daje informacije o naslednjih ključnih temah posla dajanja zagotovil in revidiranja IS:
2.1 Proučitev uporabe dela drugih strokovnjakov
2.2 Presoja ustreznosti drugih strokovnjakov
2.3 Načrtovanje in pregledovanje dela drugih strokovnjakov
2.4 Ocenjevanje dela drugih strokovnjakov, ki niso del skupine za revizijski posel
2.5 Dodatni preizkusni postopki
2.6 Revizijsko mnenje ali sklep

2206 Uporaba dela drugih strokovnjakov *(nadaljevanje)*

2.1 Proučitev uporabe dela drugih strokovnjakov

2.1.1 Kadar strokovnjaki dajanja zagotovil in revidiranja IS nimajo potrebnih sposobnosti za opravljanje (dela) revizijskega posla, naj bi proučili možnost, da poiščejo pomoč drugih strokovnjakov, ki imajo zahtevane veščine.

2.1.2 O uporabi dela drugih strokovnjakov je treba razmisliti, kadar bi omejitve lahko oslabile revizijsko delo, ki ga je treba opraviti, npr. zaradi tehničnega znanja, potrebnega glede na naravo nalog, ki jih je treba opraviti, pomanjkanja virov za izvedbo revizije ali časovnih omejitev, in obravnavati morebitna vprašanja neodvisnosti. O uporabi drugih strokovnjakov je treba razmisliti tudi, kadar bi s tem dosegli višjo kakovost posla.

2.1.3 Strokovnjaki dajanja zagotovil in revidiranja IS naj bi dovolj dobro poznali opravljeno delo, tako da ga lahko usmerjajo in pregledujejo, ne sme pa se od njih pričakovati znanja na enaki ravni, kot ga imajo drugi strokovnjaki.

2.1.4 Strokovnjaki dajanja zagotovil in revidiranja IS naj bi izbrali posebne strokovnjake in uporabili njihovo delo na podlagi objektivnih meril.

2.1.5 Strokovnjaki dajanja zagotovil in revidiranja IS naj bi sporočili in dokumentirali zahteve drugim strokovnjakom v pogodbi ali sporazumu, preden bi ti drugi strokovnjaki začeli delati pri poslu.

2.1.6 Kadar notranje usmeritve podjetja prepovedujejo dostop do zapisov ali sistemov, bi morali strokovnjaki dajanja zagotovil in revidiranja IS določiti ustrezen obseg uporabe dela drugega strokovnjaka in opiranja na to delo.

2.1.7 Če ni mogoče pridobiti potrebnih strokovnjakov, naj bi strokovnjaki dajanja zagotovil in revidiranja IS dokumentirali vpliv tega dejstva na doseganje revizijskih ciljev in vključili v revizijski načrt določene naloge za obvladovanje posledičnega revizijskega tveganja. Če posledičnih revizijskih tveganj ni mogoče obvladati, bodo morali strokovnjaki dajanja zagotovil in revidiranja IS revizijski posel morda odkloniti.

2.2 Presoja ustreznosti drugih strokovnjakov

2.2.1 Kadar revizijski posel vključuje uporabo dela drugih strokovnjakov, naj bi strokovnjaki revidiranja in dajanja zagotovil IS razmislili o ustreznosti drugih strokovnjakov pri načrtovanju dela za revizijo IS. To vključuje:

- presojo neodvisnosti in nepristranskosti drugih strokovnjakov,
- presojo njihove strokovna izobrazbe, usposobljenosti, ustreznih izkušenj, virov in uporabe kakovostnih kontrolnih postopkov.

2.2.2 Strokovnjaki dajanja zagotovil in revidiranja IS naj bi skrbno proučili neodvisnost in nepristranskost drugih strokovnjakov, kadar uporabljajo njihovo delo. Postopki za izbiro in imenovanje, organizacijski status, linija poročanja in učinek njihovih priporočil na ravnanje poslovodstva so značilni znaki neodvisnosti in nepristranskosti drugih strokovnjakov.

2.3 Načrtovanje in pregledovanje dela drugih strokovnjakov

2.3.1 Strokovnjaki revidiranja in dajanja zagotovil IS naj bi pri načrtovanju revizijskega dela upoštevali aktivnosti drugih strokovnjakov in njihov učinek na cilje revizije IS. To vključuje:

- seznanjanje z njihovim obsegom dela, pristopom, časovnim razporedom dela in uporabo postopkov kontrole kakovosti,
- določitev ravni zahtevanega pregleda.

2.3.2 Strokovnjaki revidiranja in dajanja zagotovil IS naj bi preverili in potrdili, da revizijska listina ali listina o poslu določa njihovo pravico dostopa do dela drugih strokovnjakov. Strokovnjaki revidiranja in dajanja zagotovil IS naj bi imeli dostop do vsega delovnega gradiva, dokazne dokumentacije in poročil, ki so jih izdelali drugi strokovnjaki, če tak dostop ne povzroča pravnih vprašanj.

2.3.3 Vrsta, čas in obseg zahtevanih revizijskih dokazov bodo odvisni od pomembnosti in obsega dela drugih strokovnjakov. Pri načrtovanju naj bi strokovnjaki določili raven potrebnega pregleda, da se zagotovijo zadostni in ustrezni revizijski dokazi za uspešno izpolnitev celovitega cilja revizije IS. Strokovnjaki revidiranja in dajanja zagotovil IS naj bi pregledali končno poročilo, metodologijo ali revizijske programe in delovno gradivo drugih strokovnjakov.

2.3.4 Pri pregledovanju delovnega gradiva drugih strokovnjakov naj bi strokovnjaki revidiranja in dajanja zagotovil IS ocenili, ali je bilo delo drugih strokovnjakov ustrezno načrtovano, nadzirano, dokumentirano in pregledano, presodili ustreznost in sprejemljivost revizijskih dokazov, ki so jih priskrbeli, in določili obseg uporabe njihovega dela in svojega opiranja nanj. Ta ocena lahko vključuje ponovni preizkus dela drugih strokovnjakov. Oceniti je treba tudi skladnost z ustreznimi strokovnimi standardi. Skratka, strokovnjaki revidiranja in dajanja zagotovil IS naj bi ocenili, ali je delo drugih strokovnjakov tako ustrezno in popolno, da ga lahko vključijo v sedanje cilje revizije IS in dokumentirajo sklep.

2.3.5 Strokovnjaki revidiranja in dajanja zagotovil IS naj bi dovolj skrbno pregledali končna poročila drugih strokovnjakov in lahko potrdili, da:

- je obseg, določen v revizijski listini, opisu nalog in pristojnosti ali listini o poslu, izpolnjen,
- so bile vse pomembne predpostavke, ki so jih uporabili drugi strokovnjaki, prepoznane,
- so ugotovitve in sklepi, vključeni v poročilo, ustrezno podprti z dokazi.

2206 Uporaba dela drugih strokovnjakov *(nadaljevanje)*

2.4 Ocenjevanje dela drugih strokovnjakov, ki niso del skupine za revizijski posel

2.4.1 Današnje medsebojne odvisnosti med naročniki in dobavitelji v zvezi z obdelovanjem in zunanjim izvajanjem neključnih aktivnosti vodijo v zapletenejše revizijsko okolje. Dele revidiranega okolja lahko nadzorujejo in revidirajo druge neodvisne službe ali organizacije. Zaradi tega bodo organizacije, ki delo oddajajo v izvajanje, prejele poročila teh tretjih izvajalcev o kontrolnem okolju revidiranih področij delovanja. V nekaterih primerih to lahko zmanjšuje potrebo po revizijskem pokritju IS, čeprav strokovnjaki nimajo dostopa do dokazne dokumentacije in delovnega gradiva. Vsekakor pa naj bi bili strokovnjaki previdni pri izdajanju mnenja o takih primerih.

2.4.2 Strokovnjaki revidiranja in dajanja zagotovil IS naj bi ocenili koristnost in ustreznost poročil, ki so jih izdali drugi strokovnjaki, in proučili vse pomembni ugotovitve, o katerih poročajo drugi strokovnjaki. Dolžnost strokovnjakov revidiranja in dajanja zagotovil IS je, da se odločijo, ali se bodo na delo drugih strokovnjakov zanesli in ga neposredno vključili v poročilo ali pa se bodo nanj sklicevali v ločenem delu poročila. Strokovnjaki revidiranja in dajanja zagotovil IS morajo tudi oceniti učinek ugotovitev in sklepov drugih strokovnjakov na celoviti cilj revizije IS ter preveriti in potrditi, da je dokončano vse dodatno delo, potrebno za dosego celovitega cilja revizije IS. Vse trditve drugih strokovnjakov naj bi preverilo in uradno potrdilo poslovodstvo; podrobna navodila o tej temi lahko najdete v Standardu 1007 Trditve.

2.5 Dodatni preizkusni postopki

2.5.1 Na podlagi ocene dela drugih strokovnjakov naj bi strokovnjaki revidiranja in dajanja zagotovil IS uporabili dodatne preizkusne postopke, da bi pridobili zadostne in ustrezne revizijske dokaze v okoliščinah, ko delo drugih strokovnjakov takih dokazov ne daje.

2.5.2 Strokovnjaki revidiranja in dajanja zagotovil IS naj bi razmislili tudi o tem, ali je potrebno dodatno preverjanje dela drugih strokovnjakov.

2.6 Revizijsko mnenje ali sklep

2.6.1 Na koncu so za oblikovanje revizijskega mnenja ali sklepa vedno odgovorni strokovnjaki dajanja zagotovil in revidiranja IS. Ugotoviti morajo, ali je bilo opravljeno delo drugih strokovnjakov zadostno za oblikovanje revizijskega mnenja ali sklepa.

2.6.2 Če izvedeni dodatni preizkusni postopki ne dajo zadostnih in ustreznih revizijskih dokazov, bi morali strokovnjaki izdati temu ustrezno revizijsko mnenje ali sklep in vanj po potrebi vključiti omejitve obsega.

2.6.3 Če strokovnjaki dajanja zagotovil in revidiranja IS za oblikovanje mnenja uporabijo poročilo drugih strokovnjakov, naj bi bila njihova stališča in pripombe o sprejemljivosti in pomembnosti poročila drugih strokovnjakov del poročila revizijskega posla.

2.6.4 Kadar je to primerno, naj strokovnjaki dajanja zagotovil in revidiranja IS proučijo, v kolikšnem obsegu je poslovodstvo izvedlo priporočila drugih strokovnjakov. To naj vključuje tudi oceno, ali se je poslovodstvo zavezalo v ustreznih rokih popraviti pomanjkljivosti zadev, ki so jih ugotovili drugi strokovnjaki, in kakšno je sedanje stanje teh popravkov.

---

3. Povezava s standardi in procesi v COBIT 5

3.0 Uvod

To poglavje daje pregled ustreznih:
3.1 Povezav s standardi
3.2 Povezav s procesi v COBIT 5
3.3 Drugih navodil

2206 Uporaba dela drugih strokovnjakov *(nadaljevanje)*

3.1 Povezava s standardi

V tabeli je pregled:
- najpomembnejših standardov ISACA, ki jih neposredno podpira ta smernica;
- tistih zahtev standardov, ki so najpomembnejše za to smernico.

Opomba: Naštete so samo tiste zahteve standardov, ki so pomembne za to smernico.

Naslov standarda	Pomembne zahteve standarda
1007 Trditve	Strokovnjaki dajanja zagotovil in revidiranja IS morajo pregledati trditve, na podlagi katerih bodo presojali obravnavano zadevo, da bi ugotovili, ali je mogoče takšne trditve revidirati in ali so te trditve zadostne, veljavne in ustrezne.
1203 Izvedba in nadzor	Strokovnjaki dajanja zagotovil in revidiranja IS lahko sprejmejo samo naloge, ki so v okviru njihovega strokovnega znanja in veščin, ali naloge, za katere upravičeno pričakujejo, da bodo veščine pridobili med izvajanjem posla ali da jih bodo opravili pod nadzorom. 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.
1206 Uporaba dela drugih strokovnjakov	Če je primerno, morajo strokovnjaki dajanja zagotovil in revidiranja IS proučiti možnost uporabe dela drugih strokovnjakov pri poslu. Strokovnjaki dajanja zagotovil in revidiranja IS morajo pred začetkom izvajanja posla oceniti in odobriti ustreznost strokovne usposobljenosti, sposobnosti, izkušenj, virov, neodvisnosti in postopkov nadzora kakovosti drugih strokovnjakov. 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. Strokovnjaki dajanja zagotovil in revidiranja IS morajo odločiti, ali je delo drugih strokovnjakov, ki niso člani skupine za posel, zadostno in popolno za sklepanje o trenutnih ciljih posla, ter sklep jasno dokumentirati. 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. Strokovnjaki dajanja zagotovil in revidiranja IS morajo izvesti dodatne preizkusne postopke za pridobitev zadostnih in ustreznih dokazov v okoliščinah, v katerih delo drugih strokovnjakov ne zagotavlja zadostnih ali ustreznih dokazov. Strokovnjaki dajanja zagotovil in revidiranja IS morajo zagotoviti ustrezno revizijsko mnenje ali sklep ter vključiti vsakršne omejitve obsega, če potrebni dokazi niso pridobljeni s pomočjo dodatnih preizkusov.

3.2 Povezava s procesi v COBIT 5

V tabeli je pregled najpomembnejših:
- procesov v COBIT 5,
- namenov procesov v COBIT 5.

Posebne aktivnosti, ki se izvajajo kot del teh procesov, so v *COBIT 5: Omogočanje procesov*.

Proces v COBIT 5	Namen procesa
MEA02 Spremljajte, vrednotite in ocenjujte sistem notranjih kontrol.	Ključnim deležnikom omogočite pregled nad ustreznostjo sistema notranjih kontrol in s tem zagotovite zaupanje v delovanje, vero v doseganje ciljev podjetja in ustrezno razumevanje preostalega tveganja.

