

Revidiranje informacijskih sistemov

ITK₃ UN IS, ITK₃ UN TK

Predavanje 3 od 14

Maribor, 17. oktober 2014

Vsebina tretjega predavanja

- Odprte zadeve predhodnega predavanja
- Kratka ponovitev vsebine drugega predavanja
- Revizija IS - organizacije
- Smisel revizije
- Revizijska dokumentacija
- Za razmislek
- Zaključek / povzetek

- Vprašanje

- **Vprašanje:** Stališče revizije IS do piškotkov?
- Skladnost spletnih mest z ZEKom-1
 - Zakon o elektronskih komunikacijah (ZEKom-1, Uradni list RS, št. 109/2012) od 15. 6. 2013 tudi v Sloveniji uvaja Direktivo o zasebnosti v elektronskih komunikacijah 2002/58/ES, ki je bila spremenjena z Direktivo 136/2009/ES
 - 157. člen zakona govori o piškotkih
- Predlog:
 - Na decembrskih predavanjih bomo eno uro, lahko tudi več, namenili tej temi

- Revizija informacijskih sistemov
- Tipi revizij
- Standardi revidiranja in hierarhija dokumentov
- Za razmislek

Revizija informacijskih sistemov

- Obisk revizorja informacijskih sistemov
- Temelji revizije IS
- Kaj revizija IS je in kaj ni
- Revizor IS

Tipi revizij

- Notranja revizija
- Zunanja revizija
- Zunanje izvajanje notranje revizije

Standardi revidiranja in hierarhija dokumentov

- Struktura in razmerja
- Hierarhija pravil
- Poklicna etika
- Struktura in uporaba standardov

Za razmislek

- Hierarhijo pravil
- Oba kodeksa etike

- Ali so kakšna vprašanja vezana na drugo predavanje?
- Ali so kakšne nejasnosti?
- Ali ste uspeli na UM Moodle predmeta Revidiranje IS (9371):
 - Pregledati / prenesti drugo predavanje?
 - Pregledati / prenesti tretje – to predavanje?

Revizija IS - organizacije

- V Sloveniji
- V tujini
- ISACA slovenski odsek



Slovenski inštitut za revizijo

Dunajska 106,

1000 Ljubljana

www.si-revizija.si

- ustanovljen 11. januarja 1994
- podlaga za njegovo ustanovitev Zakon o revidiranju , VII.1993
- član pomembnih mednarodnih organizacij:
 - Mednarodno združenje računovodskih strokovnjakov (International Federation of Accountants, IFAC);
 - Zveza evropskih revizorjev (Federation des Experts Comptables Europeens, FEE);
 - vet za mednarodne standarde ocenjevanja vrednosti (International Valuation Standards Committee, IVSC).



- 7 sekcij:
 - Revizorji;
 - Računovodje;
 - Revizorji IS;
 - Finančniki;
 - Ocenjevalci vrednosti;
 - Notranji revizorji;
 - Davčniki.



- Preizkušeni revizorji informacijskih sistemov:
 - Odbor sekcije
 - Seznam aktivnih preizkušenih revizorjev informacijskih sistemov (43 aktivnih PRIS)
 - Register vseh preizkušenih revizorjev informacijskih sistemov (105 PRIS)
 - Obvestila sekcije
 - Pravila stroke
 - *Vsak prvi torek v mesecu ob 16.30 predavanja.*



- Preizkušeni revizorji informacijskih sistemov:
 - v okviru inštituta deluje tudi



- podrobnosti o ISACA v nadaljevanju
- *Vsak prvi torek v mesecu ob 16.30 predavanja.*



Agencija za javni nadzor nad revidiranjem
Glinška 3
1000 Ljubljana
www.anr.si

- z delovanjem pričela 1.3.2009.
- pristojnosti in odgovornosti so:
 - sprejemanjem pravil revidiranja (standardov revidiranja, etičnih poklicnih standardov, standardov obvladovanja revidiranja) in določanjem hierarhije pravil revidiranja, ki niso predpisi;
 - izobraževanjem za pridobitev naziva pooblaščen revizor;
 - izdajo dovoljenj za opravljanje dejavnosti revidiranja in nalog pooblaščenega revizorja ter registracijo zakonitih revizorjev in revizijskih družb tretjih držav;
 - stalnim izobraževanjem pooblaščenih revizorjev;
 - zagotavljanjem kakovosti revizijskega dela pooblaščenih revizorjev in revizijskih družb.



