FESTIVAL KVALITETA 2012

39. NACIONALNA KONFERENCIJA O KVALITETU

7. NACIONALNA KONFERENCIJA O KVALITETU ŽIVOTA

ZBORNIK ABSTRAKATA

7-9, jun, 2012, Kragujevac
Fakultet inženjerskih nauka u Kragujevcu

39. NACIONALNA KONFERENCIJA O KVALITETU
7. NACIONALNA KONFERENCIJA O KVALITETU ŽIVOTA

Zbornik abstrakata

ISBN: 978 - 86 - 86663 - 83 - 2

Urednici: ***Dr Slavko Arsovski,*** redovni professor,
Mašinski fakultet, Kragujevac
Dr Miodrag Lazić, redovni professor,
Mašinski fakultet, Kragujevac
Dr Miladin Stefanović, vanredni profesor
Mašinski fakultet, Kragujevac

Izdavač: **FAKULTET INŽENJERSKIH NAUKA**
34000 KRAGUJEVAC
Sestre Janjić 6

CENTAR ZA KVALITET
34000 KRAGUJEVAC
Sestre Janjić 6

Za izdavača: ***Prof. dr Miroslav Babić***
Prof. dr Slavko Arsovski

Tiraž: 200

Štampa: Grafički atelje ***Skver***, Kragujevac

Publication of Conference manual and organization of
Quality Festival 2012 is supported by:

Department of Education and Science,

Republic of Serbia

Izdavanje Zbornika radova, organizovanje i održavanje
Festivala kvaliteta 2012 podržalo je:

Ministarstvo za prosvetu i nauku, Republike Srbije

39. Nacionalna konferencija o kvalitetu

TEME:

- Kultura kvaliteta
- Sistem kvaliteta u javnoj upravi i javnim preduzećima

- Socijalne inovacije put ka društvenoj izvrsnosti
- Put ka poslovnoj izvrsnosti
- Integrisani menadžment sistemi
- Kretanje kvaliteta kroz organizaciju
- Kvalitet proizvoda
- Kvalitert i bezbednost u lancima hrane
- Inovacije u zdravstvu i kvalitet
- Liderstvo-potrebne veštine za biznis i komunikaciju
- Inovacije i kvalitet u turizmu
- Konkurentnost u 21. Veku
- Merenje, kontrola i kvalitet u proizvodnji
- Jačanjem procesa do unapreĎenja performansi
- Sistemi sertifikacije i kvalitet u procesu akreditacije

7. Nacionalna konferencija o kvalitetu života

TEME:

- Novi pogledi na kvalitet života i upravljanje resursima za život
- Merenje, vrednovanje i praćenje kvaliteta života
- Satisfakcija životom u inoviranom konceptu življenja
- Nov način razmišljanja i planiranja kvaliteta života
- Kvalitet životne sredine i zdravlje ljudi
- Zadovoljstvo sopstvenim životom
- Održivi razvoj i kvalitet života

- Trendovi kvaliteta života
- Kultura i kvalitet života
- Kapacitet planete i razvoj ljudske civilizacije
- Nova ljudska staništa i kvalitet života
- Rizici opstanka ljudske civilizacije

PROGRAMSKI ODBOR

1. Prof. dr Slavko Arsovski, Fakultet inženjerskih nuaka, Kragujevac, predsednik
2. Jurij Gusakov, European Organization for Quality (EOQ)
3. Jerry J. Mairani, The American Society for Quality (ASQ), SAD
4. Prof. Dr. Bernhard Müller, Leibniz Institute of Ecological and Regional Development, Dresden, Nemacka
5. Prof. dr Milan Perović, Mašinski fakultet, Podgorica, Crna Gora
6. Prof. dr Branislav Marjanović, Univerzitet Johanesburg, JAR
7. Prof. dr Goran Putnik, Univerzitet Minho, Portugal
8. Alena Plášková, Czech Society for Quality, Ceška
9. Mr Risto Lintula, Center for Excellence Finland, Finska
10. Matahiro Ueda, Japan Quality Assurance Organization (JQA), Japan
11. Prof. dr Mirko Soković, Fakultet za strojništvo Ljubljana, Slovenija
12. Božidar Ljubić, HDK-Hrvatsko društvo za kvalitetu, Hrvatska
13. Dr Predrag Injac, Oskar, Zagreb, Hrvatska
14. Prof. dr Ljupco Arsov, Elektrotehnicki fakultet Skoplje, Makedonija
15. Prof. dr Zdravko Krivokapić, Mašinski fakultet, Podgorica, Crna Gora
16. Prof. dr Miodrag Bulatović, Mašinski fakultet, Podgorica, Crna Gora
17. Prof. dr Mile Pešaljević, FON, Beograd
18. Prof. dr Dragan Cvetković, FZR, Niš
19. Prof. dr Miodrag Lazić, Fakultet inženjerskih nuaka, Kragujevac
20. Prof. dr Dobrica Milovanović, predsednik Supštine Grada Kragujevac