2206 Uporaba dela drugih strokovnjakov *(nadaljevanje)*

3.3 Druga navodila Pri izvajanju standardov in smernic naj strokovnjaki po potrebi poiščejo še druga navodila. Za dajanje zagotovil in revidiranje IS jih lahko pridobijo:

- od kolegov v podjetju,
- od vodstva,
- od organov upravljanja v organizaciji, npr. od revizijske komisije,
- od strokovnih organizacij ali strokovnih medijskih skupin,
- iz drugih strokovnih navodil (npr. knjig, člankov, drugih smernic).

4. Izrazi

Izraz	Pomen
Drug strokovnjak	V podjetju ali zunaj njega se drug strokovnjak lahko nanaša na: • revizorja IS iz zunanjega revizijskega podjetja, • svetovalca poslovodstvu, • izvedenca na področju posla, ki ga je imenovalo poslovodstvo ali skupina.

5. Datum uveljavitve

5.1 Datum uveljavitve Ta smernica velja za vse posle dajanja zagotovil in revidiranja IS, ki se začnejo 1. septembra 2014 ali pozneje.

2207 Nepravilnosti in nezakonita dejanja

Smernica je predstavljena v naslednjih poglavjih:
1. Namen smernice in povezava s standardi
2. Vsebina smernice
3. Povezava s standardi in procesi v COBIT 5
4. Izrazi
5. Datum uveljavitve

1. Namen smernice in povezava s standardi

1.0 Uvod

V tem poglavju so razjasnjeni:
1.1 Namen smernice
1.2 Povezava s standardi
1.3 Uporaba izrazov ‘revidiranje’ in ‘strokovnjaki’

1.1 Namen

1.1.1 Namen te smernice je dati strokovnjakom dajanja zagotovil in revidiranja IS navodila, kako obravnavati nepravilnosti in nezakonita dejanja.

1.1.2 Smernica podrobno določa zadolžitve poslovodstva in strokovnjakov dajanja zagotovil in revidiranja IS v zvezi z nepravilnostmi in nezakonitimi dejanji. Daje tudi navodila, kako obravnavati nepravilnosti in nezakonita dejanja med načrtovanjem in izvajanjem revizijskega dela. Ne nazadnje smernica predlaga dobre prakse za notranje in zunanje poročanje o nepravilnostih in nezakonitih dejanjih.

1.1.3 Strokovnjaki dajanja zagotovil in revidiranja IS naj bi upoštevali to smernico pri odločanju, kako izvajati standard, uporabiti strokovno presojo pri uporabi, utemeljiti vsako odstopanje in po potrebi poiskati dodatna navodila.

1.2 Povezava s standardi

1.2.1 Standard 1005 Potrebna poklicna skrbnost
1.2.2 Standard 1201 Načrtovanje posla
1.2.3 Standard 1202 Ocenjevanje tveganja pri načrtovanju
1.2.4 Standard 1207 Nepravilnosti in nezakonita dejanja
1.2.5 Standard 1401 Poročanje

1.3 Uporaba izrazov

1.3.1 V nadaljnjem besedilu:
- se ‘dajanje zagotovil in revidiranje IS’ imenuje ‘revidiranje’;
- se ‘strokovnjaki dajanja zagotovil in revidiranja IS’ imenujejo ‘strokovnjaki’.

2. Vsebina smernice

2.0 Uvod

Poglavje o vsebini smernice je sestavljeno tako, da daje informacije o naslednjih ključnih temah posla dajanja zagotovil in revidiranja IS:
2.1 Nepravilnosti in nezakonita dejanja
2.2 Zadolžitve poslovodstva
2.3 Zadolžitve strokovnjakov
2.4 Nepravilnosti in nezakonita dejanja med načrtovanjem posla
2.5 Zasnova in pregledovanje postopkov posla
2.6 Odzivanje na nepravilnosti in nezakonita dejanja
2.7 Notranje poročanje
2.8 Zunanje poročanje

2.1 Nepravilnosti in nezakonita dejanja

2.1.1 Nepravilnosti in nezakonita dejanja lahko neposredno vplivajo na podjetje na več (negativnih) načinov, saj prizadenejo finančno stanje in dobro ime podjetja, posredno pa vplivajo tudi na učinkovitost in ohranjanje delovnih mest. Zato je pomembno, da se podjetja te nevarnosti zavedajo in imajo vzpostavljene mehanizme za preprečevanje in odkrivanje, ki hitro prepoznajo nepravilnosti in nezakonita dejanja. Večja verjetnost za nepravilnosti in nezakonita dejanja je na področjih, na katerih ni kontrol ali pa so te slabo zasnovane ali ne delujejo pravilno.

2207 Nepravilnosti in nezakonita dejanja *(nadaljevanje)*

2.1 Nepravilnosti in nezakonita dejanja (nadaljevanje)

2.1.2 Nepravilnosti in nezakonita dejanja lahko storijo zaposleni na vseh ravneh v podjetju in lahko med drugim vključujejo aktivnosti, kot so:

- prevara, ki je vsako dejanje, ki vključuje zavajanje za pridobitev nezakonite prednosti,
- namerno napačna predstavitev dejstev zaradi pridobivanja nezakonite prednosti ali prikrivanja nepravilnosti ali nezakonitih dejanj,
- dejanja, ki vključujejo neskladnost z zakoni in predpisi, vključno z neizpolnjevanjem zakonov in predpisov, ki veljajo za sisteme IT,
- nepooblaščeno razkritje podatkov, ki so zaščiteni po zakonih o varstvu osebnih podatkov in zasebnosti,
- dejanja, ki vključujejo neskladnost s sporazumi in pogodbami podjetja s tretjimi strankami, kot so banke, dobavitelji, prodajalci, izvajalci storitev in deležniki,
- prirejanje, ponarejanje, poneverjanje in spreminjanje zapisov ali dokumentov (v elektronski obliki ali na papirju),
- zmanjšanje ali opustitev učinkov transakcij/poslov iz zapisov ali dokumentov (v elektronski obliki ali na papirju),
- neprimerno ali namerno dopuščanje uhajanja zaupnih informacij,
- evidentiranje transakcij v finančnih ali drugih zapisih (v elektronski obliki ali na papirju), ki nimajo podlage in se zanje ve, da so napačni (npr. lažno izplačilo, prevare pri plačah, izogibanje davku),
- nezakonita prisvojitev in zloraba sredstev,
- prestrezanje ali poneverba, kar je nezakonita prisvojitev gotovine, preden je priliv vpisan v finančne evidence podjetja,
- namerna ali nenamerna dejanja, da kršijo pravice industrijske lastnine, kot so avtorske pravice, blagovne znamke ali patenti,
- dodelitev nepooblaščenega dostopa do informacij in sistemov,
- napake v finančnih ali drugih evidencah, ki so posledica nepooblaščenega dostopa do podatkov in sistemov.

2.1.3 Ugotovitev, da je določeno dejanje nezakonito, naj na splošno temelji na nasvetu poučenega strokovnjaka, ki ima pravno izobrazbo, ali pa je treba počakati na končno odločitev sodišča. Strokovnjaki naj predvsem upoštevajo učinek ali morebitni učinek nepravilnega ravnanja ne glede na to, ali gre za sum ali dokaz nezakonitega dejanja.

2.1.4 Vseh nepravilnosti ni treba obravnavati kot prevarantske dejavnosti. Opredelitev prevarantskih dejavnosti je odvisna od zakonske opredelitve pojma prevare v pravnem redu posamezne države. Prevarantske nepravilnosti so med drugim:

- namerno izogibanje kontrolam zaradi prikrivanja ponavljajoče se prevare,
- nepooblaščena uporaba sredstev ali storitev,
- napeljevanje na tovrstne dejavnosti ali pomoč pri njihovem prikrivanju.

Neprevarantske nepravilnosti lahko vključujejo:

- namerne kršitve sprejete upravljavske usmeritve,
- namerne kršitve predpisanih zahtev,
- namerne napačne navedbe ali izpuščanje informacij, ki se nanašajo na revidirano področje ali podjetje kot celoto,
- huda malomarnost,
- nenamerna nezakonita dejanja.

2.2 Zadolžitve poslovodstva

2.2.1 Poslovodstvo je predvsem odgovorno za vzpostavitev kontrol, ki odvračajo, preprečujejo in odkrivajo nepravilnosti in nezakonita dejanja.

2.2.2 Za pridobitev sprejemljivega zagotovila, da so nepravilnosti in nezakonita dejanja pravočasno odvrnjena, preprečena ali odkrita, uporablja poslovodstvo običajno naslednja sredstva:

- načrtovanje, vzpostavitev in vzdrževanje sistemov notranjih kontrol za preprečevanje in odkrivanje nepravilnosti ali nezakonitih dejanj. Notranje kontrole vključujejo pregled in odobritev transakcij/poslov in postopke za upravljavske preglede;
- usmeritve in postopki za urejanje ravnanja zaposlenih;
- postopki za potrjevanje in spremljanje skladnosti;
- načrtovanje, vzpostavitev in vzdrževanje primernih sistemov za poročanje, evidentiranje in obvladovanje dogodkov v zvezi z nepravilnostmi ali nezakonitimi dejanji;
- usmeritve in postopki za urejanje skladnosti in predpisanih zahtev.

2.2.3 Poslovodstvo naj bi strokovnjakom razkrilo vse, kar ve o kakršnih koli domnevnih, slutenih ali dokazanih nepravilnostih ali nezakonitih dejanjih in udeleženih področjih ter o ukrepih poslovodstva, če so bili izvedeni.

2.2.4 Kadar koli gre za domnevno, sluteno ali odkrito nepravilnost ali nezakonito dejanje, naj bi poslovodstvo pomagalo pri preiskovanju in poizvedovanju.

2207 Nepravilnosti in nezakonita dejanja *(nadaljevanje)*

2.3 Zadolžitve strokovnjakov

2.3.1 Strokovnjaki naj proučijo, ali bodo v revizijski listini ali listini o poslu opredelili zadolžitve poslovodstva in vodstva dajanja zagotovil in revidiranja IS v zvezi s preprečevanjem in odkrivanjem nepravilnosti ter poročanjem o njih, tako da bodo te jasno razumljene za vse revizijske naloge. Kadar so te zadolžitve že dokumentirane v usmeritvah organizacije ali podobnem dokumentu, naj revizijska listina vključuje izjavo o tem.

2.3.2 Strokovnjaki naj bi razumeli, da kontrolni mehanizmi ne morejo popolnoma odpraviti možnosti pojavljanja nepravilnosti ali nezakonitih dejanj. Strokovnjaki so zadolženi za ocenjevanje tveganj pojavljanja nepravilnosti ali nezakonitih dejanj, ovrednotenje vpliva prepoznanih nepravilnosti ter zasnovo in izvedbo preizkusov, ki so primerni glede na naravo revizijskega posla.

2.3.3 Strokovnjaki pa niso zadolženi za preprečevanje ali odkrivanje nepravilnosti ali nezakonitih dejanj. Revizijski posel ne more jamčiti, da bodo nepravilnosti odkrite. Tudi če je revizija ustrezno načrtovana in izvedena, lahko nepravilnosti ostanejo neodkrite, npr. kadar gre za nedovoljeno dogovarjanje med zaposlenimi, nedovoljeno dogovarjanje med zaposlenimi in strankami zunaj organizacije, ali če je poslovodstvo samo vpleteno v te nepravilnosti. Cilj revizije pa je ugotoviti, ali so kontrole vzpostavljene, ustrezne, učinkovite in ustrezno izvajane.

2.3.4 Kadar imajo strokovnjaki določene informacije o obstoju nepravilnosti ali nezakonitega dejanja, so dolžni o njih poročati.

2.3.5 Strokovnjaki naj obvestijo poslovodstvo in pristojne za upravljanje, kadar prepoznajo stanje ali razmere povečanega tveganja za morebitno nepravilnost ali nezakonito dejanje, pa čeprav to še ni odkrito.

2.3.6 Strokovnjaki naj primerno dobro poznajo pregledovano področje, da lahko prepoznajo dejavnike tveganja, ki utegnejo prispevati k nastanku nepravilnega ali nezakonitega dejanja.

2.4 Nepravilnosti in nezakonita dejanja med načrtovanjem posla

2.4.1 Strokovnjaki naj ocenijo tveganje pojava nepravilnosti ali nezakonitih dejanj, povezanih z revidiranim področjem, s pomočjo ustrezne metodologije. Pri pripravi te ocene naj strokovnjaki upoštevajo dejavnike, kot so:

- organizacijske značilnosti, npr. podjetniška etika, organizacijska struktura, ustreznost nadzora, sistem nagrajevanja, pritiski za uspešno poslovanje podjetja, usmeritev podjetja;
- zgodovina podjetja, pojavi nepravilnosti v preteklosti in aktivnosti, ki so jim sledile za ublažitev ali zmanjšanje izsledkov, povezanih z nepravilnostmi;
- nedavne spremembe v poslovodstvu, operacijah ali sistemih IS in sedanja strateška usmeritev podjetja;
- vplivi novih strateških partnerstev;
- vrste sredstev, ki jih ima podjetje, ali storitev, ki jih ponuja, in njihova dovzetnost za nepravilnosti;
- ocenjevanje moči ustreznih kontrol in možnosti, da se vzpostavljenim kontrolam izognejo ali 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 z deležniki in finančni trgi;
- zmožnosti človeških virov;
- zaupnost in celovitost pomembnih tržnih informacij;
- revizijske ugotovitve iz prejšnjih revizij;
- panoga in konkurenčno okolje, v katerem podjetje deluje;
- ugotovitve pregledov, opravljenih zunaj obsega revizije, kot so ugotovitve svetovalcev, skupin za zagotavljanje kakovosti ali posebne preiskave poslovodstva;
- ugotovitve, ki so se pokazale med rednim poslovanjem;
- obstoj procesne dokumentacije in/ali sistem upravljanja kakovosti;
- tehnična dovršenost in zapletenost informacijskega sistema ali sistemov, ki podpirajo revidirano področje;
- obstoj v podjetju razvitih/vzdrževanih aplikacijskih sistemov za ključne poslovne sisteme v primerjavi s standardno programsko opremo;
- vpliv nezadovoljstva zaposlenih;
- morebitni delavci na čakanju, oddajanje del zunanjim izvajalcem, odprodaja poslovnih sredstev ali prestrukturiranje;
- obstoj sredstev, ki so zelo dovzetna za nezakonito prisvojitev;
- slaba organizacijska, finančna in/ali poslovna uspešnost;
- odnos poslovodstva do etičnih vprašanj;
- nepravilnosti in nezakonita dejanja, ki so običajna za določeno panogo ali so se zgodila v podobnih organizacijah.