Računsko sodišče Republike Slovenije
Slovenska cesta 50
1000 Ljubljana
www.rs-rs.si

- Računsko sodišče lahko revidira pravilnost in smotrnost poslovanja, revidira pa lahko akt o poslovanju v preteklem letu kakor tudi akt o načrtovanem poslovanju uporabnika javnih sredstev. Uporabnik javnih sredstev po zakonu o računskem sodišču je:
 - pravna oseba javnega prava ali njene enote;
 - pravna oseba zasebnega prava, če
 - je prejela pomoč iz proračuna Evropske unije, državnega proračuna ali proračuna lokalne skupnosti;
 - je koncesionar;
 - je gospodarska družba, banka ali zavarovalnica, v kateri imata država in lokalna skupnost večinski delež;



Računsko sodišče Republike Slovenije

- Uporabnik javnih sredstev po zakonu o računskem sodišču je:
 - fizična oseba, če zanjo velja,
 - da je prejela pomoč iz proračuna Evropske unije, državnega proračuna ali proračuna lokalne skupnosti ali,
 - da izvaja javno službo ali zagotavlja javne dobrine na podlagi koncesije.

Računsko sodišče Republike Slovenije / št. revizij v teku: 90

REVIZIJA	FAZA REVIZIJE			POROČILO
	SKLEP	OSNUTEK	PREDLOG	
Financiranje volilne kampanje za volitve poslancev iz Republike Slovenije v Evropski parlament v letu 2014 pri organizatorju volilne kampanje: Društvo za uveljavljanje pravne in socialne države VERJAMEM	X			
Financiranje volilne kampanje za volitve poslancev iz Republike Slovenije v Evropski parlament v letu 2014 pri organizatorju volilne kampanje: Socialni demokrati	X			
Financiranje volilne kampanje za volitve poslancev iz Republike Slovenije v Evropski parlament v letu 2014 pri organizatorju volilne kampanje: Piratska stranka Slovenije	X			
Financiranje volilne kampanje za volitve poslancev iz Republike Slovenije v Evropski parlament v letu 2014 pri organizatorju volilne kampanje: Nova Slovenija – Krščanski demokrati	X			
Dodeljevanje tekočih transferov v letu 2012 v Občini Jezersko			X	
Pravilnost poslovanja Pokrajinskega muzeja Ptuj Ormož v letu 2013			X	
Nenujni reševalni prevozi			X	



ISACA (*Information System Audit and Control Association*)

3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008 USA

www.isaca.org

- 1969: ustanovljeno kot EDPAA (*Electronic Data Processing Audit Association*)
- 1993: preimenovano v ISACA
- 2006: spremenjen logo, ime ostaja
- danes vključuje več kot 110.000 članov po svetu
- v več kot 80 državah
- v več kot 200 odsekih



Poslanstvo:

- Neprofitno, neodvisno člansko združenje ISACA je vodilni globalni ponudnik znanja, certifikacij, skupnosti, zagovorništva in izobraževanja o zagotavljanju, nadzoru in varnosti informacijskih sistemov, vodenju IT v podjetjih, ter z IT povezanih tveganjih in skladnostjo.

ISACA pomaga svojim članom in njihovim delodajalcem zagotoviti zaupanje v informacijske sisteme in korist od njih.



Aktivnosti:

- Razvija in upravlja 4 vodilne certifikacije
- Sponzorira in izvaja tehnično podporo za konference in izobraževanja na 5 kontinentih
- Razvija in posodablja
 - COBIT
 - Val IT
 - Risk IT
 - IT Assurance Framework (ITAF)
 - Business Model for Information Security (BMIS)
- Izdaja: ISACA Journal (6 izvodov letno)

Nazivi (certifikacije):

- CISA – *Certified Information System Auditor*
 - od 1978, več kot 103.000 podeljenimi nazivi (111 v SVN)
- CISM – *Certified Information System Manager*
 - od 2002, več kot 22.500 podeljenimi nazivi (37 v SVN)
- CGEIT – *Certified in the Governance of Enterprise IT*
 - od 2007, več kot 5.600 podeljenimi nazivi (15 v SVN)
- CRISC – *Certified in Risk and Information System Control*
 - od 2010, več kot 16.800 podeljenimi nazivi (9 v SVN)



Tipi članstva:

- Profesionalno;
- Študentsko;
- Akademsko.



