

Revizija IS

Nepotrebna obremenitev ali
dobrodošla pomoč
informatiki?

Uroš Žust, CISA, CISM,

Preizkušeni revizor informacijskih sistemov

Deloitte Slovenia, Manager, Oddelek poslovnega svetovanja



Revizija IS - ključne organizacije

- **Slovenski inštitut za revizijo** - opravlja naloge in pristojnosti na področju revidiranja in drugih strokovnih področjih, povezanih z revidiranjem
 - **Sekcija revizorjev informacijskih sistemov** - skrbi za sprotno dopolnjevanje Hierarhije pravil revidiranja informacijskih sistemov, sprejem pravil revidiranja informacijskih sistemov (stališč, pojasnil) ter za vključenost v oblikovanje zakonodaje za področje delovanja preizkušenih revizorjev informacijskih sistemov.
- **ISACA** - neprofitno, neodvisno člansko združenje, vodilni globalni ponudnik znanja, certifikacij in izobraževanja o zagotavljanju, nadzoru in varnosti informacijskih sistemov, vodenju IT v podjetjih, ter z IT povezanih tveganjih in skladnosti:



Pravila stroke

Prva raven

- a) Zakon o revidiranju (UL, 65/08)
- b) Zakoni, ki urejajo revidiranje informacijskih sistemov, in predpisi, izdani na njihovi podlagi
- c) Mednarodni standardi za strokovnjake revidiranja, kontrol in dajanja zagotovil na področju IT
- d) Kodeks poklicne etike preizkušenega revizorja informacijskih sistemov



Druga raven

- a) Mednarodne smernice za strokovnjake revidiranja, kontrol in dajanja zagotovil na področju IT
- b) Mednarodna orodja in tehnike za strokovnjake revidiranja, kontrol in dajanja zagotovil na področju IT
- c) pojasnila Strokovnega sveta Inštituta
- d) navodila sveta Inštituta

Tretja raven

- a) metodološka gradiva Inštituta in priročniki Inštituta
- b) strokovna literatura in objavljeni strokovni prispevki (doma in v tujini)
- c) splošno sprejeta načela revidiranja informacijskih sistemov v tuji praksi



Vrste storitev na področju revizije IS

- revizija
- pregled
- dogovorjeni postopki



Znanja informatika in revizorja IS

Znanja informatika

- Tehnično visoko znanje s področja IT okolja
- Podrobno poznavanje IT okolja organizacije v kateri je zaposlen
- Kontinuiran pristop
- Dnevne izkušnje z delovanjem IT sistemov in okolja
- Poznavanje problemov IT okolja v družbi

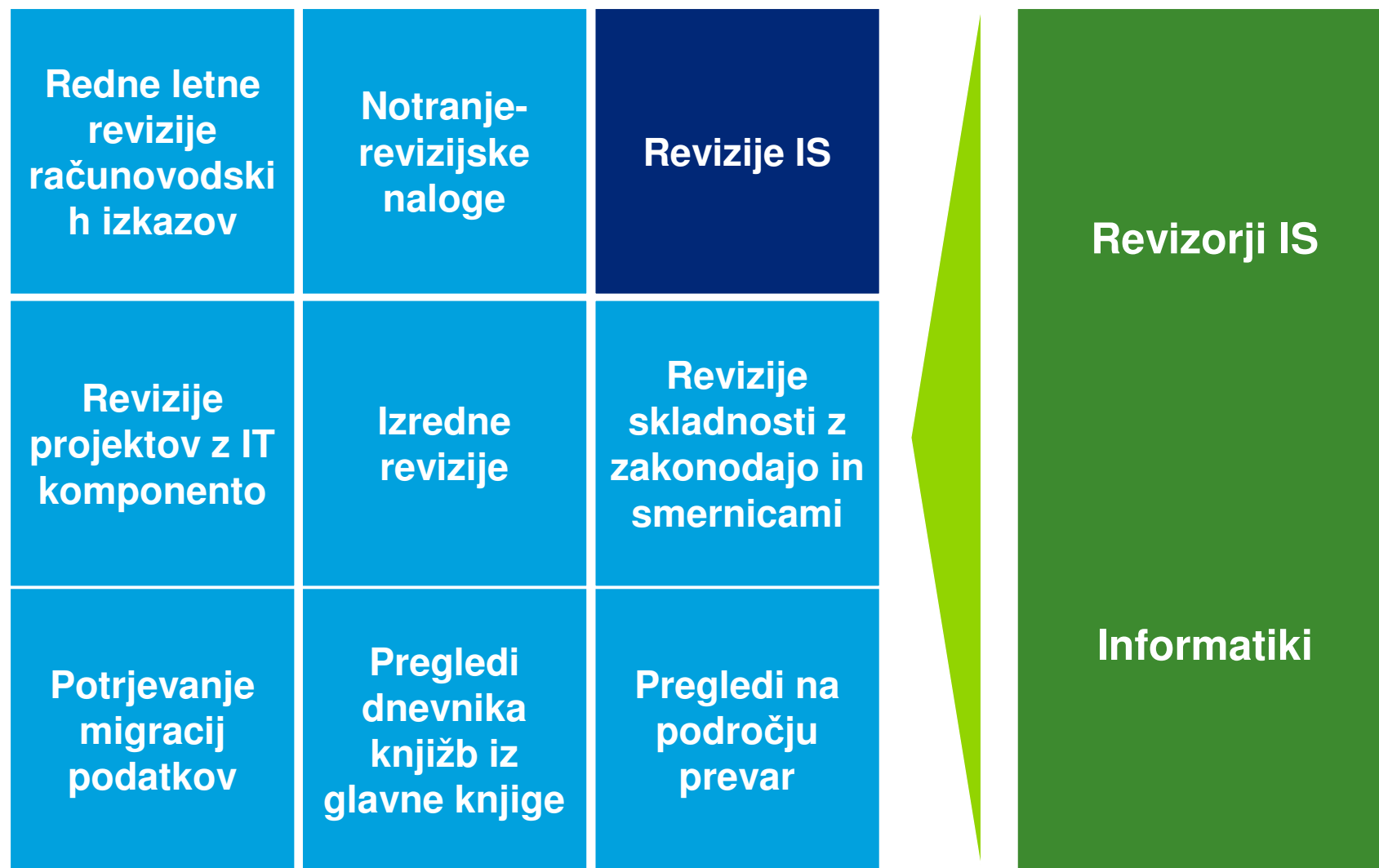
Znanja revizorja informacijskih sistemov

