SIR IUS 5/21
SLOVENSKI INŠTITUT za REVIZIJO
Revija za teorijo in prakso revizije, računovodstva, davkov, financ, ocenjevanja vrednosti in drugih sorodnih področij

Kazalo

Iz prakse za prakso

Novosti in obvestila

Dr. Tina Beranič, Miroslav Beranič

Uporaba standardov pri revidiranju inženiringa zahtev programske opreme

Application of the relevant standards in auditing software requirement engineering

Povzetek • *Inženiring zahtev je ključni začetni korak pri razvoju programske opreme. Gre za skupek procesov, katerih namen je pretvorba ugotovljenih potreb deležnikov v primerno oblikovane specifikacije zahtev programske opreme. Te predstavljajo vhod in so izhodišče za nadaljnje korake v razvoju programske opreme. Neprimerno in nepopolno oblikovane zahteve lahko povzročijo številne ovire ter vplivajo na uspešnost projekta razvoja programske opreme. Zato je smiselno, da pri pripravah zahtev programske opreme sledimo obstoječim dobrim praksam, smernicam in standardom. Eden izmed slednjih je tudi standard ISO/IEC/IEEE 29148:2018. Aktualna verzija v domeno inženiringa zahtev programske opreme uvršča tri procese življenjskega cikla, opredeljene v sorodnih standardih.*

V prispevku so predstavljeni omenjeni standard in z njim močno prepletena standarda. Prikazan je njihov pomen pri izvedbi revizijskega posla preverjanja skladnosti inženiringa zahtev s standardom ISO/IEC/IEEE 29148:2018. V teoretičnem delu prispevka najprej predstavimo pojma programska oprema in programsko inženirstvo ter življenjski cikel programske opreme. Sledi obravnava domene in procesov inženiringa zahtev, pri čemer s praktičnimi primeri preverjanja skladnosti opravil v aktivnostih procesa prikažemo eno izmed možnih poti revidiranja inženiringa zahtev programske opreme.

Ključne besede • *programsko inženirstvo, življenjski cikel programske opreme, inženiring zahtev, ISO/IEC/IEEE 29148:2018, zahteve programske opreme*

Summary • *Software requirement engineering is a key initial step within the software development process. It represents a set of processes resulting in appropriately defined software requirement specifications based on the identified stakeholders needs. Requirements present input and provide the basis for the following steps in the software development process. Improperly and incompletely formulated requirements can pose several challenges and impact the success of a software development project. Therefore, it is crucial to follow existing good practices, guidelines and standards when outlining software requirements. One of the available standards is the ISO/IEC/IEEE 29148:2018. The current version covers three processes addressing the software requirements engineering domain that are de-*

fined by related standards.

The paper presents the ISO/IEC/IEEE 29148:2018 standard and intertwined standards, emphasising their importance within audit, focusing on verifying the compliance of software requirement engineering. The paper first presents the concepts of software, software engineering and software life cycle, followed by the presentation of the software requirement engineering domain from the perspective of considered standards. The second part of the paper supplement the theoretical knowledge by presenting several practical audit examples addressing the verification of the compliance with the selected standard, presenting one of the possible ways of auditing the software requirement engineering domain.

Key words • *software engineering, software life cycle, requirement engineering, ISO/IEC/IEEE 29148:2018, software requirements*

Dr. Boštjan Kežmah

Pregled kibernetske varnosti

Cyber Security Review

Povzetek • *Pojem kibernetske varnosti ni soglasno določen, zato pregled tega področja zahteva jasno določitev ciljev, omejitev in predvsem sodil pregleda. Pri sodilih je razen splošnih okvirov upravljanja in vodenja informacijskih sistemov, kot sta COBIT 2019 in ITIL, ali standardov, kot je SIST EN ISO/IEC 27001:2017, smiselno uporabiti tudi podrobnejše izvedbene tehnične smernice in dobre prakse, kot so na primer okvir NIST in CIS-ove kontrole. Le z dovolj podrobnimi sodili je mogoče utemeljeno, brez proste presoje, izvesti pregled ter strokovno utemeljiti ugotovitve in priporočila. Ne glede na uporabljene smernice je pregled kibernetske varnosti povezan s podrobnimi tehničnimi kontrolami, pri pregledu katerih mora smiselno sodelovati ustrezno usposobljen strokovnjak.*