2207 Nepravilnosti in nezakonita dejanja *(nadaljevanje)*

2.4 Nepravilnosti in nezakonita dejanja med načrtovanjem posla (nadaljevanje)

2.4.2 V okviru načrtovanja in ocenjevanje tveganj naj strokovnjaki povprašajo poslovodstvo in po potrebi pridobijo pisne predstavitve glede zadev, 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 proti organizaciji ali v njej;
- odgovornost poslovodstva za zasnovo in uvedbo notranjih kontrol za preprečevanje nepravilnosti in nezakonitih dejanj;
- kako spremljajo ali upravljajo tveganje nepravilnosti ali nezakonitih dejanj;
- kakšni postopki so vzpostavljeni za obveščanje ustreznih deležnikov o domnevah, sumih ali dejanskih nepravilnostih ali nezakonitih dejanjih;
- nacionalni in regionalni zakoni, ki veljajo v državi, v kateri organizacija deluje, in koliko njihova pravna služba sodeluje z odborom za obvladovanje tveganj in/ali revizijsko komisijo.

2.5 Zasnova in pregledovanje postopkov posla

2.5.1 Čeprav strokovnjaki niso izrecno odgovorni za odkrivanje ali preprečevanje nezakonitih dejanj ali nepravilnosti, naj za revizijski posel vendarle oblikujejo postopke, ki upoštevajo prepoznano raven tveganja nepravilnosti in nezakonitih dejanj.

2.5.2 Strokovnjaki naj izide ocenjevanja tveganj uporabijo za določitev vrste, časa in obsega preizkusov, potrebnih za pridobitev zadostnih revizijskih dokazov za sprejemljivo zagotovilo, da so ugotovljene:
- nepravilnosti, ki bi lahko pomembno vplivale na revidirano področje ali na podjetje kot celoto,
- šibkosti kontrol, ki ne bi uspešno preprečile ali odkrile pomembnih nepravilnosti,
- vse pomembne pomanjkljivosti v načrtovanju ali delovanju notranjih kontrol, ki bi lahko vplivale na zmožnost lastnika, da evidentira, obdela in povzame poslovne podatke ter o njih poroča.

2.5.3 Strokovnjaki naj bi pregledali izide postopkov posla, da bi ugotovili znake morebitnih nepravilnosti ali nezakonitih dejanj. Uporaba računalniško podprtih revizijskih tehnik (CAAT) lahko pomembno pomaga pri učinkovitem in uspešnem odkrivanju nepravilnosti ali nezakonitih dejanj.

2.5.4 Pri izvajanju tega ocenjevanja je treba pregledati dejavnike tveganja iz točke 2.4.1 na podlagi dejansko izvedenih postopkov in tako pridobiti primerno zagotovilo, da so bila obdelana vsa prepoznana tveganja.

2.6 Odzivanje na nepravilnosti in nezakonita dejanja

2.6.1 Med revizijskim poslom lahko strokovnjaki opazijo znake nepravilnosti ali nezakonitih dejanj. Upoštevajo naj morebitne učinke nepravilnosti ali nezakonitih dejanj na obravnavano zadevo posla, revizijske cilje, poročilo o revizijskem poslu in podjetje.

2.6.2 Strokovnjaki naj pokažejo <u>poklicno nezaupljivost</u>. Znaki (včasih imenovani ‘prevare ali opozorilni znaki’) oseb, ki storijo nepravilnosti ali nezakonita dejanja, so:
- neupoštevanje kontrol s strani poslovodstva,
- nepravilno ali slabo pojasnjeno obnašanje poslovodstva,
- dosledno pretirano delovanje v primerjavi z zastavljenimi cilji,
- težave ali zamude pri prejemanju zahtevanih informacij ali dokazov,
- transakcije, ki se ne izvajajo po običajnih postopkih odobritev,
- povečanje delovanja določene stranke,
- povečanje števila reklamacij strank,
- odstopanje kontrol dostopa za nekatere aplikacije ali uporabnike.

Strokovnjaki naj bodo posebej pozorni, kadar opazijo takšne pojave.

2.6.3 Kadar strokovnjaki dobijo informacijo o morebitni nepravilnosti ali nezakonitem dejanju, naj proučijo možnost, da po navodilih ustreznega pristojnega pravnega organa ukrepajo, tako da:
- se seznanijo z naravo dejanja,
- razumejo okoliščine, v katerih se je dejanje zgodilo,
- zberejo dokaze o nastanku dejanja (npr. pisma, sistemske zapise, računalniške datoteke, varnostne dnevnike, podatke o kupcu prodajnih informacij),
- ugotovijo vse osebe, vpletene v storitev dejanja,
- pridobijo zadostne dodatne informacije, da lahko ovrednotijo vpliv dejanja,
- izvedejo omejene dodatne postopke, da ugotovijo, kakšen je učinek dejanja in ali obstajajo še dodatna dejanja,
- dokumentirajo in shranijo vse dokaze in opravljeno delo.

2.6.4 Strokovnjaki naj se nato posvetujejo z vodstvom revizije, da opredelijo svoje nadaljnje ravnanje, kar lahko vključuje poročanje o dogodku poslovodstvu podjetja, predajo nadaljnjega ukrepanja notranjim preiskovalcem prevar in/ali poročanje organom pregona ali upravnim organom (regulatorjem).

2.6.5 Če je v nepravilnost vpleten član poslovodstva, naj strokovnjaki ponovno proučijo zanesljivost navedb poslovodstva. Običajno naj bi strokovnjaki sodelovali z ustrezno ravnijo vodenja, ki je nadrejena tisti, ki je povezana z nepravilnostjo ali nezakonitim dejanjem.

2207 Nepravilnosti in nezakonita dejanja *(nadaljevanje)*

2.7 Notranje poročanje

2.7.1 Strokovnjaki naj o odkritju nepravilnosti in nezakonitih dejanj (pisno ali ustno) pravočasno obvestijo ustrezne ljudi v podjetju. Obvestilo mora biti naslovljeno na raven vodenja, ki je nadrejena tisti, za katero obstaja sum pojava nepravilnosti. Poleg tega je treba o nepravilnostih in nezakonitih dejanjih poročati pristojnim za upravljanje v podjetju, kot so nadzorni svet ali upravni odbor, skrbniki, revizijska komisija ali tem enakovreden organ, razen če gre za zadeve, ki očitno nimajo pomembnega finančnega učinka in ne kažejo pomembnih slabosti v delovanju kontrol.

Če strokovnjaki sumijo, da so vpletene vse ravni vodenja, je treba o ugotovitvah zaupno poročati neposredno pristojnim za upravljanje podjetja, kot so nadzorni svet ali upravni odbor, skrbniki, revizijska komisija ali ustrezen organ v skladu z lokalno veljavnimi zakoni in predpisi. Lokalni zakoni in predpisi lahko prepovedujejo poročanje drugim strankam, razen tistim, ki jih je s predpisom določil pristojni upravni organ.

2.7.2 Pri poročanju o nepravilnosti ali nezakonitem dejanju naj strokovnjaki uporabijo strokovno presojo. Z ustrezno ravnijo vodenja, ki je najmanj za eno raven višja od domnevno vpletenih oseb, naj se pogovorijo o izsledkih in o vrsti, času in obsegu kakršnih koli nadaljnjih postopkov, ki jih je treba opraviti. V takšnih okoliščinah je še posebej pomembno, da strokovnjaki ohranijo neodvisnost.

2.7.3 Skrbno je treba razmisliti, katere posameznike vključiti v notranje razdeljevanje poročil o nepravilnostih ali nezakonitih dejanjih. Pojav in učinek nepravilnosti ali nezakonitih dejanj je občutljiva zadeva in tudi razdeljevanje poročila je povezano s tveganji, kot so:

- nadaljnja zloraba slabosti v delovanju kontrol kot posledica objave njihovih podrobnosti,
- izguba strank, dobaviteljev in vlagateljev, če pride do (pooblaščenega ali nepooblaščenega) razkritja zunaj podjetja,
- izguba ključnega osebja in poslovodstva, vključno s tistimi, ki niso bili vpleteni v nepravilnost ali nezakonito dejanje, ker upade zaupanje v poslovodstvo in prihodnost podjetja.

2.7.4 Strokovnjaki naj razmislijo o poročanju o nepravilnosti ali nezakonitem dejanju ločeno od vseh drugih revizijskih zadev, če bi to pomagalo pri nadzoru nad razdeljevanjem poročila.

2.7.5 Strokovnjaki naj se skušajo izogniti opozarjanju kogar koli, ki bi bil lahko povezan ali vpleten v nepravilnost ali nezakonito dejanje, da zmanjšajo možnost, da bi taki posamezniki uničili ali prikrili dokaze.

2.7.6 V revizijski listini naj bi bile opredeljene zadolžitve strokovnjakov glede poročanja o nepravilnostih ali nezakonitih dejanjih.

2.8 Zunanje poročanje

2.8.1 Zunanje poročanje o prevarah, nepravilnostih ali nezakonitih dejanjih utegne biti zakonska ali drugače predpisana obveznost. Ta obveznost lahko velja za poslovodstvo podjetja ali za posameznike, ki so vključeni v odkrivanje nepravilnosti, ali za oboje. Za zakonsko predpisane zahteve poročanja revizorja velja pravni red države ne glede na notranjo usmeritev organizacije in/ali pogodbene dogovore. Dodatne okoliščine, pri katerih je lahko zahtevano zunanje poročanje, so še:

- skladnost z zakonskimi ali drugimi predpisanimi zahtevami,
- odredba sodišča,
- agencija za financiranje ali vladna agencija v skladu z zahtevami za revizijo organizacij, ki prejemajo državno finančno pomoč,
- zahteve zunanjega revizorja.

2.8.2 Kadar je zahtevano zunanje poročanje, bi morala obliko in vsebino poročanih informacij pred zunanjo objavo odobriti ustrezna raven vodstva dajanja zagotovil in revidiranja IS in jih pregledati skupaj z izvršnim vodstvom revidiranca, razen če to preprečujejo veljavni predpisi ali posebne okoliščine revizijskega posla. Primeri posebnih okoliščin, ki bi lahko preprečili pridobitev soglasja izvršnega vodstva revidiranca, so med drugim:

- dejavna vpletenost izvršnega vodstva revidiranca v nepravilnost ali nezakonito dejanje,
- nedejavna privolitev izvršnega vodstva revidiranca v nepravilnost ali nezakonito dejanje.

2.8.3 Če se izvršno vodstvo revidiranca ne strinja z zunanjo objavo poročila in je zunanje poročanje zakonska ali drugače predpisana obveznost, naj strokovnjaki razmislijo o posvetovanju z revizijsko komisijo in pravnim svetovalcem o tem, ali je priporočljivo poročati o ugotovitvah zunaj podjetja in kakšna so s tem povezana tveganja. Celo kadar so strokovnjaki zaščiteni z imuniteto, naj pred tovrstnim razkritjem poiščejo pravno pomoč in nasvet, da si zagotovijo, da so s tako imuniteto dejansko zaščiteni.

2.8.4 Strokovnjaki naj z odobritvijo vodstva dajanja zagotovil in revidiranja IS poročilo o nepravilnostih ali nezakonitih dejanjih pravočasno oddajo ustreznim upravnim organom. Če podjetje ne razkrije znane nepravilnosti ali nezakonitega dejanja ali če od strokovnjakov zahteva, da take ugotovitve prikrijejo, morajo strokovnjaki poiskati pravno pomoč in nasvet.

2.8.5 Če so nepravilnost ali nezakonito dejanje odkrili strokovnjaki sami, naj o tem pravočasno obvestijo zunanje revizorje.

2.8.6 Kadar je strokovnjakom znano, da je poslovodstvo dolžno prijaviti prevarantske aktivnosti zunanji organizaciji, morajo uradno opozoriti poslovodstvo na to njihovo obveznost.

2207 Nepravilnosti in nezakonita dejanja *(nadaljevanje)*

3. Povezava s standardi in procesi v COBIT 5

3.0 Uvod

To poglavje daje pregled ustreznih:
3.1 Povezav s standardi
3.2 Povezav s procesi v COBIT 5
3.3 Drugih navodil

3.1 Povezava s standardi

V tabeli je pregled:
- najpomembnejših standardov ISACA, ki jih neposredno podpira ta smernica;
- tistih zahtev standardov, ki so najpomembnejše za to smernico.

Opomba: Naštete so samo tiste zahteve standardov, ki so pomembne za to smernico.