- Nižja splošna tehnična specializacija
- Splošno poznavanje okolja organizacije
- Posamični namenski pregledi
- Večja širina poznavanja praks iz naslova izkušenj z različnimi okolji
- Poznavanje tipičnih problemov IT okolij

Ključne razlike v vlogi in pristopu

	Informatik	Revizor informacijskih sistemov
Lokacija	Notranji strokovnjak	Zunanji strokovnjak
Vloga	Aktivno sodeluje pri vzpostavitvi IT okolja	Neodvisen pri vzpostavitvi IT okolja
Naloge	Izvajanje procesov, včasih tudi svetovanje in usmerjanje	Presoja in dajanje zagotovil, včasih tudi svetovanje in usmerjanje
Poročanje	Izobraževanje posloводства in uporabnikov	Informiranje posloводства
Pristop	Kontinuiran pristop	Posamični (samostojni) pregledi
Tveganja	Zmanjševanje in upravljanje tveganj	Izpostavljanje tveganj
Fokus	Delovanje in zagotovljena podpora poslovnim procesom je ključni vidik	Varnost je ključni vidik, fokus so kontrole

Področja pogostega sodelovanja revizorjev IS z informatiki



Pogosta percepcija

Welcome to Q&A for system administrators and desktop support professionals — check out the [FAQ!](#)

StackExchange v

[log in](#) | [careers](#) | [blog](#) | [meta](#) | [about](#) | [faq](#)

search



serverfault

Questions

Tags

Users

Badges

Unanswered

Ask Question

Our security auditor is an idiot, how do I give him the information he wants?

CAREERS 2.0
by stackoverflow



+



Read anything good lately?
Add favorite books to your profile!

Greetings!

This is a collaboratively edited question and answer site for **system administrators and desktop support professionals**. It's 100% free, no registration required.

Got a question about the site itself? [meta](#) is the place to talk about things like what questions are appropriate, what tags we should use, etc.

[about](#) » [faq](#) » [meta](#) »

tagged

[security](#) × 2595

[security-policy](#) × 83

asked 4 months ago

viewed 186,456 times

963



1010

A security auditor for our servers has demanded the following within two weeks:

- A list of current usernames and plain-text passwords for all user accounts on all servers
- A list of all password changes for the past six months, again in plain-text
- A list of "every file added to the server from remote devices" in the past six months
- The public and private keys of any SSH keys
- An email sent to him every time a user changes their password, containing the plain text password



We're running Red Hat Linux 5/6 and CentOS 5 boxes with LDAP authentication.



As far as I'm aware, everything on that list is ether impossible or incredibly difficult to get, but if I don't provide this information we lose access to our payments platform, and any income we might have got while we move away. Any suggestions for how I can solve or fake this information?

The only way I can think to get all the plain text passwords, is to get everyone to reset their password and make a note of what they set it to. That doesn't solve the problem of the past six months of password changes, because I can't retroactively log that sort of stuff, the same goes for logging all the remote files.

Getting the public and private parts of the SSH keys is possible, but annoying as we have a few users with a few computers, all with their own SSH keys. Unless I've missed an easier way to do that?