Ključne besede • *kibernetska varnost*

Summary • *The concept of cyber security is not defined unanimously, so the review of this area requires a clear definition of the objectives, limitations, and, above all, the review criteria. In addition to general frameworks for the management and governance of information systems such as COBIT 2019 and ITIL or standards such as SIST EN ISO / IEC 27001: 2017, it makes sense to use more detailed technical guidelines and good practices, such as the NIST framework and CIS Controls. Only with the use of sufficiently clear criteria is it possible to carry out a reasoned review and professionally substantiate findings and recommendations without discretion. Irrespective of the guidelines used, the cyber security review is linked to detailed technical controls, the assessment of which must involve a suitably qualified professional.*

Key words • *cyber security*

Iztok Jeras

Revidiranje podatkovnih baz

Database auditing

Povzetek • *Opredeliti skušamo nekaj vidikov revidiranja podatkovnih baz, vendar pa pričujoči članek ni neposredno namenjen pripravi revizijskega plana, ampak poudarja nekaj posebnosti področja. Pri revidiranju podatkovnih baz je treba upoštevati pomembnost upravljanja podatkov in tehnično zahtevnost sistema za upravljanje podatkovnih baz. To pomeni tako ustrezno ovrednotenje (klasifikacijo) podatkov oz. informacij kot tudi tehnično podkovanost revizorja informacijskih sistemov (v nadaljnjem besedilu: IS) za preverjanje upravljanja podatkovne baze (tehnične značilnosti, orodja …). Revizor IS mora pridobiti zagotovila, da strategija informacijske tehnologije (v nadaljnjem besedilu: IT) in arhitektura podatkovne baze ustrezata strategiji podjetja in delovanju poslovnih funkcij. Precejšnjo pozornost je treba posvetiti varnosti in ustreznosti varnostnih politik podatkovne baze, vključno z uporabniškimi pooblastili in revizijskimi sledmi. Z operativnimi postopki in nastavitvami skušamo preveriti in izboljšati razpoložljivost in odzivnost podatkovne baze, uporabo različnih orodij za dostop in učinkovitost nadzora. Upravljanje sprememb podatkovne baze je podvrženo temeljitemu testiranju, s katerim zagotavljamo ustrezno celovitost, zaupnost in razpoložljivost informacij. Postopki neprekinjenosti zagotavljajo delovanje oz. obnovitev podatkovne baze ob katastrofi in/ali izpadu posameznih komponent. V članku so opredeljeni tudi vidiki revidiranja podatkovne baze v oblaku. Različne oblike implementacije oblačnih storitev in podatkovne baze zahtevajo tudi različne revizorske pristope, predvsem z vidika razmejitev odgovornosti ponudnika oblačnih storitev na eni in uporabnika/naročnika na drugi strani.*

Ključne besede • *varnost podatkovne baze, šifriranje, revizijske sledi, operativni postopki, upravljanje sprememb, neprekinjenost, revidiranje baze v oblaku*

Summary • *In the article we are covering the area of database auditing, not in the sense of creating an exact auditing plan, but more to stress out certain interesting points and specifics of that area. Information system (herainafter: IS) auditor must be able to evaluate the governance of the corporate data on one hand and possess certain technical skills on the other hand. In practice this means - for example - evaluating the data classification scheme on one hand and technical possibilities of the database and database tools usage on the other hand. IS auditor must ensure that IT strategy and database architecture follow the corporate strategic goals and generate appropriate business value. Database security and user privileges always require IS auditors special attention. Through evaluation of operational procedures and database settings auditor can ensure adequate avail-*

ability and performance of the database. Also proper usage of database tools for database access and administration should be checked during the audit to achieve adequate monitoring and control of the database. Database (settings) changes must be properly tested and proper disaster recovery and business continuity procedures must be established to ensure confidentialitiy, integrity and availability of the database. In the article we arek also talking about the specifics of IS auditing the database in the cloud. Different implementations of cloud services require also different IS auditor approach.