The screenshot shows the ISACA eLibrary website interface. At the top, there is a navigation bar with various links like OWASP, STA, Gartner, etc. Below that is the ISACA eLibrary logo and a search bar. The main content area is titled "Most Recently Read Titles" and lists several books with their covers, titles, authors, and access dates. A sidebar on the left contains "Personal Folders" and "System Folders". A sidebar on the right is titled "Browse Topics" and lists various categories like Access Control, Business Continuity Management, etc.

Most Recently Read Titles

- Complete Guide to Security and Privacy Metrics: Measuring Regulatory Compliance, Operational Resilience, and ROI** by Debra S. Herrmann Auerbach Publications © 2007
Accessed 38 days ago
- IT Security Metrics: A Practical Framework for Measuring Security & Protecting Data** by Lance Hayden McGraw-Hill/Osborne © 2010
Accessed 38 days ago
- Computer Fraud Casebook: The Bytes that Bite** by Joseph T. Wells (ed) John Wiley & Sons © 2009
Accessed 42 days ago
- Oracle Data Guard 11g Handbook** by Larry Carpenter et al. Oracle Press © 2009
Accessed 42 days ago
- IT Auditing: Using Controls to Protect Information Assets, Second Edition** by Chris Davis, Mike Schiller and Kevin Wheeler McGraw-Hill/Osborne © 2011
Accessed 67 days ago
- IT Standards and Summaries of Guidelines and Tools and Techniques for Audit and Assurance and Control Professionals** by ISACA ISACA © 2010
Accessed 67 days ago
- Linux: Security, Audit and Control Features** by K.K. Mookhey, Nilesh Burghate and ISACA ISACA © 2005
Accessed 214 days ago

Browse Topics

- Access Control
- Business Continuity Management
- Business Topics
- CGEIT Exam Study Aids
- Change Management
- CISA Exam Study Aids
- CISM Exam Study Aids
- COBIT
- Compliance
- CRISC Exam Study Aids
- Information Security
- IT Auditing
- IT Governance
- ITAF
- Knowledge Management
- Non-English
- Outsourcing
- Policies & Procedures
- Privacy
- Project Management
- Risk
- Technology
- Val IT





IT Governance institute
3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008 USA
www.itgi.org

- ustanovljen leta 1998 (ISACA)
- obvladovanje in vodenje informacijske in sorodne tehnologije v podjetju
- razvoj za COBIT (*Control Objectives for Information and related Technology*) - Kontrolni cilji za informacijsko in sorodno tehnologijo (več na prihodnjih predavanjih)



www.isaca.si

deluje v okviru Slovenskega inštituta za revizijo



The screenshot shows the website of the ISACA Slovenian branch. The header features the ISACA logo and the text 'Zaupanje v informacijske sisteme in korist od njih' and 'Slovenski odsek'. Below the header is a navigation menu with links: Dobrodošli, O odseku, Člani, Izobraževanje, Nazivi, Revizija IS, and Pišite nam. The main content area is titled 'Pozdravljeni na spletnih straneh Slovenskega odseka ISACA' and includes a welcome message and a list of services. There are also several award logos and a section for free training.

ISACA®
Zaupanje v informacijske sisteme in korist od njih
Slovenski odsek

Dobrodošli O odseku Člani Izobraževanje Nazivi Revizija IS Pišite nam

Pozdravljeni na spletnih straneh Slovenskega odseka ISACA®

Spletne strani bi želeli narediti še privlačnejše, še bolj zanimive. Vabimo vas, da sodelujete [s svojimi željami, pripombami in predlogi!](#) [Uporabljene blagovne znamke ...](#)

Slovenski odsek ISACA
Dunajska cesta 106
SI-1000 Ljubljana, Slovenija
Tel.: 01 568 55 54
Faks: 01 568 63 32
e-pošta: info@isaca.si

Brezplačna izobraževanja

4. novembra bo Tomaž Aljaž predstavil Teorijo omejitev (2 CPE). [Več ...](#)

Obveščamo, napovedujemo ...

