SIR IUS 5/13

SLOVENSKI INŠTITUT za REVIZIJO

Revija za teorijo in prakso revizije, računovodstva, davkov, financ, ocenjevanja vrednosti in drugih sorodnih področij

Renato Burazer

Izzivi pri revidiranju testiranja programske opreme

Challenges of software testing audit

POVZETEK ● *Testiranje programske opreme predstavlja ključni korak pri preverjanju skladnosti uporabniških zahtev z dejanskim stanjem razvite programske opreme. V prispevku so predstavljene glavne dileme pri testiranju in pristop k revidiranju testiranja. Poskušali bomo odgovoriti na vprašanje, kdaj je testiranja dovolj in kje je meja med nalogami in zadolžitvami uporabnikov in programerjev, ki jo mora revizor informacijskih sistemov upoštevati pri načrtovanju revidiranja testiranja.*

Ključne besede ● *revidiranje testiranja programske opreme, stresni test, testne specifikacije, funkcionalno testiranje, varnostno testiranje, funkcionalne specifikacije, integracijsko testiranje*

SUMMARY ● *Software testing represents the key step in verifying compliance of a developed software application with user specifications. This article introduces key challenges related to software application testing and the approach for auditing the testing of software. We will try to answer when testing is sufficient and where the border is between the responsibilities of end users and programmers that IT Auditor needs to take into account when planning the audit of software testing.*

Key words ● *Software testing audit, stress test, test specifications, functional testing, integration testing*

JEL: M42

Peter Grasselli, Jožica Kržič

Priprava načrta ocenjevanja skladnosti delovanja informacijskih sistemov na osnovi COBIT®5

How to prepare COBIT®5 based information system compliance audit plan

POVZETEK ● *Revizorji informacijskih sistemov se dostikrat znajdemo pred nalogo, ko je treba oceniti skladnost delovanja informacijskega sistema družbe glede na zakonske zahteve ali zahteve nadzornih institucij. Za vsak revizijski*

posel je treba v skladu s Hierarhijo pravil revidiranja informacijskih sistemov pripraviti revizijski načrt, katerega pomemben del je opredelitev obsega postopkov, potrebnih za izvedbo pregleda. Preslikava zakonodajnih zahtev v procese COBIT 5 olajša in pospeši razvoj načrta ter pripomore k njegovi usklajenosti z Okvirom dajanja zagotovil IT združenja ISACA.

V prispevku so opisana izhodišča in metodologija preslikave zahtev predpisov v procese COBIT 5. Postopek preslikave vključuje vsebinske zahteve in zahteve, ki se nanašajo na zrelost poslovanja. Izvedena je preslikava Sklepa o upravljanju tveganj in izvajanju procesa ocenjevanja ustreznega notranjega kapitala za banke in hranilnice v kontrolne cilje COBIT 5. Rezultati preslikave so osnova za pripravo načrta pregleda, zasnovanega na COBIT 5. Tako pripravljen načrt je vodilo, ki revizorju informacijskih sistemov pomaga pri obvladovanju revizijskega tveganja in obsega pregleda v kombinaciji z oceno tveganja.

Pričakovanje, da bo sama preslikava zožila obseg pregleda, se ni uresničilo. Zahteve sklepa s področja upravljanja in vodenja IT se preslikajo v vse procese COBIT 5, razen enega, ter na večino praks upravljanja in vodenja IT.

Ključne besede ● *COBIT 5, preslikava, revizijski načrt, skladnost, zakonodaja*

SUMMARY ● *It is often a task of an IT auditor to assess whether the enterprise information system operates in compliance with laws and regulations. Definition of the scope and description of procedures are important parts of the audit plan that should be prepared for each assignment according to the Hierarchy of information system audit rules. Mapping of legislation requirements to COBIT 5 processes facilitates and accelerates the development of the audit plan and improves compliance with ISACA Information Technology Assurance Framework.*

The Article describes baselines and methodology of mapping the legislation requirements to COBIT 5 processes. The mapping procedure includes both substantive and operational maturity requirements. The Decision regulating risk management and implementation of the adequate internal capital assessment procedure for banks and savings banks has been mapped to COBIT 5 control objectives. The audit plan developed on the basis of such mapping then guides the information system auditor and supports him in managing the audit risk and the scope of audit in combination with the risk assessment.

