SIR IUS 5/17

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

SLOVENSKI INŠTITUT za REVIZIJO

Marko Anžič

Tveganja interneta stvari, ki bodo zaznamovala našo družbo

IoT related risks that will impact our society

POVZETEK ● *Internet stvari (IoT) povezuje vse več naprav in oseb v globalno omrežje, v katerem se podatki neprenehoma ustvarjajo, medsebojno izmenjujejo in analizirajo. Priložnosti, ki jih ponuja, se zdijo neskončne, omejene le z domišljijo. Pa vendar vsaka revolucija na področju tehnologije povzroči revolucijo človeške družbe. Vse posledice revolucije niso pozitivne, a dobra pripravljenost na tveganja nastanka negativnih posledic lahko te precej omili. Revizor lahko ob ustrezni proaktivnosti veliko pripomore k obvladovanju teh tveganj. V članku obravnavam raznolikost, obsežnost ter predvsem novost tveganj, povezanih z IoT-om, ki jih bo moral revizor ustrezno prepoznati in z uporabo ustreznih okvirov oceniti ter naročniku pomagati pri njihovem obvladovanju.*

Ključne besede ● *internet stvari, priložnosti, tveganja, prihodnost, revizorjeva vloga*

SUMMARY ● *Internet of Things (IoT) is growing by including more and more devices and persons in a global network, in which data is being constantly generated, exchanged and analyzed. Opportunities that it offers seem limited only by our imagination. Yet every technological revolution results also in a social revolution. Not all consequences will be positive, yet proper preparedness for the related risks can substantially reduce the negative side effects. An auditor, by being proactive, can significantly contribute to managing these risks. This article intends to highlight the diversity, breadth and, most importantly, the novelty of risks, related to IoT, which the auditor will have to properly identify and using appropriate frameworks evaluate them, and help its client manage them.*

Key words ● *Internet of Things, opportunities, risks, future, auditor's role*

Dr. Boštjan Delak

Revizija stanja kibernetske varnosti

Cybersecurity auditing

POVZETEK ● *Dogodki na področju kibernetske varnosti v prvi polovici 2017 v Sloveniji in svetu nas opozarjajo, kako zelo smo ranljivi in premalo ozaveščeni na tem področju. Kibernetski napadi manjših in večjih razsežnosti se dogajajo in so del naše stvarnosti. Države, podjetja in posamezniki se različno odzivajo na te grožnje in ranljivosti. Dvigovanje odpornosti proti tem tveganjem lahko izvajamo samo z načrtnim in rednim spremljanjem varnostnih dogodkov, sprotnim nadgrajevanjem zaščitnih in varnostnih ukrepov in rednim preverjanjem – revizijo kibernetske varnosti.*

Prispevek seznani bralca s trenutnim stanjem v Sloveniji ter predstavi pomembne standarde, metodologije in dobre prakse na tem področju. Podrobno je opisan celovit okvir za preverjanje stanja kibernetske varnosti. V prispevku so predstavljene tudi izkušnje iz dajanja zagotovil na tem področju v Sloveniji ter nekatere možne aktivnosti v zvezi z njihovim izvajanjem. Revizorji informacijskih sistemov moramo biti pri dajanju zagotovil, revizijah ali pregledih pozorni na celovitost in kompleksnost tega področja. Prispevek osvešča revizorje informacijskih sistemov in jih usmerja k uporabi predstavljenega celovitega okvira za revizijo kibernetske varnosti.

Ključne besede ● *kibernetska varnost, revizija kibernetske varnosti, načrt revidiranja kibernetske varnosti, ozaveščanje*

SUMMARY ● *Events in the field of cyber security in Slovenia as well as in the world in the first half of 2017 remind us how much we are vulnerable, and how big is lack of awareness in this area. Cyberattacks of smaller and larger dimensions happen and are part of our reality. Countries, companies and individuals respond differently to these threats and vulnerabilities. Raising resistance against these risks can only be carried out with systematic and regular monitoring of security events, ongoing upgrading security and safety measures and regular checking – auditing cybersecurity. The paper acquaints the reader with the current situation in Slovenia and presents the relevant standards, methodologies and best practices in this field. The framework for cybersecurity is presented. In addition, the paper presents the experience with regard to providing assurance in this field in Slovenia, as well as some of the possible activities in relation to their implementation. Information systems auditors have to pay attention to the integrity and complexity of this area. The paper raises the awareness of information system auditors and instructs them on the use of the presented integrated framework for cybersecurity audits.*

Key words ● *cybersecurity, cybersecurity audit, cybersecurity audit plan, raising awareness*