Novica! Vse, ki vas zanima revidiranje IS vabimo, da se v **četrtek, 16. oktobra ob 18.30**, udeležite brezplačnega webinarja **CISA Booster Course: Where Theory is put into practice (3 CPE)**. Webinar organizira **Chapter ISACA** odsek v ustanavljanju, mesto za člane ISACA, ki niso vključeni v lokalne odseke. Izvedla ga bo mag. Jutta Edith Zilian, CISA, CISM, s katero smo že sodelovali pri izvedbi spletnih pripravilnih seminarjev in CISM Booster webinarja. Webinar je tudi odlična priložnost za dodatno pripravo na prihajajoči CISA izpit. [Vabljeni, da se nam pridružite!](#)

Oktober je evropski mesec varnosti v internetu (cybersecurity)! Agencija Evropske unije za omrežno in informacijsko varnost **ENISA** in **partnerji**, med katerimi je tudi **ISACA®**, posebej s svojim programom **Cybersecurity Nexus CSXTM**, s 1. oktobrom 2014 uradno začnejo **Evropski mesec kibervarnosti (ECISM)**. Cilj vseevropske kampanje je spodbuditi ozaveščenost o kibernetiki varnosti med državljani ter zagotoviti najnoveše informacije z izobraževanjem, dobrimi praksami in tekmovanji. Slovenija bo sodelovala z nacionalnim programom ozaveščanja **Varni na internetu**, ki

POZOR! Spremljajte nas na:  

ISACA®



Članstvo:

- 150 članov, od tega 28 članic; 3 akademski zagovorniki, 130 z univerzitetno ali višjo izobrazbo, 111 z več kot 14 let delovnih izkušenj
- 19 s platinasta (prek 15 let), 41 zlata (10-14 let), 49 srebrna (5-9 let) in 21 bronasta raven članstva,
- 126 z nazivi (84%).



Kaj delamo (1):

- vzdržujemo spletno stran (lani prenovili vsebino , obliko usklajujemo z ISACA predlogo);
- izdajamo – pošiljamo Mesečnik in Obvestila (~2x/mesec) na 420 e-naslovov (vsakomur, ki to želi);
- organiziramo mesečne izobraževalne dogodke (9/leto):
 - 6 v 2013, povprečno 43,5 udeležencev (37 članov),
 - 9 v 2012, povprečno 39,1 udeležencev, od tega 31,6 članov.



Kaj delamo (2):

- tesno sodelujemo s Slovenskim inštitutom za revizijo – sekcijo PRIS:
 - skupaj smo izdali Hierarhijo pravil za revidiranje IS (objavljeno v Uradnem listu)
- organiziramo letno konferenco o reviziji in nadzoru IS, letos že 21.
 - teme: COBIT 5, operativna tveganja, kraje in zlorabe, varovanje informacij – ISO2700x, upravljanje incidentov, upravljanje sprememb, zagotavljanje kakovosti pri razvoju, testiranju in implementaciji, standardi, smernice, dobre prakse pri vodenju IS, metodologija revidiranja IS (praktični primeri), notranje revidiranje -vloga, standardi, dobre prakse);
- organiziramo pripravljalne seminarje CISA, CISM, CRISC in CGEIT



Kaj delamo (3):

- prevedli smo COBIT 4.1, ISACA standarde & smernice, zdaj prevajamo nove standarde...;
- prevedli smo ISACA pojmovnik, želeli bi ga objaviti kot del obstoječega slovenskega e-slovarja informatike (www.islovar.org);
- praktična uporaba ISACA standardov & smernic (revizijska mapa; s sekcijo PRIS);
- manjše iniciative (stiki z regulatorji, stroko...).

Načrti za prihodnje:

Nadaljevanje realizacije programa

- Prevodi;
- Sodelovanje z univerzami in fakultetami;
- Promocija stroke, ISACA in njenih izdelkov;
- Sodelovanje s sorodnimi organizacijami;
- Obveščanje članov.