21. Prof. dr Nebojša Arsenijević, dekan, Medicinski fakultet, Kragujevac
22. Prof. dr Janko Hodolič, Fakultet tehnickih nauka, Novi Sad
23. Prof. dr Živadin Stefanović, Ekonomski fakultet, Kragujevac
24. Prof. dr Jovan Filipović, FON, Beograd
25. Prof. dr Zora Arsovski, Ekonomski fakultet, Kragujevac
26. Prof. dr Ljiljana Čomić, Prirodno matematicki fakultet, Kragujevac
27. Prof. dr Ljubo Zirojević, Fakultet za proizvodnju i menadžment, Trebinje
28. Prof. dr Gordana Mitić, Ekonomski fakultet, Kragujevac
29. Prof. dr Radovan Vukadinović, Pravni fakultet, Kragujevac
30. Dr Mirko Đapić, Mašinski fakultet, Kraljevo
31. Zoran Radojević, direktor, Grupa Zastava vozila
32. Dr Miljko Kokić, zamenik direktora, Grupa Zastava vozila
33. Miljko Erić, direktor, "Zastava automobili"
34. Dr Zoran Punoševac, predsednik AQS
35. Dr Ratko Uzunović, "VIBEX", Beograd
36. Dr Miloš Jelić, Akreditaciono telo SCG
37. Dr. Miladin Stefanović, Fakultet inženjerskih nuaka, Kragujevac
38. Dr Predrag Popović, Institut Vinca
39. Prof. dr Gordana Radosavljević, Beograd

FESTIVAL KVALITETA 2010

Dragi prijatelji kvaliteta ,

Festival kvaliteta 2012 ima zadatak da obezbedi meĎunarodni forum eksperata iz industrije i akademskih institucija sa ciljem razmene ideja i prezentovanja rezultata aktuelnih projekata kroz veliki izbor razlicitih tema.
pozivam Vas da učestvujete na 8-om Festivalu kvaliteta koji će se održati u Kragujevcu od 7. do 9. juna 2012. u Kragujevcu, Republika Srbija.
Festival se održava pod motom "Kvalitetom do poslovne izvrsnosti u javnom sektoru" i obuhvata dvekonferencije:

39. Nacionalna konferencija o kvalitetu
***7. Konferencija o kvalitetu** života.*
kao i više okruglih stolova.

Iskreno vaš,
Predsednik organiyacionog odbora
Festival Kvaliteta 2012
Prof. dr Slavko Arsovski

FQ2012
FESTIVAL
KVALITETA

SADRŽAJ:

Sadržaj 7

39. Nacionalna konferencija o kvalitetu 16

1. **KONTROVERZE SERTIFIKACIJE** 18
CONTROVERSIS OF SERTIFICATION
Milan Perović

2. **ZNANJE – KVALITET - VREDNOST** 19
KNOWLEDGE – QUALITY – VALUE
Slavko Arsovskić

3. **RAZVOJ NOVOG PRISTUPA UNAPREĐENJU KVALITETA** 20
DEVELOPMENT OF THE NEW APPROACH IN QUALITY IMPROVEMENT
Slavko Arsovski, Zora Arsovski, Miladin Stefanović , Aleksandar Đorđević

4. **LEAN FILOZOFIJA U FUNKCIJI UNAPREĐENJA SISTEMA OBRAZOVANJA** 21
LEAN CONCEPT AS A TOOL FOR EDUCATION SYSTEM IMPROVEMENT
Goran Manojlović, Ivan Mačužić, Branislav Jeremić, Slavko Arsovski