Naslov standarda	Pomembne zahteve standarda
1005 Potrebna poklicna skrbnost	Strokovnjaki dajanja zagotovil in revidiranja IS morajo pri načrtovanju in izvajanju poslov ter poročanju o izidih ravnati s potrebno poklicno skrbnostjo, vključno z upoštevanjem veljavnih strokovnih standardov za revizijo.
1201 Načrtovanje posla	Strokovnjaki dajanja zagotovil in revidiranja IS morajo načrtovati vsak posel dajanja zagotovil in revidiranja IS z namenom, da obravnavajo: • 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 značilna za posel, • zahteve glede dokumentacije in poročanja.
1202 Ocenjevanje tveganja pri načrtovanju	Pri dajanju zagotovil in revidiranju IS morata biti za pripravo celotnega načrta revidiranja IS in določitev prednosti za učinkovito dodelitev virov za revizijo IS uporabljena ustrezen pristop in pripadajoča metodologija za oceno tveganja. Strokovnjaki dajanja zagotovil in revidiranja IS morajo pri načrtovanju posameznih poslov prepoznati in oceniti tveganje, ki se nanaša na področje pregleda. Strokovnjaki dajanja zagotovil in revidiranja IS morajo proučiti tveganja, povezana z obravnavano zadevo, revizijsko tveganje in vpliv na izpostavljenost podjetja.
1207 Nepravilnosti in nezakonita dejanja	Strokovnjaki dajanja zagotovil in revidiranja IS morajo med izvajanjem posla upoštevati tveganja nepravilnosti in nezakonitih dejanj. Strokovnjaki dajanja zagotovil in revidiranja IS morajo med izvajanjem posla ohranjati poklicno nezaupljivost. Strokovnjaki dajanja zagotovil in revidiranja IS morajo dokumentirati in primerni stranki pravočasno sporočiti vsako pomembno nepravilnost ali nezakonito dejanje.
1401 Poročanje	Strokovnjaki dajanja zagotovil in revidiranja IS morajo zagotoviti, da so ugotovitve v revizijskem poročilu podprte z zadostnimi in ustreznimi revizijskimi dokazi.

2207 Nepravilnosti in nezakonita dejanja *(nadaljevanje)*

3.2 Povezava s procesi v COBIT 5

V tabeli je pregled najpomembnejših:
- procesov v COBIT 5,
- namenov procesov v COBIT 5.

Posebne aktivnosti, ki se izvajajo kot del teh procesov, so v *COBIT 5: Omogočanje procesov*.

Proces v COBIT 5	Namen procesa
EDM03 Zagotovite optimizacijo tveganja.	Zagotovite, da tveganje, povezano z IT v podjetju, ne preseže pripravljenosti za prevzemanje tveganj in sprejemljivega tveganja, da je vpliv tveganja IT na vrednost podjetja prepoznan in obvladovan ter da so možnosti za neskladnost s predpisi čim manjše.
APO12 Upravljajte tveganje.	Združite upravljanje tveganja, povezanega z IT, s celotnim obvladovanjem tveganja v podjetju (ERM) in izravnajte stroške in koristi upravljanja tveganja, povezanega z IT v podjetju.
MEA02 Spremljajte, vrednotite in ocenjujte sistem notranjih kontrol.	Ključnim deležnikom omogočite pregled nad ustreznostjo sistema notranjih kontrol in s tem zagotovite zaupanje v delovanje, vero v doseganje ciljev podjetja in ustrezno razumevanje preostalega tveganja.
MEA03 Spremljajte, vrednotite in ocenjujte skladnost z zunanjimi zahtevami.	Zagotovite, da podjetje ravna v skladu z vsemi veljavnimi zunanjimi zahtevami.

3.3 Druga navodila

Pri izvajanju standardov in smernic naj strokovnjaki po potrebi poiščejo še druga navodila. Za dajanje zagotovil in revidiranje IS jih lahko pridobijo:
- od kolegov v podjetju,
- od vodstva,
- od organov upravljanja v podjetju, npr. od revizijske komisije,
- od strokovnih organizacij,
- iz drugih strokovnih navodil (npr. knjig, člankov, drugih smernic).

4. Izrazi

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

5. Datum uveljavitve

5.1 Datum uveljavitve

Ta smernica velja za vse posle dajanja zagotovil in revidiranja IS, ki se začnejo 1. septembra 2014 ali pozneje.

2208 Vzorčenje

Smernica je predstavljena v naslednjih poglavjih:
1. Namen smernice in povezava s standardi
2. Vsebina smernice
3. Povezava s standardi in procesi v COBIT 5
4. Izrazi
5. Datum uveljavitve

1. Namen smernice in povezava s standardi

1.0 Uvod

V tem poglavju so razjasnjeni:
1.1 Namen smernice
1.2 Povezava s standardi
1.3 Uporaba izrazov ‘revidiranje’ in ‘strokovnjaki’

1.1 Namen

1.1.1 Namen te smernice je dati strokovnjakom dajanja zagotovil in revidiranja IS navodila za zasnovo in izbiro revizijskega vzorca in za ovrednotenje izidov vzorca. Ustrezno vzorčenje in ocenjevanje bo pomagalo pri doseganju zahtev po zadostnih in ustreznih dokazih.

1.1.2 Strokovnjaki dajanja zagotovil in revidiranja IS naj bi upoštevali to smernico pri odločanju, kako izvajati standard, uporabiti strokovno presojo pri uporabi, utemeljiti vsako odstopanje in po potrebi poiskati dodatna navodila.

1.2 Povezava s standardi

1.2.1 Standard 1006 Strokovna usposobljenost
1.2.2 Standard 1202 Ocenjevanje tveganja pri načrtovanju
1.2.3 Standard 1203 Izvedba in nadzor
1.2.4 Standard 1205 Dokazi

1.3 Uporaba izrazov

1.3.1 V nadaljnjem besedilu:
- se ‘dajanje zagotovil in revidiranje IS’ imenuje ‘revidiranje’;
- se ‘strokovnjaki dajanja zagotovil in revidiranja IS’ imenujejo ‘strokovnjaki’.

2. Vsebina smernice

2.0 Uvod

Poglavje o vsebini smernice je sestavljeno tako, da daje informacije o naslednjih ključnih temah posla dajanja zagotovil in revidiranja IS:
2.1 Vzorčenje
2.2 Zasnova vzorca
2.3 Izbira vzorca
2.4 Ovrednotenje izidov vzorca
2.5 Dokumentacija

2.1 Vzorčenje

2.1.1 Pri oblikovanju mnenja ali sklepa strokovnjaki pogosto ne proučijo vseh razpoložljivih informacij, ker bi bilo to težko izvedljivo (preiskovanje vseh informacij bi na primer zahtevalo preveč časa tako revidiranca kot strokovnjakov) in je do veljavnih sklepov mogoče priti z uporabo revizijskega vzorčenja.

2.1.2 Pri uporabi statističnih ali nestatističnih metod vzorčenja morajo strokovnjaki oblikovati in izbrati revizijski vzorec, izvesti revizijske postopke in ovrednoti izide vzorca, da pridobijo zadostne in ustrezne dokaze za oblikovanje sklepa. Kadar uporabljajo metode vzorčenje za oblikovanje sklepa o celotni populaciji, morajo strokovnjaki uporabiti statistično vzorčenje.

2208 Vzorčenje *(nadaljevanje)*

2.2 Zasnova vzorca

2.2.1 Pri oblikovanju velikosti in sestave revizijskega vzorca morajo strokovnjaki upoštevati posebne cilje revizije IS, revizijske postopke, s katerimi bo te cilje najverjetneje mogoče doseči, naravo populacije, pomembne podskupine v populaciji ter metode vzorčenja in izbiranja. Poleg tega je treba pri ustreznem revizijskem vzorčenju upoštevati tudi naravo iskanih dokazov, morebitne možnosti napak in možne vzroke zanje.

2.2.2 Pri oblikovanju revizijskega vzorca naj strokovnjaki ob upoštevanju ciljev revizije IS proučijo še:

- namen vzorca,
- enoto vzorčenja,
- populacijo,
- tveganje pri vzorčenju in velikost vzorca,
- dopustno napako,
- pričakovano porazdelitev (npr. Poissonovo, binomsko, normalno, eksponencialno),
- obnašanje v času (npr. sezonstvo, upadanje moči),
- podpopulacije ali podskupine, ki se naravno pojavljajo in jih je treba upoštevati zaradi operativne pomembnosti,
- odstopanja,
- majhne populacije negativnih ali redkih dogodkov,
- podatke iz zunanjih pomožnih orodij, uporabljenih za potrditev ali dopolnitev izidov vzorčenja.

2.2.3 Strokovnjaki naj bi upoštevali namen vzorca:

- **Preizkušanje skladnosti/preizkus kontrol** – revizijski postopek, zasnovan za ovrednotenje uspešnosti delovanja kontrol in preprečevanje ali odkrivanje in popravljanje pomembnih slabosti v njihovem delovanju. Primeri preizkušanja skladnosti kontrol, pri katerih bi bilo mogoče razmisliti o vzorčenju, so med drugim pravice uporabnikov do dostopa, postopki za kontroliranje sprememb v programu, dokumentacija postopkov, programska dokumentacija, nadaljnja obravnava izjem, pregled dnevnikov in revizije licenc za programsko opremo.
- **Preizkušanje podatkov/preizkus podrobnosti** – revizijski postopek, zasnovan za odkrivanje pomembnih slabosti na ravni trditev. Primeri preizkusov podatkov, pri katerih bi bilo mogoče upoštevati vzorčenje, so med drugim ponovno izvajanje zapletenega izračuna (npr. obresti) na vzorcu obračunov, vzorcu transakcij za potrditev dokazne dokumentacije itd.

2.2.4 Enota vzorčenja je odvisna od namena vzorca. Za preizkušanje skladnosti kontrol, pri katerem je enota vzorčenja neki dogodek ali transakcija (npr. kontrola, kot je potrditev računa), se običajno uporablja vzorčenje lastnosti, ker je uporabljeno za določitev značilnosti populacije. Za preizkušanje podatkov, pri čemer je enota vzorčenja denarna, se pogosto uporablja vzorčenje spremenljivk, ker je uporabljeno za določitev denarnega ali volumetričnega vpliva značilnosti populacije.

2.2.5 Populacija je celoten zbir podatkov, iz katerega želijo strokovnjaki vzeti vzorec, da pridejo do sklepa o populaciji. Zato mora biti populacija, iz katere je vzorec vzet, ustrezna za preizkus zasnove in/ali delovanja uspešnosti kontrol in preverjeno popolna za določen cilj in obseg revizije IS.

2.2.6 V pomoč za uspešno in učinkovito oblikovanje vzorca je primerno tudi razslojevanje pri vzorčenju. Razslojevanje je proces razdelitve populacije na podpulacije z izrecno opredeljenimi podobnimi značilnostmi, tako da lahko vsaka enota vzorčenja pripada samo enemu sloju.

2.2.7 Pri določanju velikosti vzorca naj strokovnjaki upoštevajo tveganje pri vzorčenju, količino napak, ki bi bila še sprejemljiva, in pričakovani obseg napak. Tveganje pri vzorčenju izhaja iz možnosti, da se sklep strokovnjakov lahko razlikuje od sklepa, do katerega bi prišli, če bi za isti revizijski postopek pregledali celotno populacijo. Poznamo dve vrsti tveganja pri vzorčenju:

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

2.2.8 Velikost vzorca vpliva na raven tveganja pri vzorčenju, ki so jo strokovnjaki pripravljeni sprejeti. Tveganje pri vzorčenju je treba obravnavati tudi glede na model revizijskega tveganja in njegove sestavine, to je tveganje pri delovanju, tveganje pri kontroliranju in tveganje pri odkrivanju, kot so podrobno opisane v Standardu 1202 Ocenjevanje tveganja pri načrtovanju.

2.2.9 Dopustna napaka je največja napaka v populaciji, ki so jo strokovnjaki pripravljeni sprejeti in pri tem še vedno sklepati, da je cilj preizkusa dosežen. Za preizkuse podatkov je dopustna napaka povezana s presojo strokovnjakov o pomembnosti. Pri preizkusih skladnosti je to največja stopnja odstopanja od predpisanega kontrolnega postopka, ki so jo strokovnjaki še pripravljeni sprejeti.

2208 Vzorčenje *(nadaljevanje)*

2.2. Zasnova vzorca *(nadaljevanje)*

2.2.10 Če strokovnjaki pričakujejo, da bodo v populaciji napake, je treba pregledati večji vzorec, kot če jih v njem ni pričakovati, da lahko ugotovijo, da dejanska napaka v populaciji ni večja od pričakovane dopustne napake. Manjše velikosti vzorcev so upravičene, kadar se pričakuje, da v populaciji ni napak. Pri oceni pričakovanih napak v populaciji naj strokovnjaki upoštevajo zadeve, kot so:

- količine napak, ugotovljene v prejšnjih revizijah,
- spremembe postopkov v podjetju,
- dokazi, ki so na razpolago iz ocenjevanja sistema notranjih kontrol, izidov analitičnih pregledov in/ali izidov predhodnih preizkusov populacije.

2.2.11 Strokovnjaki naj upoštevajo, da je treba, kadar je to primerno, k zasnovi in analizi zapletenih načinov vzorčenja pritegniti specialiste; taki so na primer razslojeni naključni vzorci, ki morajo biti statistično veljavni, ali vzorčenje na podlagi uveljavljenih metodologij kontrole kakovosti (npr. 6-Sigma).

2.2.12 Če bi strokovnjaki ugotovili, da vzorčenje ne omogoča doseganja ciljev revizije IS in je treba preizkusiti celotno populacijo, naj upoštevajo možnost stalnega dajanja zagotovil, ker tak pristop omogoča pravočasno in stroškovno učinkovito preizkušanje celotne populacije.

2.3 Izbira vzorca

2.3.1 Strokovnjaki naj zagotovijo, da je populacija popolna, in nadzorujejo izbiro vzorca, da ohranijo revizijsko neodvisnost. Strokovnjaki naj izberejo vzorec tako, da je v vzorcu pričakovana reprezentativna populacija glede na značilnosti, ki se preizkušajo.