The expectation that mapping itself would narrow the scope of audit has not come true. The decision requirements concerning the IT management and governance are mapped to all COBIT 5 processes except one and to the majority of IT management and governance practices

Key words ● *COBIT5, mapping, audit plan, compliance, legislation*

JEL: M42

Boštjan Kežmah

Obveznosti aktivnega preizkušenega revizorja informacijskih sistemov pri revidiranju osebnih podatkov

Obligations of active certified information system auditors when auditing personal data

POVZETEK ● *V prispevku obravnavamo formalni odnos med naročnikom in revizorjem informacijskih sistemov na področju varstva osebnih podatkov. Izhajamo iz zakonske podlage, ki revizorju omogoča obdelavo osebnih podatkov, ki mu jih posreduje revidirana enota. Pri tem je lahko revizor pogodbeni obdelovalec ali upravljavec osebnih podatkov. Vrsta razmerja bistveno vpliva na obseg obveznosti revizorja. Tveganje lastne skladnosti z varstvom osebnih podatkov revizor najlažje zmanjša s skrbnim načrtovanjem revizije ob upoštevanju sorazmernosti obsega obdelave osebnih podatkov.*

Ključne besede ● *revizija informacijskih sistemov, zasebnost, varstvo osebnih podatkov*

SUMMARY ● *In this paper we discuss the formal relationship between the client and the information systems auditor in the field of protection of personal data. We explain the legal basis allowing the auditor to process personal data transferred by the audited entity. The auditor may be either contractor data processor or data controller. Type of relationship significantly affects the scope of auditor liability. The best approach to reducing the risk of non-compliance with data protection regulations is careful audit planning, considering the principle of proportionality in personal data processing.*

Key words ● *IS audit, privacy, personal data protection*

JEL: M42

Rado Ključevšek

Skupno življenje in sinergija COBIT 5 in ISO/IEC 27001/27002

Coexistence and synergy of COBIT 5 and ISO/IEC 27001/27002

POVZETEK ● *Cilj prispevka je primerjava dveh načinov ureditve informacijske varnosti v organizaciji in analiza njunih skupnih značilnosti in razlik. Primerjamo COBIT 5 za informacijsko varnost, ki je nedavno izšel pri organizaciji ISACA, in standarda ISO/IEC 27001:2005 in 27002:2005. Opiramo se na obstoječo preslikavo okvira COBIT 5 za informacijsko varnost v druge okvire informacijske varnosti. Preslikavo obrnemo, da je urejena po poglavjih vsakega od standardov ISO/IEC in ne več po procesih okvira COBIT. V preslikavi smo označili poglavja in kontrole, pri katerih mora biti revizor ali svetovalec še posebej pozoren. To so predvsem področja, ki pri drugem načinu ne nastopajo. Opisali smo skupne značilnosti in razlike obeh načinov. Vsak ima svoje prednosti in slabosti in tudi priložnosti in grožnje. Za vsakega posebej smo naredili analizo SWOT in jo tabelarično predstavili. Po analizi in primerjavi smo povzeli še koristi njunega skupnega delovanja in našteli možne sinergije. Na koncu smo predlagali še način njune skupne uvedbe, pri čemer smo se oprli na življenjska kroga, ki ju vsak posebej vpeljuje v svoj način. Ker sta kroga različna, smo naredili ustrezno preslikavo enega v drugega.*

Ključne besede ● *COBIT 5, COBIT 5 za informacijsko varnost, ISO/IEC 27001, ISO/IEC 27002, informacijska varnost*

SUMMARY ● *The article compares two approaches to information security arrangement in an organization: COBIT 5 for information security that has been recently published by ISACA and the standards ISO/IEC 27001:2005 and 27002:2005. The comparison is based on the existing mapping of the COBIT 5 framework for information security to some other information security frameworks. The mapping has been turned around, so that it is now arranged according to the chapters of the standards and not to the processes of COBIT. In the mapping, we have marked some chapters and controls to which the auditor or consultant should pay special attention. Mostly, these are the areas which do not appear in the other approach. The article continues with a description of the common features and the differences of the approaches. Each of them has its own strengths, weaknesses, opportunities and threats. A SWOT analysis is done for each approach separately, and presented in a table. After the analysis and comparison has been done, a summary is given of the benefits from their common operation and of possible synergies. At the end, the authors suggest a way for their common implementation on the basis of the life cycles that each of the approaches makes use of. Because the life cycles are different, a mapping from one to the other is made, accordingly.*

Key words ● *COBIT 5, COBIT 5 for information security, ISO/IEC 27001, ISO/IEC 27002, information security*

JEL: M15 IT Management

John Mitchell, PhD

Digital Forensics: finding and preserving the hidden evidence

Računalniško preiskovanje (dobre, slabe in grde strani preiskovanja)

POVZETEK ● *Preiskovanje digitalnih dokazil je kot izlet v preteklost, vendar potrebujemo informacijo o tem, kdaj in kam v preteklost želimo odpotovati. Obstoj stvari/dokazil na računalniku je običajno danost. Pomembna vprašanja so: Kako so prišla tja, kdaj so prišla in ali je kdo vedel, da so prišla? Namen je pomemben pri obravnavi, vendar dokaz sam molči o tem in tako se namen dokazuje z okoliščinami. Pogosto se od forenzičnega preiskovalca zahteva, da pridobi dokaze, ki podpirajo ali izpodbijajo posebnost primera, kar samo po sebi opredeljuje delo, ki ga je treba opraviti. Dejstva so absolutna, mnenja so osebna. Dejstva morajo podpreti mnenja, vendar je vprašanje, ali je vedno tako. Predavanje bo obravnavalo dobre, slabe in grde strani forenzičnega preiskovanja*