Smisel revizije

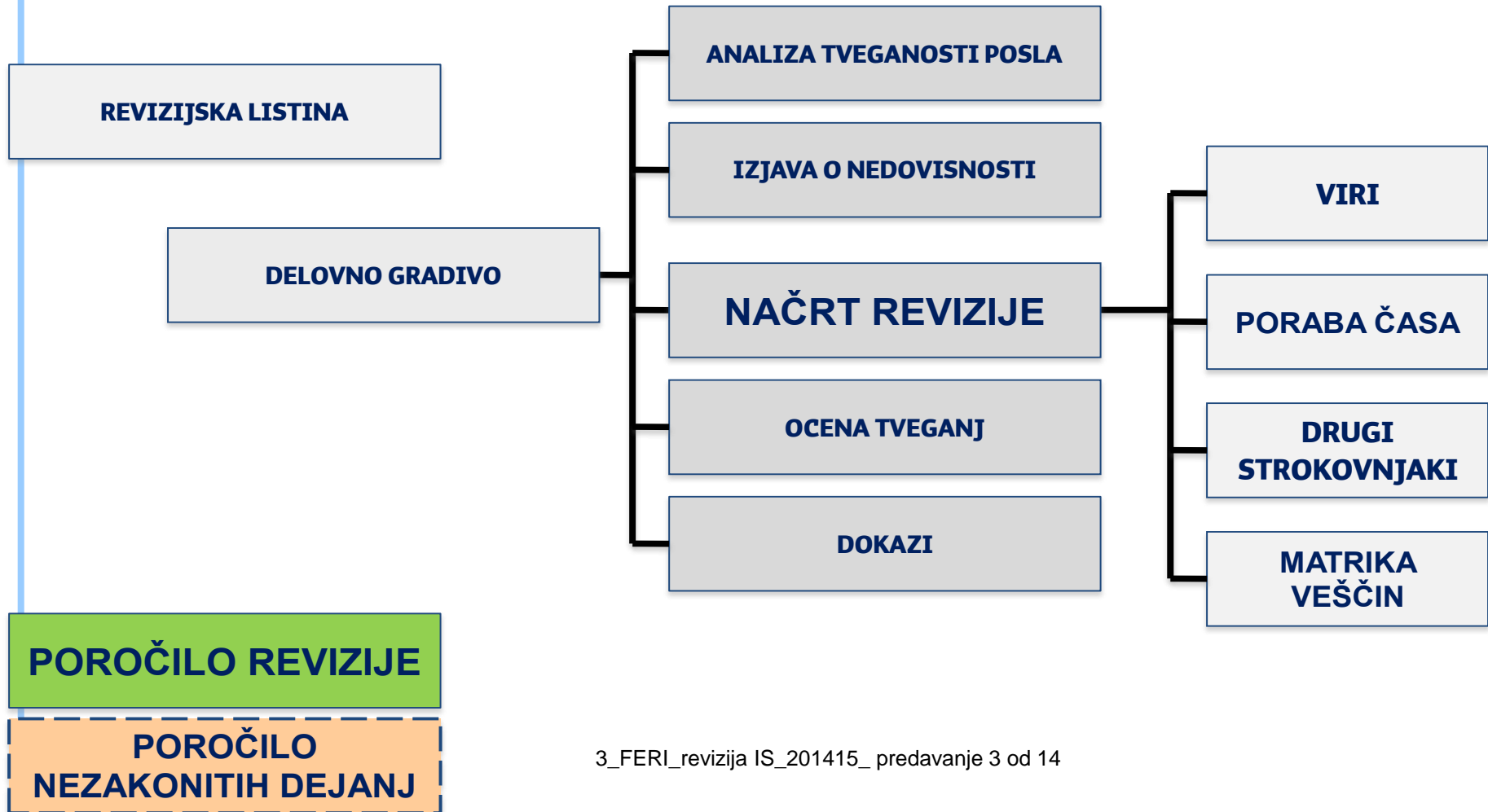
- Kdo je zainteresiran za revizijo IS?