2.3.2 Da bo vzorec reprezentativen za celotno populacijo, naj bi imele vse enote vzorčenja v populaciji enako ali znano, neničelno verjetnost, da so izbrane. To pomeni uporabo statističnih metod vzorčenja, saj te vključujejo uporabo tehnik, iz katerih je mogoče priti do matematično zgrajenih ugotovitev za celotno populacijo. Strokovnjaki morajo torej preveriti in potrditi popolnost populacije in s tem zagotoviti, da je vzorec izbran iz ustreznega niza podatkov.

2.3.3 Nestatistično vzorčenje uporabljajo strokovnjaki, ki želijo uporabiti svoje lastne izkušnje, znanje in strokovno presojo za določitev vzorca. Ta metoda vsebuje človeško pristranskost, ker nima statistične podlage in ne zagotavlja, da ima vsaka enota vzorčenja znano, neničelno verjetnost, da je izbrana; zato se njenih izidov ne sme ekstrapolirati na vso populacijo, ker vzorec verjetno ni reprezentativen za celotno populacijo. Nestatistično vzorčenje se sme uporabiti, kadar so hitro potrebni izidi za potrditev nekega predloga, ne sme pa se ga uporabiti za pridobitev matematično sestavljenega sklepa v zvezi s celotno populacijo.

2.3.4 Običajno se uporablja pet metod vzorčenja, ki se delijo na statistične metode vzorčenja ali na nestatistične metode vzorčenja.

- Metode statističnega vzorčenja so:
  - **enostavno naključno vzorčenje** zagotavlja, da imajo vse kombinacije enot vzorčenja v populaciji enako možnost, da so izbrane;
  - **sistematično vzorčenje** vključuje izbiranje enot vzorčenja z uporabo določenega intervala med izbiro enot, pri čemer se prvi interval začne naključno. Tak primer je vzorčenje po denarni enoti ali izbira po tehtani vrednosti, pri čemer ima vsaka posamezna denarna vrednost (npr. 1000 USD) v populaciji enako možnost, da je izbrana. Ker posamezne denarne enote običajno ni mogoče pregledovati ločeno, je za pregledovanje izbrana postavka, ki vsebuje to denarno enoto. Ta metoda sistematično tehta izbiro v korist večjih zneskov. Drug primer pa je izbiranje vsake n-te enote vzorčenja;
  - **razslojeno naključno vzorčenje** zagotavlja, da imajo vse enote vzorčenja v vsaki podskupini znano, neničelno možnost, da so izbrane.

  Strokovnjaki naj upoštevajo možnost uporabe statistične programske opreme za izračunavanje standardnih odstopanj in drugih zbirnih statističnih podatkov za izide statističnega vzorčenja.
- Nestatistične metode vzorčenja so:
  - **vzorčenje na slepo** – strokovnjaki izberejo vzorec brez kakršne koli strukturirane metode, pri čemer se izogibajo vsake zavestne pristranskosti ali predvidljivosti. Vendar pa se na analizo na slepo izbranega vzorca ne smejo opirati pri oblikovanju sklepa o populaciji;
  - **vzorčenje po presoji** – strokovnjaki sestavijo vzorec po lastni presoji (npr. vse enote vzorčenja nad določeno vrednostjo, vse enote za določeno vrsto izjeme, vse negativne postavke). Opozoriti je treba, da po presoji izbran vzorec nima statistične podlage in se izidov ne sme ekstrapolirati na vso populacijo, ker vzorec verjetno ni reprezentativen za celotno populacijo.

2208 Vzorčenje *(nadaljevanje)*

2.3 Izbira vzorca *(nadaljevanje)*

2.3.5 Običajno se uporabljata dve metodi izbiranja:

- izbiranje po evidencah in podskupinah populacije; običajne metode so:
  - enostavno naključno vzorčenje,
  - razslojeno naključno vzorčenje,
  - vzorčenje na slepo,
  - vzorec po presoji;
- izbiranje po količinskih merilih (npr. denarne enote); običajne metode so:
  - enostavno vzorčenje na slepo,
  - sistematično vzorčenje.

2.4 Ovrednotenje izidov vzorca

2.4.1 Potem ko so za vsako postavko vzorca izvedeni revizijski postopki, ki ustrezajo določenemu cilju revizije IS, naj strokovnjaki analizirajo vse odkrite morebitne napake v vzorcu, da ugotovijo, ali so to dejanske napake, in če je primerno, tudi vrsto in vzrok teh napak. Če je bila uporabljena statistična metoda vzorčenja, je treba napake, ki so ocenjene kot dejanske, projicirati kot ustrezne za celotno populacijo.

2.4.2 Pregledati je treba vse morebitne odkrite napake v vzorcu, da se ugotovi, ali so to dejanske napake. Strokovnjaki naj upoštevajo kakovostne vidike napak. To sta med drugim narava in vzrok napake in možni učinek napake na druge faze revizije. Napake, ki so posledica okvare avtomatiziranega procesa, imajo običajno na primer širši vpliv kot človeške napake.

2.4.3 Kadar pričakovanih revizijskih dokazov v zvezi z določeno vzorčno enoto ni mogoče pridobiti, naj strokovnjaki proučijo, ali lahko pridobijo zadostne in ustrezni revizijske dokaze za izbrano postavko z izvajanjem drugih možnih postopkov ali z izbiranjem in preizkušanjem nadomestne vzorčne enote.

2.4.4 Strokovnjaki naj upoštevajo projiciranje izidov vzorca na populacijo z metodo projiciranja, ki je skladna z metodo, uporabljeno za izbiro enote vzorčenja. 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.

2.4.5 Razprava o izidih nestatističnega vzorčenja (na slepo ali po presoji) naj bo omejena samo na opis izidov analiziranja vzorca v povezavi s populacijo kot celoto.

2.4.6 Strokovnjaki naj proučijo, ali bi napake v populaciji lahko presegle dopustno napako, in sicer tako, da primerjajo projicirano napako populacije z ocenjeno ali opredeljeno dopustno napako, pri čemer upoštevajo izide drugih revizijskih postopkov, pomembnih za cilj revizije. Dopustna napaka je lahko ocenjena ali opredeljena z revizijskimi merili, panožnimi standardi, pogodbenimi zahtevami, specifikacijami programske opreme itd. Kadar je projicirana napaka populacije večja od dopustne napake, morajo strokovnjaki ponovno oceniti tveganje pri vzorčenju, in če je tveganje nesprejemljivo, razmisliti o razširitvi revizijskega postopka, ponovnem izračunu velikosti vzorca ob uporabi na novo opredeljene dopustne napake in o preizkušanju dodatnih vzorčnih enot ali izvajanju drugih možnih revizijskih postopkov.

2.5 Dokumentacija

2.5.1 Delovno gradivo naj bi vključevalo dovolj podrobnosti za jasen opis cilja vzorčenja in uporabljenih postopkov vzorčenja. Delovno gradivo naj bi vključevalo:

- namen vzorca, vključno z vzorčno enoto,
- vir populacije, opredelitev pojma populacije in njeno razmerje do obsega revizije,
- parametre vzorčenja, npr. velikost vzorca (vključno z vsemi premisleki glede tveganja pri vzorčenju), naključno začetno ali izhodiščno številko ali metodo za določitev naključnega začetka, interval vzorčenja,
- metodo vzorčenja,
- izbrane postavke in pri uporabi nestatističnega vzorčenja tudi utemeljitev za izbrane postavke,
- podrobnosti izvedenih revizijskih preizkusov, vključno z ocenjevanjem napak, in če je ustrezno, druge možne revizijske postopke,
- sprejete sklepe.

2208 Vzorčenje *(nadaljevanje)*

3. Povezava s standardi in procesi v COBIT 5

3.0 Uvod

To poglavje daje pregled ustreznih:
3.1 Povezav s standardi
3.2 Povezav s procesi v COBIT 5
3.3 Drugih navodil

3.1 Povezava s standardi

V tabeli je pregled:
- najpomembnejših standardov ISACA, ki jih neposredno podpira ta smernica;
- tistih zahtev standardov, ki so najpomembnejše za to smernico.

Opomba: Naštete so samo tiste zahteve standardov, ki so pomembne za to smernico.

Naslov standarda	Pomembne zahteve standarda
1006 Strokovna usposobljenost	Strokovnjaki dajanja zagotovil in revidiranja IS morajo imeti 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.
1202 Ocenjevanje tveganja pri načrtovanju	Strokovnjaki dajanja zagotovil in revidiranja IS morajo proučiti tveganja, povezana z obravnavano zadevo, revizijsko tveganje in vpliv na izpostavljenost podjetja.
1203 Izvedba in nadzor	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. Strokovnjaki dajanja zagotovil in revidiranja IS morajo revizijski postopek dokumentirati z opisi revizijskega dela in revizijskimi dokazi, ki podpirajo ugotovitve in sklepe. Strokovnjaki dajanja zagotovil in revidiranja IS morajo prepoznavati in sklepati na podlagi ugotovitev.
1205 Dokazi	Strokovnjaki dajanja zagotovil in revidiranja IS morajo pridobiti zadostne in ustrezne dokaze, da lahko sprejmejo primerne sklepe, s katerimi utemeljijo izide posla. Strokovnjaki dajanja zagotovil in revidiranja IS morajo ovrednotiti zadostnost dokazov, pridobljenih za utemeljitev sklepov in doseganje ciljev posla.

3.2 Povezava s procesi v COBIT 5

V tabeli je pregled najpomembnejših:
- procesov v COBIT 5,
- namenov procesov v COBIT 5.

Posebne aktivnosti, ki se izvajajo kot del teh procesov, so v *COBIT 5: Omogočanje procesov*.

Proces v COBIT 5	Namen procesa
APO12 Upravljajte tveganje.	Združite upravljanje tveganja, povezanega z IT, s celotnim obvladovanjem tveganja v podjetju (ERM) in izravnajte stroške in koristi upravljanja tveganja, povezanega z IT v podjetju.
MEA02 Spremljajte, vrednotite in ocenjujte sistem notranjih kontrol.	Ključnim deležnikom omogočite pregled nad ustreznostjo sistema notranjih kontrol in s tem zagotovite zaupanje v delovanje, vero v doseganje ciljev podjetja in ustrezno razumevanje preostalega tveganja.
MEA03 Spremljajte, vrednotite in ocenjujte skladnost z zunanjimi zahtevami.	Zagotovite, da podjetje ravna v skladu z vsemi veljavnimi zunanjimi zahtevami.

2208 Vzorčenje *(nadaljevanje)*

3.3 Druga navodila Pri izvajanju standardov in smernic naj strokovnjaki po potrebi poiščejo še druga navodila. Za dajanje zagotovil in revidiranje IS jih lahko pridobijo:

- od kolegov v podjetju,
- od vodstva,
- od organov upravljanja v organizaciji, npr. od revizijske komisije,
- od strokovnih organizacij,
- iz drugih strokovnih navodil (npr. knjig, člankov, drugih smernic).

4. Izrazi

Izraz	Pomen
Vzorčenje lastnosti	Metoda izbiranja dela populacije na podlagi prisotnosti ali odsotnosti nekaterih značilnosti.
Revizijsko vzorčenje	Uporaba revizijskih postopkov na manj kot 100 odstotkih elementov v populaciji za pridobitev revizijskih dokazov o določeni značilnosti populacije.
Nestatistično vzorčenje	Metoda izbiranja dela populacije s pomočjo lastne presoje in izkušenj za hitro potrjevanje kakšnega predloga. Ta metoda ne omogoča izvajanja matematičnih sklepov za celotno populacijo.
Populacija	Celoten zbir podatkov, iz katerih je izbran vzorec, in o katerih želi revizor IS priti do sklepov.
Tveganje pri vzorčenju	Verjetnost, da je revizor IS prišel do napačnega sklepa, ker je bil preizkušen le revizijski vzorec, ne pa celotna populacija. Opomba: tveganje pri vzorčenju je sicer mogoče zmanjšati na sprejemljivo nizko raven z uporabo ustrezne velikosti vzorca in izbiro metode, nikoli pa ga ni mogoče odpraviti.
Razslojevanje pri vzorčenju	Razdelitev populacije na podpopulacije z izrecno opredeljenimi značilnostmi, tako da vsaka enota vzorčenja lahko pripada samo enemu sloju.
Statistično vzorčenje	Metoda izbiranja dela populacije s pomočjo matematičnih izračunov in verjetnosti za pridobitev znanstveno in matematično utemeljenih sklepov glede značilnosti celotne populacije.
Dopustna napaka	Največja napaka v populaciji, ki so jo strokovnjaki pripravljeni sprejeti in pri tem še vedno sklepati, da je revizijski cilj dosežen. Za postopke preizkušanja podatkov je dopustna napaka povezana s presojo strokovnjakov o pomembnosti. Pri preizkusih skladnosti je to največja stopnja odstopanja od predpisanega kontrolnega postopka, ki so ga strokovnjaki še pripravljeni sprejeti.
Vzorčenje spremenljivk	Metoda vzorčenja, ki se uporablja za oceno povprečne ali skupne vrednosti populacije na podlagi vzorca; statistični model, uporabljen za projiciranje neke količinske značilnosti, kot je na primer denarni znesek.

5. Datum uveljavitve

5.1 Datum uveljavitve Ta smernica velja za vse posle dajanja zagotovil in revidiranja IS, ki se začnejo 1. septembra 2014 ali pozneje.

Smernice poročanja

Smernici poročanja sta:
2401 Poročanje
2402 Nadaljnja obravnava

Smernice so tukaj vključene v celoti. Za povezave s posameznimi standardi obiščite *www.isaca.org/standard*.

2401 Poročanje

Smernica je predstavljena v naslednjih poglavjih:
1. Namen smernice in povezava s standardi
2. Vsebina smernice
3. Povezava s standardi in procesi v COBIT 5
4. Izrazi
5. Datum uveljavitve

1. Namen smernice in povezava s standardi

1.0 Uvod

V tem poglavju so razjasnjeni:
1.1 Namen smernice
1.2 Povezava s standardi
1.3 Uporaba izrazov ‘revidiranje’ in ‘strokovnjaki’

1.1 Namen

1.1.1 Ta smernica daje navodila za strokovnjake dajanja zagotovil in revidiranja IS o različnih vrstah poslov revidiranja IS in z njimi povezanih poročil.

