

Dr. Boštjan Delak

Prepoznavanje znanja in tveganja pri upravljanju znanja

Identification of knowledge and knowledge management risks

POVZETEK ● Znanje je največja konkurenčna prednost podjetja. Prepoznavanje znanja je poseben izziv, ki ga je treba ustrezno obravnavati. Poznamo dve vrsti znanj – implicitno, ki je del veččin zaposlenih in ni dokumentirano, ter eksplicitno, ki je zabeleženo v različnih oblikah zapisov – dokumentov. Prispevek seznanja bralca s terminologijo znanja, z življenjskim ciklom znanja ter s tveganji, povezanimi z znanjem. Poleg tega predstavi procesa upravljanja znanja, in sicer COBIT 5 – Upravljanje kadre in Upravljanje znanje, ki ju lahko učinkovito uporabimo pri reviziji področja upravljanja znanja v sklopu revizije informacijskih sistemov. Predstavljene so tudi aktivnosti, ki se pojavljajo v svetu glede neodvisnih revizij področja upravljanja znanja. Revizorji informacijskih sistemov moramo biti s takimi možnostmi seznanjeni, saj bo v prihodnje temu področju posvečeno vedno več pozornosti.

Ključne besede ● znanje, kritično znanje, poznavanje tveganj, izguba znanja, upravljanje znanja

SUMMARY ● Knowledge is the greatest competitive advantage. Identification of knowledge is a particular challenge, which needs to be properly addressed. There are two types of knowledge – implicit knowledge, which is in the minds of employees and not documented and explicit knowledge recorded in a variety of formats – documents. The paper informs the reader with the terminology of knowledge, the life cycle of knowledge, and the risks related to knowledge. In addition, the paper presents the process of knowledge management and the COBIT 5 processes – Manage Human Resources and Manage Knowledge – that can be effectively used in the knowledge management audits carried out as part of the information system audits. The paper also presents activities that occur in the world in the field of independent knowledge management auditing. As information system auditors, we have to be familiar with such options, since more and more attention will be paid to this area in the future.

Key words ● knowledge, critical knowledge, knowledge related risk, knowledge loss, knowledge management

Mag. Igor Karnet

Odtekanje podatkov – ali so tehnične rešitve sploh pravi pristop?

Leakage of data – Are technical solutions the right approach at all?

POVZETEK ● Prispevek obravnava področje informacijske varnosti, ki je samo toliko močna, kot je močan njen najšibkejši člen. Pogosto so najšibkejši člen ljudje. Tveganja spreminjajo najnovejši družbenimi trendi, tehnologije, funkcionalnosti in storitve, ki jih uporabljamo dnevno. Zavedanje o možnih škodnih dogodkih in posledicah pri njihovi uresničitvi je ključno. V prispevku je nakazano, kakšno je stanje v organizacijah, še posebej v sektorjih za informacijsko tehnologijo, kaj lahko naredimo, da bodo uporabniki dobili ponujene, zelene funkcionalnosti, da bo za varnost zaupnih in občutljivih podatkov vseeno poskrbljeno v skladu s stopnjo tveganja, ki jo je organizacija pripravljena sprejeti, v okviru teh pa bo čim manj možnosti za nepooblaščen odtekanje podatkov. Dodani so predlogi, kako obstoječe stanje izboljšati in zagotoviti dovolj varno okolje.

Ključne besede ● odtekanje podatkov, tveganja, zavedanje, tehnične rešitve, incident

SUMMARY ● The paper addresses information security, which is only as strong as its weakest link. It is quite often that the weakest link are people. Risks have changed due to the latest social trends, technology, functionality and services used by end-users. However, awareness of incidents/risks and potential consequences is crucial. The paper will bring to attention, what can be done that the users will be able to use the needed services of desired functionality and the security of personal and sensitive data will be achieved at an acceptable level of risk, ensuring at the same time that the risk of unauthorised leakage will be as low as possible. Some suggestions are added, how to improve the current situation and to provide a sufficiently safe environment.