<http://www.youtube.com/watch?v=I6HIJ1-FcdM>

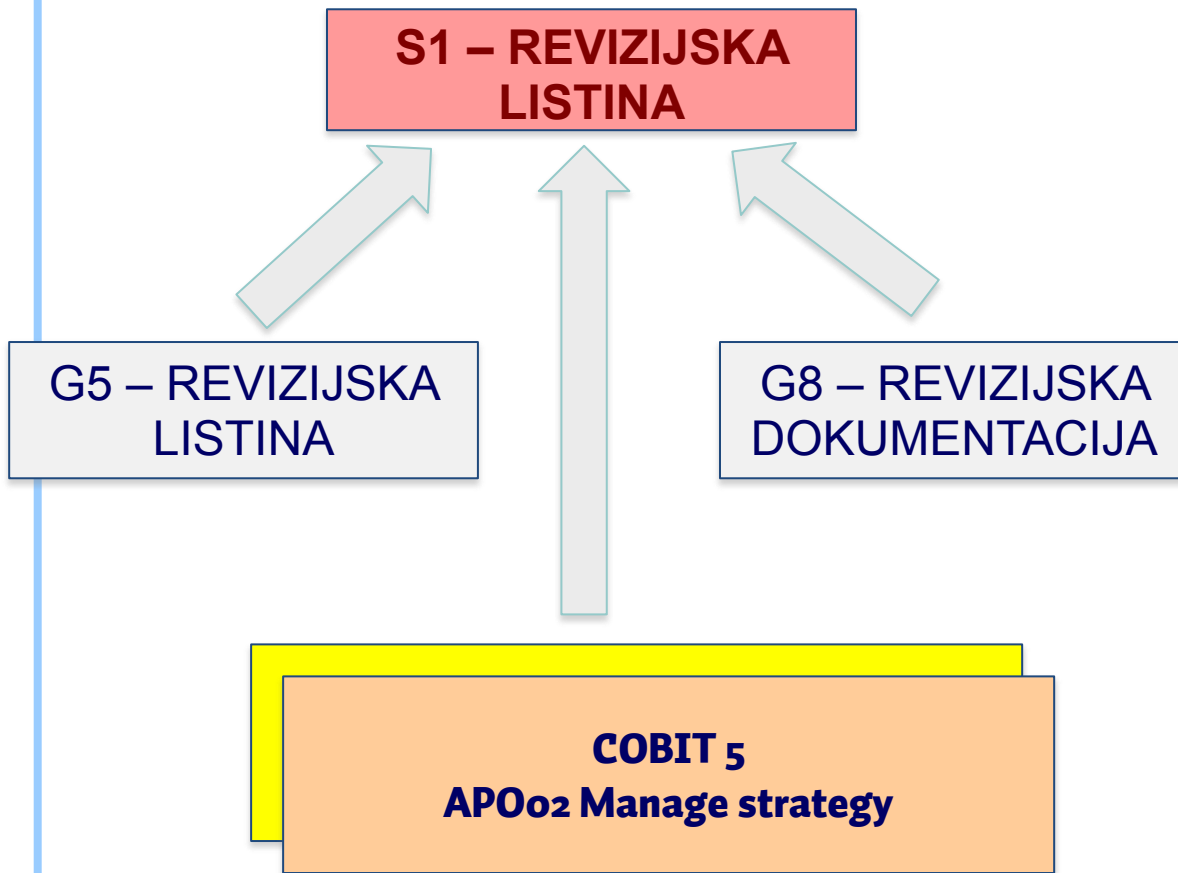
Smisel revizije

- Podjetja so vse bolj odvisna od delovanja IKT.
- Zagotavljanje nemotenega delovanja IKT je zelo zahtevna naloga.
- Kdo daje zagotovilo, da IKT deluje?
- Kdo potrebuje zagotovilo, da IKT deluje?

Revizijska dokumentacija



Revizijska dokumentacija



ITAF - SLO (2
izdaja)

Ta razmislek / do naslednjč

- Pregledati
 - www strani organizacij
 - ITAF - 1001
- Razmisliti
- Pripraviti vprašanja za diskusijo

Zaključek / povzetek

Pridobili ste informacije o:

- Revizija IS – organizacije;
 - V Sloveniji, v tujini, ISACA odsek
- Smisel revizije
- Revizijska dokumentacija
 - Vrste poslov
 - Revizijska listina
 - ITAF
- Za razmislek / do naslednjič

Za konec

- Pripombe
- Komentarji
- Predlogi