1.1.2 Smernica podrobno določa vse vidike, ki naj bi bili vključeni v poročilo revizijskega posla in daje strokovnjakom dajanja zagotovil in revidiranja IS navodila, kaj morajo upoštevati pri pripravi in dokončanju poročila o revizijskem poslu.

1.1.3 Strokovnjaki dajanja zagotovil in revidiranja IS naj bi upoštevali to smernico pri odločanju, kako izvajati standard, uporabiti strokovno presojo pri uporabi, utemeljiti vsako odstopanje in po potrebi poiskati dodatna navodila.

1.2 Povezava s standardi

1.2.1 Standard 1007 Trditve
1.2.2 Standard 1205 Dokazi
1.2.3 Standard 1401 Poročanje
1.2.4 Standard 1402 Nadaljnja obravnava

1.3 Uporaba izrazov

1.3.1 V nadaljnjem besedilu:
- se ‘dajanje zagotovil in revidiranje IS’ imenuje ‘revidiranje’;
- se ‘strokovnjaki dajanja zagotovil in revidiranja IS’ imenujejo ‘strokovnjaki’.

2. Vsebina smernice

2.0 Uvod

Poglavje o vsebini smernice je sestavljeno tako, da daje informacije o naslednjih ključnih temah posla dajanja zagotovil in revidiranja IS:
2.1 Vrste poslov
2.2 Zahtevane vsebine poročila o revizijskem poslu
2.3 Poznejši dogodki
2.4 Dodatno obveščanje

2401 Poročanje *(nadaljevanje)*

2.1 Vrste poslov

2.1.1 Strokovnjaki lahko opravljajo vsako od naslednjih vrst revizijskih poslov:
- preiskovanje,
- pregled,
- dogovorjeni postopki.

Opomba: Ti pojmi so opredeljeni v ITAF, 2. izdaja.

2.1.2 Tako posli preiskovanja kot posli pregleda vključujejo:
- načrtovanje posla;
- ovrednotenje uspešnosti zasnove kontrolnih postopkov;
- preizkušanje uspešnost delovanja kontrolnih postopkov (vrsta, čas in obseg preizkušanja se razlikujejo med obema vrstama poslov);
- oblikovanje sklepa in poročanje o zasnovi in/ali uspešnosti delovanja kontrolnih postopkov na podlagi opredeljenih meril:
  – sklep za posel dajanja sprejemljivega zagotovila je izražen kot pozitivno mnenje in daje visoko raven zagotovila,
  – sklep za posel dajanja omejenega zagotovila je izražen kot negativno mnenje in daje le zmerno raven zagotovila.

2.1.3 Posel izvajanja dogovorjenih postopkov se ne konča z izražanjem kakršnega koli zagotovila strokovnjakov. Strokovnjaki so najeti za izvedbo določenih postopkov za zagotovitev potrebnih informacij strankam, ki so se dogovorile za postopke, ki jih je treba opraviti (npr. izvršno vodstvo, organ nadzora ali pristojni za upravljanje). Strokovnjaki izdajo poročilo o dejanskih ugotovitvah tistim strankam, ki so se dogovorile za postopke. Prejemniki iz tega poročila oblikujejo svoje sklepe, ker vrsta, čas in obseg postopkov strokovnjakom ne omogočajo, da bi izrazili kakršno koli zagotovilo. Poročilo je omejeno na tiste stranke, ki so se dogovorile za postopke, ki jih je treba opraviti, ker drugi ne poznajo razlogov za te postopke in bi si njihove izide lahko napačno razlagali.

2.1.4 Poročilo o dogovorjenih postopkih bi bilo lahko poslano tudi tretji stranki (npr. regulativnemu organu), kadar so stranke, ki so se dogovorile za postopke, tako vnaprej določile in odobrile še pred začetkom dejanskega dela. Strokovnjaki morajo to upoštevati in ravnati po svoji strokovni presoji glede na tveganje napačnega tolmačenja dela, ki ga je treba opraviti.

2.1.5 Strokovnjaki, od katerih se pred dokončanjem revizijskega posla zahteva, da revizijski posel iz posla preiskovanja ali pregleda spremenijo v posel o dogovorjenih postopkih, naj razmislijo o ustreznost takega ravnanja in s tako spremembo ne morejo soglašati, kadar zanjo ni razumne utemeljitve. Sprememba na primer ni primerna, če naj bi se s tem izognili poročilu s pridržki.

2.2 Zahtevane vsebine poročila o revizijskem poslu

2.2.1 Pri pripravi poročila je treba upoštevati vse pomembne pridobljene dokaze, ne glede na to, ali informacije zadevo potrjujejo ali ji nasprotujejo. Kadar je dano mnenje, naj bo to podprto z izidi kontrolnih postopkov na podlagi opredeljenih meril. Strokovnjaki morajo ugotoviti, ali so pridobljeni zadostni in ustrezni dokazi za utemeljitev sklepov v poročilu o revizijskem poslu. Podrobnejša navodila lahko najdete v standardu 1205 Dokazi.

2.2.2 Ob končanju posla preiskovanja ali pregleda naj bi strokovnjaki izrazili mnenje o tem, ali sta bila zasnova in/ali delovanje kontrolnih postopkov za zadevno področje dejavnosti v vseh pomembnih pogledih učinkovita. To mnenje je lahko:
- **pozitivno** – strokovnjaki naj bi izrazili pozitivno mnenje, kadar ugotovijo, da sta bila zasnova in/ali delovanje kontrolnih postopkov za zadevno področje dejavnosti v vseh pomembnih pogledih v skladu veljavnimi merili učinkovita;
- **s pridržki** – strokovnjaki naj bi izrazili mnenje s pridržki, kadar:
  – po pridobljenih zadostnih in ustreznih dokazih sklepajo, da so slabosti kontrol posamično ali vse skupaj za cilje revizije IS pomembne, vendar ne vseobsegajoče,
  – ne morejo pridobiti zadostnih in ustreznih dokazov za utemeljitev mnenja, vendar sklepajo, da bi bili morebitni učinki neodkritih slabosti na cilje revizije IS lahko pomembni, vendar ne vseobsegajoči;
- **odklonilno** – strokovnjaki naj bi izrazili negativno mnenje, kadar se ena ali več pomembnih pomanjkljivosti združujejo v pomembno in vseobsegajočo slabost;
- **zavrnjeno** – strokovnjaki naj bi zavrnili izdajo mnenja, kadar ne morejo pridobiti zadostnih in ustreznih dokazov za utemeljitev mnenja in sklepajo, da bi bili morebitni učinki neodkritih slabosti na cilje revizije IS lahko pomembni in vseobsegajoči.

2401 Poročanje *(nadaljevanje)*

2.2 Zahtevane vsebine poročila o revizijskem poslu (nadaljevanje)

2.2.3 Poročilo strokovnjakov o preiskovanju ali pregledu uspešnosti kontrolnih postopkov naj vključuje naslednje sestavine:

- ustrezen in razlikovalen naslov, po katerem se poročilo jasno razlikuje od vseh drugih vrst poročil, ki niso podrejena standardom revidiranja;
- določitev prejemnikov, ki jim je poročilo namenjeno v skladu z določili v revizijski listini ali listini o poslu;
- določitev odgovorne stranke, vključno z izjavo stranke, ki je zadolžena za obravnavano zadevo;
- opis obsega revizijskega posla, ime organizacije ali dela organizacije, na katerega se obravnavana zadeva nanaša, kar vključuje tudi:
  – opredelitev ali opis področja dejavnosti,
  – merila, uporabljena kot podlaga za sklep strokovnjakov,
  – čas ali obdobje, na katero se nanaša delo, ocenjevanje ali merjenje obravnavane zadeve,
  – izjavo, da je za vzdrževanje učinkovitega ustroja notranje kontrole, vključno s kontrolnimi postopki za področje dejavnosti, odgovorno poslovodstvo;
- izjavo z opredelitvijo vira navedbe poslovodstva o uspešnosti kontrolnih postopkov;
- izjavo, da so strokovnjaki opravili revizijski posel zato, da izrazijo mnenje o uspešnosti kontrolnih postopkov;
- opredelitev namena (to je ciljev revizije IS), za katerega je bilo poročilo strokovnjakov pripravljeno, in tistih, ki so se upravičeni nanj opirati, ter izjava o neprevzemanju odgovornosti, če se poročilo uporabi za kakršen koli drug namen ali ga uporabi kdo drug;
- opis meril ali razkritje vira teh meril. Odslej morajo strokovnjaki upoštevati razkritje:
  – vseh pomembnih tolmačenj pri uporabi meril,
  – uporabljene načine merjenja, kadar merila dopuščajo izbiro med več načini merjenja,
  – spremembe v uporabljenih standardnih načinih merjenja;
- izjavo, da je bil revizijski posel izveden v skladu s standardi ISACA za dajanje zagotovil in revidiranja IS ali drugimi veljavnimi strokovnimi standardi. Vsaka neskladnost s temi standardi mora biti v poročilu izrecno navedena;
- nadaljnje pojasnjevalne podrobnosti o spremenljivkah, ki vplivajo na dano zagotovilo, in druge ustrezne informacije;
- ugotovitve, sklepe in priporočila za popravljalne ukrepe skupaj z odzivom poslovodstva nanje. Za vsak odziv poslovodstva morajo strokovnjaki pridobiti informacije o predlaganih ukrepih za izvedbo ali obravnavanje priporočil iz poročila ter njihovo načrtovano izvedbo ali datum veljavnosti ukrepa;
  – odgovorno poslovodstvo se lahko odloči, da sprejme tveganje in ne popravi poročanega stanja zaradi stroškov, zapletenosti popravljalnega ukrepa ali drugih premislekov. Upravni odbor (ali pristojni za upravljanje) bi moral biti obveščen o priporočilih, za katera se je poslovodstvo odločilo sprejeti tveganje, da poročanega stanja ne popravi;
  – če strokovnjaki in revidiranec ne dosežejo soglasja o določenem priporočilu ali pripombi revizije, sta v sporočilih o poslu lahko navedeni obe stališči skupaj z razlogi za nesoglasje. Pisne pripombe revidiranca so lahko vključene kot dodatek poročilu o poslu. Druga možnost pa je, da so stališča revidiranca predstavljena v samem poročilu ali v spremnem pismu. Izvršno vodstvo ali pristojni za upravljanje se morajo nato odločiti, katero stališče podpirajo;
- 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 notranja kontrola 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;
- povzetek opravljenega dela, ki bo predvidenim uporabnikom poročila pomagal bolje razumeti naravo danih zagotovil;
- izraženo mnenje o tem, ali sta bila zasnova in/ali delovanje kontrolnih postopkov za zadevno področje dejavnosti v vseh pomembnih pogledih učinkovita. Kadar strokovnjaki izrazijo mnenje s pridržki, mora biti vključen odstavek z opisom razlogov za pridržke;
- kadar je to primerno, je treba upoštevati sklicevanja na druga ločena poročila, kot so ločeno poročilo o šibkih točkah varnosti, ki so zaščitene pred razkritjem in jih je treba razposlati le omejenemu seznamu prejemnikov;
- datum izdaje poročila o revizijskem poslu. V večini primerov je datum poročila enak datumu izdaje. Priporočeno je omeniti tudi datume, ko je bilo revizijsko delo dejansko izvedeno, če to ni navedeno že v povzetku opravljenega dela;
- imena posameznikov ali organizacije, odgovornih za poročilo, skupaj s krajem izdaje in ustreznimi podpisi.

2401 Poročanje *(nadaljevanje)*

2.2 Zahtevane vsebine poročila o revizijskem poslu (nadaljevanje)

2.2.4 Poročilo o dogovorjenih postopkih naj bi bilo sestavljeno v obliki postopkov in ugotovitev. Poročilo naj vsebuje naslednje sestavine:

- ustrezen in razlikovalen naslov, po katerem se poročilo jasno razlikuje od vseh drugih vrst poročil, ki niso podrejena standardom revidiranja;
- določitev prejemnikov, ki jim je poročilo namenjeno v skladu z določili v revizijski listini ali pismu o poslu;
- določitev odgovorne stranke, vključno z izjavo stranke, ki je zadolžena za obravnavano zadevo;
- izjavo, da je bil revizijski posel izveden v skladu s standardi ISACA za dajanje zagotovil in revidiranja IS ali drugimi veljavnimi strokovnimi standardi. Vsaka neskladnost s temi standardi mora biti v poročilu izrecno omenjena;
- opredelitev obravnavane zadeve (ali pisno trditev v zvezi s tem) in namen revizijskega posla (to je ciljev revizije IS);
- izjavo, da so izvedeni postopki tisti, za katere sta se dogovorili odgovorni stranki, navedeni v poročilu;
- izjavo, da sta za zadostnost postopkov odgovorni izključno le odgovorni stranki, in izjavo o omejitvi odgovornosti glede zadostnosti postopkov;
- seznam izvedenih postopkov (ali sklic nanje);
- opis ugotovitev, vključno z dovolj podrobnostmi o ugotovljenih napakah in izjemah;
- izjavo, da so strokovnjaki izvedli samo dogovorjene postopke in da zato ni izraženo nobeno zagotovilo;
- izjavo, da bi strokovnjaki, če bi izvedli dodatne postopke, utegnili opaziti še druge zadeve in bi o njih poročali;
- izjavo o omejitvi uporabe poročila, ker je namenjeno samo za uporabo določenih strank;
- izjavo, da se poročilo nanaša samo na navedene sestavine in jih ne presega;
- sklice na vsa druga ločena poročila, ki jih je treba upoštevati;
- datum izdaje poročila o revizijskem poslu. V večini primerov je datum poročila enak datumu izdaje. Priporočeno je omeniti tudi datume, ko je bilo revizijsko delo dejansko izvedeno, če to ni navedeno že v povzetku opravljenega dela;
- imena posameznikov ali organizacije, odgovornih za poročilo, skupaj s krajem izdaje in ustreznimi podpisi.