Key words • *database security, cyphering, database audit trails, operations, change management, database recovery, cloud auditing*

Jaka Kosmač

Revizija kibernetske varnosti v javnem sektorju – pomembni premiki v Evropi in Sloveniji

Auditing cyber security in public sector – important developments in Europe and Slovenia

Povzetek • *Kibernetska varnost in zavedanje o njenem pomenu se v zadnjih letih vedno bolj krepi v družbi in javnem sektorju, saj smo zaradi vedno večje povezljivosti omrežij in sistemov na tem področju tudi ranljivejši. Kibernetski napadi na kritično infrastrukturo so vse pogostejši, s seboj prinašajo velike stroške ter vse bolj neposredno vplivajo na zdravje in varnost ljudi, kar je lahko ena izmed stranskih posledic kibernetskih napadov na zdravstvo. Evropsko računsko sodišče se zaveda, da sta kibernetska varnost in digitalna avtonomija za Evropsko unijo in njene države članice strateško pomembna tema. Z zviševanjem stopnje ogroženosti je treba krepiti prizadevanja za zaščito kritičnih informacijskih sistemov in digitalne infrastrukture pred kibernetskimi napadi. Vrhovne revizijske institucije kot nadzorne institucije imajo na tem področju svoj dolg in mesto, saj lahko z izvajanjem revizij pri kibernetski varnosti pravočasno in pomembno pripomorejo k izboljšavam in napredku na tem področju. Evropsko računsko sodišče je konec leta 2020 izdalo Kompendij revizijskih poročil o kibernetski varnosti v Evropski uniji in njenih državah članicah, v katerem je med drugim povzelo ugotovitve 12 revizijskih poročil vrhovnih revizijskih institucij, objavljenih med letoma 2014 in 2020. Tudi Računsko sodišče Republike Slovenije je dovolj zgodaj prepoznalo pomen kibernetske varnosti za Republiko Slovenijo, tako da je v začetku marca 2021 izdalo revizijsko poročilo Učinkovitost zagotavljanja kibernetske varnosti v Republiki Sloveniji. V prispevku so predstavljene pomembnejše revizije, ki so jih izvajale evropske vrhovne revizijske institucije na širšem področju kibernetske varnosti, ter revizija učinkovitosti zagotavljanja kibernetske varnosti v Republiki Sloveniji.*

Ključne besede • *kibernetska varnost, Evropsko računsko sodišče, Računsko sodišče Republike Slovenije, revizija*

Summary • *Cyber security and awareness of its importance have been growing in recent years in society as well as in the public sector, as we are more vulnerable due to the increasing connectivity of networks and systems in this area. Cyber attacks on critical infrastructure are becoming more common, costly, and have a direct impact on human health and safety, which may be one of the side effects of cyber attacks on health. The European Court of Auditors is aware that cyber security*

and digital autonomy are a strategically important issue for the European Union and its Member States, and efforts to protect critical information systems and digital infrastructure from cyber attacks need to be stepped up by increasing the level of threat. Supreme Audit Institutions, as supervisory institutions, have a duty and a place in this area, as they can make timely and important contributions to improvements and progress in this area by conducting cyber security audits. At the end of 2020, the European Court of Auditors issued a Compendium of Audit Reports on Cyber Security of the EU and its Member States, summarizing the findings of 12 Supreme Audit Institutions audit reports published between 2014 and 2020. The Court of Auditors of Republic of Slovenia also recognized the importance of cyber security for the Republic of Slovenia and in the beginning of March 2021 issued an audit report on the efficiency of cyber security in the Republic of Slovenia. In this article, I will present important audits carried out by the European Supreme Audit Institutions in the broader field of cyber security and the audit of the Efficiency of cyber security in the Republic of Slovenia.