Key words ● Leakage of data, technical solutions, risk, awareness, incident

Robert Malačič

Vrednotenje kakovosti informacijskih rešitev s konceptom tehničnega dolga

Evaluating the quality of information solutions with the concept of technical debt

POVZETEK ● Metrike programske opreme nam ponujajo možnost, da neki projekt ocenimo glede na kakovost njegove izdelave, tj. ocenimo kakovost njegove programske kode. Da bi neko programsko rešitev lahko ocenili,

moramo določiti in pregledati njene metrike, ki nam prikažejo številčne podatke o stanju programske kode, njeno zanesljivost, dokumentiranost, podvrženost napakam ipd. S pomočjo metrik programske opreme je možno oceniti, ali se neka programska rešitev drži predpisanih standardov, ki jih izbrana metrika ponazarja oz. meri.

Metrike programske opreme nam omogočajo tudi izračun t. i. tehničnega dolga, ki nam s svojo vrednostjo pove, koliko ur programerskega dela bi bilo potrebno za njegovo odpravo. Spremljanje tehničnega dolga med samim razvojem projekta pa omogoča nadzor nad kakovostjo izvirne programske kode skozi njen razvoj, s tem pa pripomore tudi k zmanjšanju stroškov.

Ključne besede ● tehnični dolg, programske metrike, SonarQube, SQA

SUMMARY ● Software metrics offer us the possibility to evaluate a software project on the basis of its design quality, which means to assess the quality of its program code. To evaluate a software solution, we must determine and review its metrics. Metrics gives us numerical data on the state of the software code, its reliability, the state of its documentation, and error proneness. Software metrics information makes it possible to evaluate whether a software solution follows the standards indicated or measured by the selected metrics.

The use of software metrics also allows us to calculate the technical debt, whose value tells us how many hours of software design a software engineer would need to fix the produced debt. Monitoring the technical debt during the development of a software project allows us to control the quality of the source code and contributes to reducing the costs.

Key words ● technical debt, software metrics, SonarQube, SQA

Manuela Šribar

Revizija računovodskih izkazov in revizor informacijskih sistemov

Financial Statements Audit and Information System Auditor

POVZETEK ● V prispevku je pojasnjeno, kaj je revizija računovodskih izkazov in kakšna zagotovila daje revizor računovodskih izkazov pri izdaji revizorjevega poročila skladno z Mednarodnimi standardi revidiranja. Predstavitev konkretnih primerov prikazuje nujnost sodelovanja med pooblaščenim revizorjem in njegovim veščakom – informatikom pri revizijah računovodskih izkazov. Posebej so izpostavljeni primeri, pri katerih velika tveganja na področju informacijskega sistema pri revidiranju nimajo nujno pomembnega vpliva na točnost in poštenost računovodskih izkazov. Prikazani so tudi primeri, pri katerih je sodelovanje revizorja računovodskih izkazov s preizkušenim revizorjem informacijskega sistema zelo priporočljivo oz. skoraj nujno, če nima ustreznih orodij in znanj.

V prispevku je opredeljeno, kako podroben naj bo pregled informacijskega sistema v okviru revizije računovodskih izkazov.

Ključne besede ● *revidiranje, revidiranje računovodskih izkazov, revizor računovodskih izkazov, revizor informacijskih sistemov, tveganja*

SUMMARY ● *The article explains the purpose of financial statements audits and the assurances provided by the auditor of financial statements in accordance with International Auditing Standards, highlighting the need for cooperation between the financial statements auditor and the information systems auditor, acting as an auditor's expert. Examples are presented to demonstrate that clients with high risks regarding their IT systems do not necessarily pose a high risk in terms of presenting a true and fair view in their financial statements. In addition, examples of situations are given where cooperation with an IS auditor is highly recommended, if not imperative, as the financial statements auditor will usually not have the relevant expert knowledge, skills and tools. The scope of an IT system review for the purpose of financial statements auditing is also presented.*

Key words ● *Auditing, auditing of financial statements, financial statements auditor, information system auditor, risks*