2.2.5 Imamo dve vrsti poročil o preiskovanju:

- **neposredna poročila** – bolj o obravnavani zadevi sami kot o neki trditvi. Poročilo naj se sklicuje samo na zadevo posla in naj ne vsebuje nobenega sklicevanja na trditev poslovodstva o obravnavani zadevi;
- **posredna poročila** – na podlagi trditev poslovodstva o obravnavani zadevi.

Podrobnejša navodila o razliki med posrednim in neposrednim poročanjem lahko najdete v standardu 1007 Trditve.

2.3 Poznejši dogodki

2.3.1 Včasih se po času ali obdobju, v katerem je bila zadeva preizkušena, vendar še pred datumom poročila strokovnjakov, zgodijo dogodki, ki pomembno vplivajo na zadevo in zahtevajo prilagoditev ali razkritje v predstavitvi zadeve ali trditev. Take pojave imenujemo poznejši dogodki. Pri izvajanju revizijskega posla naj strokovnjaki upoštevajo informacije o poznejših dogodkih, s katerimi so seznanjeni. Vendar pa strokovnjaki niso zadolženi za odkrivanje poznejših dogodkov.

2.3.2 Strokovnjaki naj bi povprašali poslovodstvo, ali vedo za kakršne koli poznejše dogodke, ki so se zgodili do datuma poročila strokovnjakov in bi lahko pomembno vplivali na obravnavano zadevo ali trditve.

2.4 Dodatno obveščanje

2.4.1 Strokovnjaki naj bi 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.

2.4.2 Strokovnjaki naj bi pristojnim za upravljanje, in kjer je to primerno, pristojnemu organu sporočili pomembne pomanjkljivosti in bistvene slabosti v kontrolnem okolju. V poročilu naj bi tudi izrecno razkrili, da so jih sporočili.

2.4.3 Strokovnjaki naj bi sporočili poslovodstvu pomanjkljivosti notranjih kontrol, ki so sicer manj pomembne, vendar ne brez posledic. V takih primerih naj bi strokovnjaki obvestili pristojne za upravljanje ali pristojne organe, da so take pomanjkljivosti notranjih kontrol sporočili poslovodstvu.

2.4.4 Strokovnjaki naj bi pridobili pisne izjave poslovodstva, ki potrjujejo vsaj naslednje trditve:

- odgovornost poslovodstva za vzpostavitev in vzdrževanje ustreznih in učinkovitih notranjih kontrol, vključno s sistemi notranjih računovodskih in administrativnih kontrol nad delovanjem pregledovanih dejavnosti in informacijskih sistemov, in aktivnosti za poznavanje vseh zakonov, pravil in predpisov, ki urejajo obravnavano področje pregleda, in za zagotavljanje skladnosti z njimi;

2401 Poročanje *(nadaljevanje)*

2.4 Dodatno obveščanje (nadaljevanje)

2.4.4 *(nadalj.)*

- skupini za posel so bile zagotovljene vse zahtevane informacije, pomembne za cilje posla, kar med drugim vključuje tudi:
  – evidence, s področjem povezane podatke, elektronske datoteke in poročila,
  – usmeritve in postopke,
  – ustrezne zaposlene,
  – izide ustreznih notranjih in zunanjih revizij, pregledov in ocen;
- po koncu dela na terenu se ni zgodil noben dogodek in niso bile odkrite nobene zadeve, ki bi imele pomemben učinek na posel;
- poslovodstvo ne ve za nobene prevare ali domnevne prevare, nepravilnosti in nezakonita dejanja, povezane z obravnavanim področjem pregleda, ki ne bi bile že razkrite, kar velja tudi za vodstvo notranje kontrole in zaposlene, ki so zanjo zadolženi;
- poslovodstvo ne ve, da bi v razgovorih prejelo od zaposlenih, strank, pogodbenih izvajalcev ali drugih kakršne koli prijave prevar ali domnevnih prevar, nepravilnosti in nezakonitih dejanj, ki bi vplivale na pregledovano področje in ne bi bile že razkrite;
- potrditev odgovornosti za zasnovo in uvedbo programov in kontrol za preprečevanje in odkrivanje prevar, nepravilnosti in nezakonitih dejanj.

3. Povezava s standardi in procesi v COBIT 5

3.0 Uvod

To poglavje daje pregled ustreznih:
3.1 Povezav s standardi
3.2 Povezav s procesi v COBIT 5
3.3 Drugih navodil

3.1 Povezava s standardi

V tabeli je pregled:
- najpomembnejših standardov ISACA, ki jih neposredno podpira ta smernica;
- tistih zahtev standardov, ki so najpomembnejše za to smernico.

Opomba: Naštete so samo tiste zahteve standardov, ki so pomembne za to smernico.

Naslov standarda	Pomembne zahteve standarda
1007 Trditve	Strokovnjaki dajanja zagotovil in revidiranja IS morajo pregledati trditve, na podlagi katerih bodo presojali obravnavano zadevo, da bi ugotovili, ali je mogoče takšne trditve revidirati in ali so te trditve zadostne, veljavne in ustrezne.
1205 Dokazi	Strokovnjaki dajanja zagotovil in revidiranja IS morajo pridobiti zadostne in ustrezne dokaze, da lahko sprejmejo primerne sklepe, s katerimi utemeljijo izide posla. Strokovnjaki dajanja zagotovil in revidiranja IS morajo ovrednotiti zadostnost dokazov, pridobljenih za utemeljitev sklepov in doseganje ciljev posla.
1401 Poročanje	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. Strokovnjaki dajanja zagotovil in revidiranja IS morajo zagotoviti, da so ugotovitve v revizijskem poročilu podprte z zadostnimi in ustreznimi revizijskimi dokazi.
1402 Nadaljnja obravnava	Strokovnjaki dajanja zagotovil in revidiranja IS morajo spremljati ustrezne informacije, da lahko sklepajo, ali je poslovodstvo načrtovalo/sprejelo ustrezne in pravočasne ukrepe za obravnavanje poročanih revizijskih ugotovitev in priporočil.

2401 Poročanje *(nadaljevanje)*

3.2 Povezava s procesi v COBIT 5

V tabeli je pregled najpomembnejših:
- procesov v COBIT 5,
- namenov procesov v COBIT 5.

Posebne aktivnosti, ki se izvajajo kot del teh procesov, so v *COBIT 5: Omogočanje procesov*.

Proces v COBIT 5	Namen procesa
EDM05 Zagotovite preglednost deležnikov.	Prepričajte se, da je komunikacija z deležniki uspešna in pravočasna in da je vzpostavljena taka podlaga za poročanje, ki povečuje uspešnost poslovanja, prepozna področja, ki jih je treba izboljšati, in potrjuje, da so cilji in strategije, povezani z IT, v skladu s strategijo podjetja.
MEA01 Spremljajte, vrednotite in ocenjujte uspešnost in skladnost.	Zagotovite preglednost izvajanja in skladnost ter spodbujajte doseganje ciljev.
MEA02 Spremljajte, vrednotite in ocenjujte sistem notranjih kontrol.	Ključnim deležnikom omogočite pregled nad ustreznostjo sistema notranjih kontrol in s tem zagotovite zaupanje v delovanje, vero v doseganje ciljev podjetja in ustrezno razumevanje preostalega tveganja.
MEA03 Spremljajte, vrednotite in ocenjujte skladnost z zunanjimi zahtevami.	Zagotovite, da podjetje ravna v skladu z vsemi veljavnimi zunanjimi zahtevami.

3.3 Druga navodila

Pri izvajanju standardov in smernic naj strokovnjaki po potrebi poiščejo še druga navodila. Za dajanje zagotovil in revidiranje jih lahko pridobijo:
- od kolegov v podjetju,
- od vodstva,
- od organov upravljanja v podjetju, npr. od revizijske komisije,
- od strokovnih organizacij,
- iz drugih strokovnih navodil (npr. knjig, člankov, drugih smernic).

4. Izrazi

Izraz	Pomen
Ustrezen dokaz	Merilo kakovosti dokazov.
Pomanjkljivost brez posledic	Pomanjkljivost je brez posledic, če bi razumna oseba po proučitvi možnosti nadaljnjih neodkritih pomanjkljivosti sklepala, da bi bile te pomanjkljivosti posamično ali združene z drugimi pomanjkljivostmi očitno nepomembne za obravnavano zadevo. Če razumna oseba v zvezi z določeno pomanjkljivostjo ne bi mogla priti do takega sklepa, je taka pomanjkljivost več kot pomanjkljivost brez posledic.
Zadosten dokaz	Merilo količine dokazov; podpira vsa pomembna vprašanja glede cilja in obsega revizije. Glejte dokaze.

5. Datum uveljavitve

5.1 Datum uveljavitve

Ta smernica velja za vse posle dajanja zagotovil in revidiranja IS, ki se začnejo 1. septembra 2014 ali pozneje.

2402 Nadaljnja obravnava

Smernica je predstavljena v naslednjih poglavjih:
1. Namen smernice in povezava s standardi
2. Vsebina smernice
3. Povezava s standardi in procesi v COBIT 5
4. Izrazi
5. Datum uveljavitve

1. Namen smernice in povezava s standardi

1.0 Uvod

V tem poglavju so razjasnjeni:
1.1 Namen smernice
1.2 Povezava s standardi
1.3 Uporaba izrazov ‘revidiranje’ in ‘strokovnjaki’

1.1 Namen

1.1.1 Namen te smernice je dati strokovnjakom dajanja zagotovil in revidiranja IS navodila pri spremljanju, ali je poslovodstvo ustrezno in pravočasno ukrepalo v zvezi s priporočili in ugotovitvami revizije iz poročila.

1.1.2 Strokovnjaki dajanja zagotovil in revidiranja IS naj bi upoštevali to smernico pri odločanju, kako izvajati standard, uporabiti strokovno presojo pri uporabi, utemeljiti vsako odstopanje in po potrebi poiskati dodatna navodila.

1.2 Povezava s standardi

1.2.1 Standard 1401 Poročanje

1.2.2 Standard 1402 Nadaljnja obravnava

1.3 Uporaba izrazov

1.3.1 V nadaljnjem besedilu:
- se ‘dajanje zagotovil in revidiranje IS’ imenuje ‘revidiranje’;
- se ‘strokovnjaki dajanja zagotovil in revidiranja IS’ imenujejo ‘strokovnjaki’.

2. Vsebina smernice

2.0 Uvod

Poglavje o vsebini smernice je sestavljeno tako, da daje informacije o naslednjih ključnih temah posla dajanja zagotovil in revidiranja IS:
2.1 Proces nadaljnje obravnave
2.2 Predlagani ukrepi poslovodstva
2.3 Prevzem tveganja neizvedbe popravljalnih ukrepov
2.4 Postopki nadaljnje obravnave
2.5 Časovni razpored in program nadaljnje obravnave
2.6 Vrsta in obseg nadaljnje obravnave
2.7 Odlaganje nadaljnje obravnave
2.8 Oblika odzivov na nadaljnjo obravnavo
2.9 Nadaljnja obravnava priporočil zunanje revizije s strani strokovnjakov
2.10 Poročanje o nadaljnji obravnavi

2402 Nadaljnja obravnava *(nadaljevanje)*

2.1 Proces nadaljnje obravnave

2.1.1 Nadaljnja obravnava, ki jo izvajajo strokovnjaki, je 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.

2.1.2 Proces nadaljnje obravnave je treba vzpostaviti v podporo dajanju sprejemljivega zagotovila, da vsak pregled, ki so ga opravili strokovnjaki, prinaša podjetju optimalne koristi z zahtevo, da se v skladu z zavezami poslovodstva izvedejo dogovorjeni ukrepi, ki izhajajo iz pregleda, ali da (izvršno) vodstvo prizna in potrdi sprejem tveganj zaradi odlaganja ali neizvajanja predlaganih ukrepov in/ali priporočil.

2.2 Predlagani ukrepi poslovodstva

2.2.1 V okviru razprav z revidirancem naj bi strokovnjaki pridobili njegovo soglasje o izidih revizijskega posla in po potrebi o načrtu ukrepanja za izboljšanje delovanja.

2.2.2 Strokovnjaki naj bi se s poslovodstvom pogovorili o predlaganih ukrepih za izvedbo ali obravnavo priporočil in revizijskih pripomb iz poročila. Te predlagane ukrepe je treba sporočiti strokovnjakom in jih zapisati kot odgovor poslovodstva v končno poročilo z obljubljenim datumom izvedbe in/ali ukrepa.

2.2.3 Če se strokovnjaki in revidiranec dogovorijo za predlagane ukrepe, naj bi strokovnjaki začeli postopke za nadaljnjo obravnavo, kot so podrobno opisani v poglavju 2.4.

2.3 Prevzem tveganja neizvedbe popravljalnih ukrepov

2.3.1 (Izvršno) vodstvo se lahko odloči, da sprejme tveganje in ne popravi poročanega stanja zaradi stroškov, zapletenosti popravljalnega ukrepa ali drugih premislekov. Upravni odbor (ali pristojni za upravljanje) naj bi bili obveščeni o odločitvi (izvršnega) vodstva glede vseh pomembnih opažanj ali priporočil posla, za katera poslovodstvo sprejema tveganje, da poročanega stanja ne popravi.

2.3.2 Kadar strokovnjaki menijo, da je revidiranec sprejel višino preostalega tveganja, ki za podjetje ni ustrezno, morajo zadevo obravnavati z vodstvom dajanja zagotovil in revidiranja IS in z izvršnim vodstvom. Če strokovnjaki še vedno ne soglašajo z odločitvijo glede preostalega tveganja, bi morali hkrati z izvršnim vodstvom zadevo predložiti v reševanje upravnemu odboru (ali pristojnim za upravljanje).