Key words • *cyber security, European Court of Auditors, Court of Audit, audit*

Aleksandra Vugrin

Vizualizacija podatkov kot pomoč pri interpretaciji revizijskih poročil

Data visualization as help for interpretation of audit reports

Povzetek • *Glavna naloga vizualizacije podatkov v revizijskih poročilih je razlaga revidirancu oz. bralcu. Prispevek v dveh delih obravnava kreiranje in oblikovanje vizualizacije podatkov. V prvem delu je predstavljena metoda oblikovalskega mišljenja, s katero rešujemo probleme prikaza, tako da bralca postavimo v središče. Določimo glavno sporočilo vizualizacije, pridobimo širši nabor zamisli in jih s prototipom testiramo še pred končnim oblikovanjem. V drugem delu prispevka na praktičnem primeru grafa pokažemo, kako lahko katero koli vizualizacijo naredimo jasnejšo in z odstranitvijo nepotrebnega balasta pridobimo izčiščeno osnovno. V prispevku obravnavamo še, kaj so predpozorni atributi – vizualne lastnosti, ki jih ljudje uporabljamo za zaznavo sprememb v vzorcu. Njihovo uporabo za usmerjanje bralčeve pozornosti ponovno prikažemo na primeru istega grafa. V zadnjem delu prispevka smo temu primeru dodali še komentar, ki bralcu informacijo postavi v kontekst, s katerim vizualizacija postane zgodba.*

Ključne besede • *vizualizacija podatkov, oblikovanje, oblikovalsko mišljenje, predpozorni atributi, pripovedovanje zgodb*

Summary • *The main task of visualizing data in audit reports is explaination of audit findigns to the auditee or the reader. The paper discusses the creation and design of data visualization in two parts. The first part presents the design thinking method with which we solve problems by placing the reader in the center. Than we define the main visualization message, obtain a wider range of ideas and test them with the help of a prototype before the final design. In the second part the paper presents a practical example of a visualization clearification and simplification. The paper then discusses the pre-attentive attributes - visual properties that people use to detect changes in patterns and their use in order to direct the reader's attention. This is shown again on the same example. In the end an annotation is added to this example which explains the context to the reader and makes the visualization a data story.*

Key words • *data visualization, design, design thinking, preattentive attributes, storytelling*

Dr. Renato Vrenčur

Zavarovanja plačil z globalnimi odstopi terjatev v zavarovanje v poslovni in sodni praksi – 2. del

Collateral of Payments with Global Assignments of Receivables in Business Practise and Case Law – Part 2

Povzetek • *Poslovna praksa zahteva uporabo različnih instrumentov zavarovanja obveznosti. S tem se okrepi upnikov položaj ob neplačevitosti dolžnika, še zlasti v stečaju ali izvršbi. Izbira ustreznega zavarovanja je zelo pomembna. V prispevku so poudarjene nekatere sodobne oblike zavarovanja (fiduciarna zavarovanja, še posebej fiduciarni odstop terjatev v zavarovanje). Nekateri instrumenti zavarovanja so izrazito akcesorne narave (na primer zastavna pravica na terjatvah), medtem ko drugi predstavljajo tipične neakcesorne modele zavarovanja (na primer fiduciarna zavarovanja). Poznavanje omenjene pravne narave obravnavanih instrumentov je več kot nujno za ustrezno izbiro in uporabo posameznih modelov v praksi.*

Ključne besede • *fiduciarna zavarovanja, terjatev, odstop terjatve v zavarovanje, insolventnost*

Summary • *The application of various instruments of collateral is required in business practice to strengthen the position of creditors in the event of default by debtors, and in particular in bankruptcy or execution. Choosing appropriate collateral is very important. The article presents contemporary forms of collateral (fiduciary collateral, especially assignment of receivables by way of security). Some collateral instruments are of a highly accessory nature (lien on the receivables, for exsample), while others constitute typical non-accessory collateral models (fiduciary collateral, for exsample). Understanding the above mentioned legal nature of the instruments is more than necessary for adequate selection and use of specific models in practice.*

Key words • *fiduciary collateral, receivable, assignment of receivables by way of security, insolvency.*