Ključne besede ● *Računalniško preiskovanje, zbiranje dokazil, zavarovanje dokazil, elektronske naprave*

SUMMARY ● *Examination of digital evidence is an excursion into the past, but just like any time traveller we need to know where and when in the past we have travelled to. The existence of items on a digital device is usually a given. The important questions are: how did it get there, when did it get there and did anyone know that it was there? Intent is a very important consideration, but the evidence is usually silent on this and intent is often proved circumstantially. The forensic examiner is often asked to either look for evidence to support, or disprove a specific case and this in itself may provide a bias to the work they undertake. Facts tend to be absolute, but opinion is personal. The facts should support the opinion, but is this always the case? This presentation will cover the good, the bad and the ugly aspects of digital forensics.*

Key words ● *Digital forensics, evidence gathering, securing evidence, digital devices*

Andrej Zimšek

Upravljanje identitet

Identity management

POVZETEK ● *Upravljanje identitet se uporablja za nadzor uporabnikov in njihovih pravic. Vpeljava sistema za upravljanje identitet zahteva urejene podatke o vseh uporabnikih v informacijskem sistemu. Prav tako morajo biti skrbno izbrani in opredeljeni procesi za dodajanje novega uporabnika v informacijski sistem in spreminjanje njegovih pravic.*

To področje je v letošnjem letu dobilo tudi dokument, ki obravnava revizijo sistemov za upravljanje identitet (angl. Identity Management Audit/Assurance Program, ISACA).

V članku so predstavljene smernice, podane v dokumentu Identity Management Audit/Assurance Program, ISACA, in praktične izkušnje pri vpeljavi programskih rešitev, ki omogočajo avtomatizacijo upravljanja identitet. Za celovito obravnavo uporabnika je treba upoštevati vse storitve uporabnika, ki jih potrebuje pri svojem delu, kar pomeni v nekaterih okoljih tudi vključevanje storitev v oblaku v celovit sistem upravljanje identitet.

Ključne besede ● *upravljanje, identiteta, uporabnik, revizija, informacijski sistem, pravice, avtomatizacija, oblak*

SUMMARY ● *Identity Management is used to manage the users and their rights. The implementation of a system for identity management requires properly ordered data of all users in the information system. All processes for adding a new user to the information system and the evolution of its rights should be carefully selected and defined.*

This year, identity management has received a document which deals with the audit of identity management systems – "Identity Management Audit /Assurance Program, ISACA".

The article presents the guidelines given in the "Identity Management Audit/Assurance Program, ISACA" and practical experience in implementing software solutions that enable automation of identity management. For a comprehensive treatment of the user it is necessary to consider all services that the user uses at work, which also means integration of cloud services into a comprehensive identity management system.

Key words ● *Identity, management, user, audit, information system, cloud services, automation.*

JEL: M12

Dr. Igor Pšunder

Mera kapitalizacije pri ocenjevanju vrednosti pravic na nepremičninah

Capitalization Rate in Real Property Appraisal

POVZETEK ● *Mero kapitalizacije lahko pri ocenjevanju vrednosti nepremičnin izračunamo na podlagi tržne primerjave in na podlagi metode dograjevanja, ki je uporabna tudi, ko ni na voljo veliko tržnih podatkov o primerljivih prodajah in oddajah nepremičnin.*

Metoda dograjevanja temelji na sestavljanju mere kapitalizacije iz donosnosti netveganih naložb in dodatnih premij. Pri tem je izpostavljena (pre)veliki subjektivnosti ocenjevalca, saj skoraj vse spremenljivke temeljijo na izkustvenih podatkih.

Pričujoč članek temelji na raziskavi, izvedeni med pooblaščenimi ocenjevalci vrednosti nepremičnin, na podlagi katere je izvedena parametrizacija spremenljivk, posebej premije za tveganje.

Ključne besede ● *mera kapitalizacije, metoda neposredne kapitalizacije, premija za tveganje, ocenjevanje vrednosti nepremičnin*

SUMMARY ● *Capitalization rate in real property appraisal can be caculated by applying the market approach or the build-up method which can also be used in cases where not much market information on comaparble sales or leases of real property is available.*

The build-up method is based on the sum of capitalization rate derived from the rate of return for risk free investments, and additional premiums (risk allowance). The method is too much exposed to subjective judgement of the appraiser since almost all the variables are based on empirical data.

The article is based on a research conducted among certified real estate appraisers, including a parametrization of variables, especially the risk allowance.

Keywords ● *Capitalization rate, direct capitalization method, risk allowance, real estate appraisal*

JEL: R30, D46 in G12