Dr. Boštjan Kežmah

Samodejno testiranje programske opreme

Automated software testing

POVZETEK ● *Testiranje programske opreme je skladno z dobro prakso in pričakovanji uporabnikov informacijskega sistema temeljna kontrola zagotavljanja kakovosti informacijskega sistema. Z uporabo samodejnih testov lahko bistveno vplivamo na kakovost programske opreme in hkrati obvladujemo stroške testiranja predvsem pri izvajanju regresijskih testov, ki dokazujejo, da vse funkcije programske opreme tudi po zadnji spremembi še vedno delujejo pravilno. Samodejno testiranje programske opreme pa še vedno ne more v celoti zamenjati vseh oblik testiranja programske opreme.*

Ključne besede ● *testiranje, programska oprema, COBIT 5*

SUMMARY ● *Software testing is compliant with good practice and expectations of information system users. It presents basic control for the information system quality assurance. By using automatic tests, we can significantly influence the quality of the software, and at the same time manage the cost of testing, especially in the implementation of regression tests, which prove that all functions of the software continue to function properly even after the last change. However, automatic software testing still cannot completely replace all forms of software testing.*

Key words ● *testing, software, COBIT 5*

Dr. Urška Kežmah

Vloga preizkušenega revizorja informacijskih sistemov v sodnih postopkih

The role of the certified information systems auditor in court proceedings

POVZETEK ● *Prispevek obravnava različne procesne vloge preizkušenega revizorja informacijskih sistemov v pravdnem postopku. Predstavljeni so sistem dokazovanja in pomen načela proste presoje dokazov ter posamezna dokazna sredstva po Zakonu o pravdnem postopku. Preizkušeni revizor informacijskih sistemov bo v pravdnem postopku najpogosteje nastopal v vlogi izvedenca, priče ali izvedene priče. Po potrebi pa je lahko v postopku udeležen tudi pri opravi drugih procesnih dejanj (npr. ogledu) po odredbi sodišča.*

Ključne besede ● *preizkušeni revizor informacijskih sistemov, pravdni postopek, izvedenec, priča, sistem dokazovanja*

SUMMARY ● *The article discusses various procedural roles of a certified information system auditor in civil procedure. A system of evidence and the importance of the principle of free assessment of evidence and individual evidence under the Civil Procedure*

Act is presented. A certified information system auditor will most often act in the role of an expert, a witness, or an expert witness in a civil procedure. If necessary, he may also be involved in the proceeding when performing other procedural acts (e.g. viewing) under a court order.

Key words ● *certified information system auditor, civil procedure, expert, witness, system of evidence*

Dr. Aleš Živkovič

Določanje vrednosti in spremljanje stroškov projektov razvoja programske opreme

Defining value and monitoring costs in software development projects

POVZETEK ● *Kljub vse večji razširjenosti računalništva v oblaku imajo projekti razvoja nove programske opreme pomembno vlogo pri zagotavljanju informacijskih storitev poslovnim uporabnikom. Vsak projekt naj bi bil posledica uresničevanja strateškega načrta informatike, z jasno določenimi cilji in projektno dokumentacijo, na podlagi katere se odgovorni projekt odobri. Del projektne dokumentacije je tudi ocena stroškov projekta, ki mora imeti podlago v oceni truda, potrebnega za izdelavo informacijske rešitve. Trud se glede na uporabljeno metodologijo razvoja programske opreme ocenjuje na različne načine.*

V prispevku smo predstavili način vrednotenja in spremljanja stroškov projektov, katerih cilj je razviti novo informacijsko rešitev. Predstavljene so formalne standardne metode za ocenjevanje obsega ter pristopi, ki se pogosto uporabljajo pri agilnem razvoju. Opisana je razlika med različnimi pristopi in vpliv na določanje skupnih stroškov. Na podlagi izkušenj smo dali tudi nekaj napotkov revizorjem informacijskih sistemov pri revidiranju projektnih predlogov, projektov v teku in zaključenih projektov. Prispevek smo zaključili z iztočnicami za uporabo metod, predstavljenih v prispevku pri drugih oblikah zagotavljanja informacijskih rešitev (npr. SaaS, zunanje izvajanje, nakup rešitve na ključ idr.), da bi ugotovili smotrnosti porabe sredstev.

Ključne besede ● *določanje stroškov, določanje truda projektov razvoja programske opreme, obseg programske opreme*

SUMMARY ● *Despite the increased popularity of Cloud Computing, software development projects remain an important element of information support to business users. Every project should be part of a strategic plan with clearly defined goals and project documentation that supports informed decisions. Cost estimates are part of project documentation; they should be based on software size and effort estimates. There are different methods to estimate the project size and effort.*

This paper presents how to evaluate and track project costs for software development projects. Formal standardized functional size measurement methods are described and compared to approaches commonly used in agile development. Based on our experience, recommendations are provided for information system auditors engaged in audits related

to ongoing or completed software development projects. Finally, the paper provides some hints on how to use the described methods in initiatives related to cloud computing or procurement of software solutions in order to monitor IT budgets.

Key words ● *costs, software size and effort estimates, software size*