2.3.3 Sprejetje tveganja bi moralo biti dokumentirano; uradno bi ga moralo odobriti izvršno vodstvo, pristojni za upravljanje pa bi morali biti o tem obveščeni.

2.4 Postopki nadaljnje obravnave

2.4.1 Postopki za nadaljnjo obravnavo naj bi bili vzpostavljeni in naj bi vključevali:

- zapis časovnega okvira, v katerem se mora poslovodstvo odzvati na dogovorjena priporočila,
- oceno odgovora poslovodstva,
- preverjanje in potrditev odgovora, če je ustrezen (glej poglavje 2.6),
- nadaljnjo obravnavo, če je primerna,
- postopke za obveščanje ustreznih ravni vodenja in pristojnih za upravljanje o nerešenih vprašanjih in nezadovoljivih odzivih in/ali ukrepih,
- postopke za pridobitev zagotovila poslovodstva, da prevzema s tem povezano tveganje, kadar se popravljalni ukrepi odlagajo ali njihovo izvajanje ni predlagano.

2.4.2 Avtomatiziran sistem sledenja ali podatkovna baza lahko pomaga pri izvajanju nadaljnje obravnave.

2.4.3 Dejavniki, ki jih je treba upoštevati pri določanju ustreznih postopkov nadaljnje obravnave, so:

- pomembnost in vpliv ugotovitev in priporočil,
- vse spremembe v okolju IS, ki utegnejo spremeniti pomembnost in vplivati na ugotovitev in priporočila,
- zapletenosti popravljanja stanja, opisanega v poročilu,
- čas, stroški in napor, ki so potrebni za popravljanje,
- učinek, če ne bi uspeli popraviti stanja, opisanega v poročilu.

2.4.4 Odgovornost za nadaljnjo obravnavo, poročanje in obveščanje višje ravni upravljanja naj bi bili opredeljeni v revizijski listini.

2402 Nadaljnja obravnava *(nadaljevanje)*

2.5 Časovni razpored in program nadaljnje obravnave

2.5.1 Pri rokih nadaljnje obravnave bi bilo treba upoštevati pomembnost ugotovitev iz poročila in njihov učinek, če popravljalni ukrepi niso sprejeti. Čas nadaljnje obravnave v razmerju do prvotnega poročanja je stvar strokovne presoje, odvisne od več premislekov, kot so narava ali velikost s tem povezanih tveganj in stroškov za podjetje.

2.5.2 Ker je nadaljnja obravnava neločljiv sestavni del revizijskega postopka, naj bi bila časovno razporejena hkrati z drugimi koraki, potrebnimi za izvedbo vsakega pregleda. Na določene postopke nadaljnje obravnave ter na čas in trajanje teh aktivnosti lahko vplivajo stopnja težavnosti, tveganje in izpostavljenost, izidi pregleda, potreben čas za izvedbo popravljalnih ukrepov itd., določijo pa se lahko po posvetovanju s poslovodstvom.

2.5.3 Dogovorjene izide v zvezi z zelo tveganimi zadevami bi bilo treba nadalje obravnavati čim prej po datumu, določenem za ukrepanje, in jih nato postopoma spremljati naprej.

2.5.4 Izvajanje vseh odzivov poslovodstva je mogoče redno spremljati (npr. vsako četrtletje) skupaj za različne revizijske posle, čeprav so datumi izvajanja, za katere se je poslovodstvo zavezalo, lahko različni. Drug možen pristop pa je, da se spremljajo posamezni odzivi poslovodstva v skladu z datumi, ko so bili dogovorjeni s poslovodstvom.

2.6 Vrsta in obseg nadaljnje obravnave

2.6.1 Revidirancu bo običajno določen rok, v katerem mora poslovodstvo odgovoriti s podrobnimi podatki o ukrepih, sprejetih za izvedbo priporočil.

2.6.2 Odgovor poslovodstva s podrobnostmi o sprejetih ukrepih je treba ovrednotiti, kar naj, če je le mogoče, opravijo strokovnjaki, ki so izvajali prvotni pregled. Kadar koli je to mogoče, je treba pridobiti tudi revizijske dokaze o izvedenih ukrepih.

2.6.3 Kadar je poslovodstvo dalo informacije o ukrepih, sprejetih za izvedbo priporočil, in strokovnjaki dvomijo v dane informacije ali v uspešnost sprejetega ukrepa, naj izvedejo ustrezne preizkuse ali druge revizijske postopke, da še pred dokončanjem nadaljnje obravnave potrdijo dejanski položaj ali stanje.

2.6.4 Kot del nadaljnje obravnave naj strokovnjaki ocenijo, ali so neizvedena priporočila še vedno aktualna ali celo še pomembnejša. Strokovnjaki lahko odločijo, da izvajanje določenega priporočila ni več ustrezno. To se lahko zgodi, če so se spremenili aplikacijski sistemi, če so bile vpeljane nadomestne kontrole ali če so se poslovni cilji ali prednostne naloge tako spremenili, da je prvotno tveganje uspešno odpravljeno ali bistveno zmanjšano. Na enak način lahko sprememba v okolju IS tako poveča pomembnost učinka nekega prejšnjega opažanja, da ga je treba reševati.

2.6.5 Morda bo treba posel nadaljnje obravnave načrtovati zato, da se preveri in potrdi izvajanje kritičnih in/ali pomembnih ukrepov.

2.6.6 Mnenje strokovnjakov o nezadovoljivih odzivih ali ukrepih poslovodstva je treba sporočiti ustrezni višji ravni vodenja.

2.7 Odlaganje nadaljnje obravnave

2.7.1 Strokovnjaki so zadolženi za pripravo razporeda nadaljnje obravnave v okviru priprave časovnega razporeda dela pri izvedbi posla. Časovni razpored postopkov nadaljnje obravnave je treba pripraviti na podlagi vsebovanega tveganja in izpostavljenosti ter stopnje težavnosti in potrebnega časa za izvedbo popravljalnih ukrepov.

2.7.2 Lahko se tudi zgodi, da strokovnjaki presodijo, 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 preverjanje in potrditev stanja lahko izvede kot del naslednjega posla, ki bo namenjen obravnavi tega sistema ali vprašanja.

2.8 Oblika odzivov na nadaljnjo obravnavo

2.8.1 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. Strokovnjaki lahko sprejmejo tudi ustne odgovore in jih sami zapišejo, te zapise pa naj, če je le mogoče, potrdi še poslovodstvo. Odgovoru je lahko priloženo tudi dokazilo o ukrepanju ali izvajanju priporočil.

2.8.2 Strokovnjaki lahko zahtevajo in/ali prejmejo 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 popravljalnimi ukrepi, ki potrebujejo več časa za dokončanje.

2402 Nadaljnja obravnava *(nadaljevanje)*

2.9 Nadaljnja obravnava priporočil zunanje revizije s strani strokovnjakov

2.9.1 Glede na obseg in pogoje revizijskega posla in v skladu z ustreznimi revizijskimi standardi se zunanji strokovnjaki za nadaljnjo obravnavo dogovorjenih priporočil lahko zanesejo na notranje revizorje. Zadolžitve v zvezi s to nadaljnjo obravnavo se lahko določijo v revizijski listini ali listini o poslu.

2.10 Poročanje o nadaljnji obravnavi

2.10.1 Poročilo o stanju dogovorjenih popravljalnih ukrepov na podlagi poročila o revizijskem poslu, vključno z dogovorjenimi priporočili, ki še niso bila izvedena, je treba predložiti ustrezni ravni vodenja in pristojnim za upravljanje (npr. revizijski komisiji).

2.10.2 Če strokovnjaki med poznejšim revizijskim poslom ugotovijo, da popravljalni ukrep, ki ga je poslovodstvo navedlo kot izvedenega, dejansko ni bil izveden, naj bi to sporočili ustrezni ravni vodenja in pristojnim za upravljanje. Če je to ustrezno, naj bi strokovnjaki pridobili aktualni načrt popravljalnih ukrepov in načrtovani datum izvedbe.

2.10.3 Ko so bili izvedeni vsi dogovorjeni popravljalni ukrepi, se lahko pošlje podrobno poročilo o vseh uvedenih in/ali dokončanih ukrepih izvršnemu vodstvu in pristojnim za upravljanje.

3. Povezava s standardi in procesi v COBIT 5

3.0 Uvod

To poglavje daje pregled ustreznih:
3.1 Povezav s standardi
3.2 Povezav s procesi v COBIT 5
3.3 Drugih navodil

3.1 Povezava s standardi

V tabeli je pregled:
- najpomembnejših standardov ISACA, ki jih neposredno podpira ta smernica;
- tistih zahtev standardov, ki so najpomembnejše za to smernico.

Opomba: Naštete so samo tiste zahteve standardov, ki so pomembne za to smernico.

Naslov standarda	Pomembne zahteve standarda
1401 Poročanje	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. Strokovnjaki dajanja zagotovil in revidiranja IS morajo zagotoviti, da so ugotovitve v revizijskem poročilu podprte z zadostnimi in ustreznimi revizijskimi dokazi.
1402 Nadaljnja obravnava	Strokovnjaki dajanja zagotovil in revidiranja IS morajo spremljati ustrezne informacije, da lahko sklepajo, ali je poslovodstvo načrtovalo/sprejelo ustrezne in pravočasne ukrepe za obravnavanje poročanih revizijskih ugotovitev in priporočil.

2402 Nadaljnja obravnava *(nadaljevanje)*

3.2 Povezava s procesi v COBIT 5

V tabeli je pregled najpomembnejših:
- procesov v COBIT 5,
- namenov procesov v COBIT 5.

Posebne aktivnosti, ki se izvajajo kot del teh procesov, so v *COBIT 5: Omogočanje procesov*.

Proces v COBIT 5	Namen procesa
EDM01 Zagotovite vzpostavitev in vzdrževanje okvira upravljanja.	Zagotovite dosleden pristop, povezan in usklajen z načinom upravljanja podjetja. Da bodo odločitve za IT sprejete v skladu s strategijami in cilji podjetja, zagotovite, da so procesi, povezani z IT, uspešno in pregledno nadzorovani, da je skladnost z zakonskimi in drugimi predpisanimi zahtevami potrjena in da so izpolnjene upravljavske zahteve za člane organa nadzora.
EDM02 Zagotovite izročitev koristi.	Zagotovite optimalno vrednost pobud, storitev in sredstev, ki jih omogoča IT, gospodarno izročitev rešitev in storitev ter zanesljiv in točen prikaz stroškov in verjetnih koristi, tako da so poslovne potrebe uspešno in učinkovito podprte.
EDM03 Zagotovite optimizacijo tveganja.	Zagotovite, da tveganje, povezano z IT v podjetju, ne preseže pripravljenosti za prevzemanje tveganj in sprejemljivega tveganja, da je vpliv tveganje IT na vrednost podjetja prepoznan in obvladovan ter da so možnosti za neskladnost s predpisi čim manjše.
MEA02 Spremljajte, vrednotite in ocenjujte sistem notranjih kontrol.	Ključnim deležnikom omogočite pregled nad ustreznostjo sistema notranjih kontrol in s tem zagotovite zaupanje v delovanje, vero v doseganje ciljev podjetja in ustrezno razumevanje preostalega tveganja.
MEA03 Spremljajte, vrednotite in ocenjujte skladnost z zunanjimi zahtevami.	Zagotovite, da podjetje ravna v skladu z vsemi veljavnimi zunanjimi zahtevami.

3.3 Druga navodila

Pri izvajanju standardov in smernic naj strokovnjaki po potrebi poiščejo še druga navodila. Za dajanje zagotovil in revidiranje jih lahko pridobijo:
- od kolegov v podjetju,
- od vodstva,
- od organov upravljanja v podjetju, npr. od revizijske komisije,
- od strokovnih organizacij,
- iz drugih strokovnih navodil (npr. knjig, člankov, drugih smernic).

4. Izrazi

Izraz	Pomen
Nadaljnja obravnava	Proces, s katerim notranji revizorji ovrednotijo ustreznost, uspešnost, in pravočasnost ukrepov, ki jih je sprejelo poslovodstva na podlagi opažanj in priporočil iz poročila, vključno s tistimi, ki so jih navedli zunanji revizorji in drugi. Vir: Inštitut notranjih revizorjev - Svetovalni napotek 2500.A1-1; Avtorske pravice © ima The Institute of Internal Auditors, Inc. Vse pravice pridržane.
Strokovna presoja	Uporaba ustreznega znanja in izkušenj za ozaveščeno odločanje o ustreznem ukrepanju v okoliščinah posla dejanja zagotovil in revidiranja IS.

5. Datum uveljavitve

5.1 Datum uveljavitve

Ta smernica velja za vse posle dajanja zagotovil in revidiranja IS, ki se začnejo 1. septembra 2014 ali pozneje.

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 ustrezne 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-IS-Assurance-Audit-/Pages/ Reference-Series.aspx* (na voljo v ISACA Bookstore);
- Kolumne o osnovah revidiranja IT v *Journal*-u, IT Audit Basics, *http://www.isaca.org/knowledge-center/itaf-is-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*.

Zapiski/*Notes*:

Obrazec za posredovanje pripomb

(Comment Submission Form)

Zanima nas vaš odziv na ITAF in kakršne koli dopolnitve/spremembe, ki bi jih lahko predlagali. Prosim, zagotovite podrobne informacije o svojem predlogu ter 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 Slovenskega 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 Slovenia Chapter secretary at 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!

Trust in, and value from, information systems

www.isaca.org

© ISACA®, december 2014. Vse pravice pridržane.
Delo je iz angleške različice ISACA® ITAF™: Okvir strokovnega ravnanja za dajanje zagotovil/revidiranje IS, 3. 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