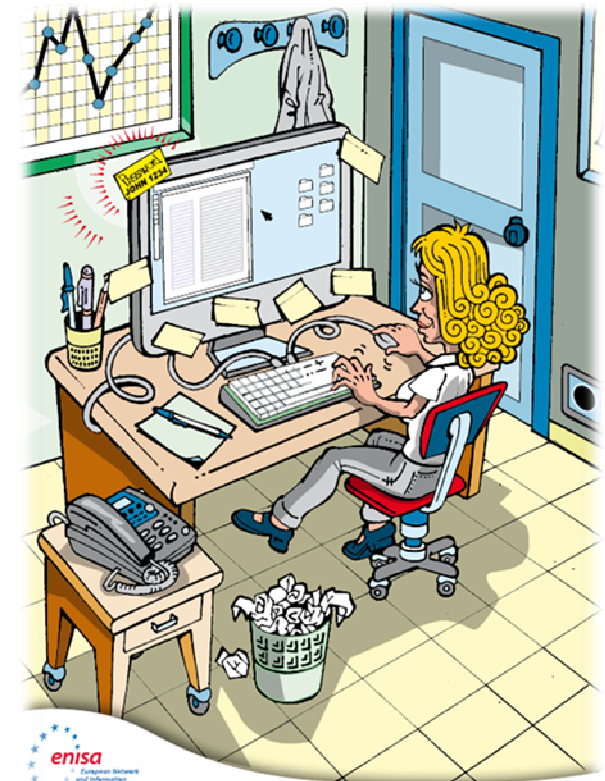
Prepletenost odnosov

Izzivi:

- Vpliv zaznanih tveganj na percepcijo posloводства
- Neustrezna komunikacija revizorjev IS in informatikov
- Neustrezna komunikacija revizorjev IS in posloводства
- Zahteve revizorjev IS
- „Motnje“ v delu informatike

Prednosti:

- Neodvisna ocena informacijskega sistema
- Zaznana tveganja kot posledica revizije IS
- Izboljšanje kontrolnega okolja
- Prenos znanj, izkušenj, pogledov in mnenj
- Komunikacija revizorjev IS in posloводства



Priporočila za „lažje“ življenje

- Sodelovanje z revizorji
- Natančen dogovor o načrtovanih postopkih
- Dokumentiranje vseh aktivnosti
- Zaupanje in obenem preverjanje
- Izmenjava znanj in mnenj



Dobre prakse

- Poslovodstvo naj informatike natančno seznani s cilji in obsegom revizijske naloge;
- Revizor informacijskih sistemov naj informatike natančno seznani s postopki, ki jih namerava opraviti;
- Informatiki in revizor informacijskih sistemov naj skupaj presodijo morebitna tveganja, ki iz načrtovanih postopkov izhajajo in jih po potrebi prilagodijo;
- Informatiki naj revizorja informacijskih sistemov opozorijo na morebitne dodatne skrbi, povezane z izvajanje revizijskih nalog in zbiranjem revizijskih dokazov;
- Informatiki naj revizorja informacijskih sistemov po potrebi posebej opozorijo na problematična področja, če so le ta zanemarjena s strani odgovornih v podjetju.
- Izmenjava mnenje in izkušenj

Vprašanja?

Hvala za vašo pozornost!

Uroš Žust, CISA, CISM

Preizkušeni revizor informacijskih sistemov

Manager | Business Advisory Services

Deloitte d.o.o. | Dunajska cesta 165, 1000 Ljubljana, Slovenia

Tel: +386 1 3072836 | Fax: +386 1 3072900 | Mobile: +386 31 337086

uzust@deloitteCE.com | www.deloitte.si | www.facebook.com/DeloitteSlovenija





Ime Deloitte se nanaša na Deloitte Touche Tohmatsu Limited, pravno osebo, ustanovljeno v skladu z zakonodajo Združenega kraljestva Velike Britanije in Severne Irske (v izvirniku »UK private company limited by guarantee«), in mrežo njenih članic, od katerih je vsaka ločena in samostojna pravna oseba.

Podroben opis pravne organiziranosti združenja Deloitte Touche Tohmatsu Limited in njenih družb članic je na voljo na www.deloitte.com/si/nasa-druzba.

Deloitte opravlja storitve revizije, davčnega svetovanja, poslovnega svetovanja in finančnega svetovanja za javne in zasebne družbe iz različnih gospodarskih panog. Z globalno povezanim omrežjem družb članic v več kot 150 državah Deloitte ponuja prvovrstne zmogljivosti in izjemno kakovostne storitve ter strankam omogoča vpogled v kompleksne izzive, s katerimi se soočajo pri svojem poslovanju. Deloitte ima približno 200.000 strokovnjakov, zavezanih k zagotavljanju odličnosti.