5. **LEAN SIX SIGMA KONCEPT** 22
LEAN SIX SIGMA CONCEPT
Vanja Rajković

6. **RADAR KONCEPT EFQM MODELA POSLOVNE IZVRSNOSTI** 23
RADAR CONCEPT OF EFQM EXELLENCE MODEL
Edin Kalač

7. **KVALITET U FUNKCIJI LOJALNOSTI:PROGRAMI LOJALNOSTI USLUŽNIH PREDUZEĆA U TURIZMU** 24
QUALITY AS A FUNCTION OF LOYALITY: LOYALITY PROGRAMS OF SERVICE COMPANIES IN TUORISM
Sofija Kovačević, Milena Ilić

8. **UNAPREĐENJE PROCESA U TELEKOMUNIKACIONIM KOMPANIJAMA** 25
IMPROVEMENT OF PROCESSES IN TELECOMMUNICATION COMPANIES
Slavko Arsovski, Zora Arsovski, Goran Marković, M. Dabetić

9. **VEZA IZMEĐU ELEMENATA MARKETING MIKSA I KVALITETA U TURIZMU** **26**
CONECTION BETWEEN MARKETING MIX ELEMENTS AND QUALITY IN TOURISM
Sofija Kovačević

10. **PLANIRANJE I PROVOĐENJE INTERNOG I EKSTERNOG AUDITA ISMS POMOĆU SOFTVERA AUDITMAN** **27**
PLANING AND CONDUCTING INTERNAL AND EXTERNAL AUDIT ISMS USING SOFTWARE AUDITMAN
Adelsberger Dejan, dr. Adelsberger Zdenko, dr. Buntak Krešimir

11. **AUDITIRANJE ISMS PREMA NORMAMA ISO 27 007 I ISO 27 008** **28**
AUDITING OF ISMS ACCORDING TO ISO 27 007 AND ISO 27 008
dr. Adelsberger Zdenko, dr. Buntak Krešimir, Adelsberger Dejan

12. **UTJECAJ KVALITETE PROIZVODA NA POSLOVANJE ORGANIZACIJE** **29**
IMPACT OF PRODUCTS QUALITY ON BUSINESS ORGANIZATIONS
dr. Krešimir Buntak, dr. Adelsberger Zdenko, dr. Ivan Nađ

13. **VIRTUALNA OBUKA I KONSULTACIJE** **30**
VIRTUAL TRAINING AND CONSULTATION
Kostić Radoslav

14. **KONCEPT OTVORENOG UČENJA I UČENJA NA DALJINU** **31**
CONCEPT OF OPEN LEARNING AND DISTANCE LEARNING
Ivona Zenović, Dragiša RanĎić, Ivan Bagarić

15. **EKSPERIMENTALNE METODE ISPITIVANJA I ANALIZE SPOSOBNOSTI PROCESA KAO SASTAVNI DEO AKTIVNOSTI UPRAVLJANJA KVALITETOM** **32**
EXPERIMENTAL METHODS TESTING AND ANALYSIS CAPABILITIES PROCESS AS PART IF THE QUALITY MANAGEMENT ACTIVITIES
Nikola M. Bralović, Petar Nikšić, Danka Kuzmanović

16. **UPRAVLJANJE PROCESIMA I KVALITETOM PROIZVODA** **33**
MANAGEMENT PROCESS AND PRODUCT QUALITY
Ivona Zenović, Dragiša RanĎić

17. **UPRAVLJANJE ULJIMA I MAZIVIMA U SKLADU SA ZAHTEVIMA STANDARDA ISO 14001 U ZP RUDNIK I TERMOELEKTRANA NA GACKO** **34**
TO MANAG OIL AND LUBRICANTS IN COMPABILITY WITH DEMANDS ISO 14001 STANDARD OF MINE AND POWER PLANT GACKO
Petar Nikšić, ĐorĎe Milović, Radmila Ivković

18. **ZNAČAJ INFORMATIČKIH TEHNOLOGIJA U MENADŽMENTU KVALITETOM** **35**
THE IMPORTANCE OF INFORMATION TECHNOLOGY IN QUALITY MANAGEMENT
Miloš Jovičić, Goran Zarić, Danijela Milovanović

19. **FAKTORI RIZIKA U UVOĐENJU KMS-A** **36**
INTRODUCTION RISK FACTORS IN A KMS
Miloš Petronijević, Ana Janković

20. **METODE ZA PROCENU RIZIKA ALE** **37**
ANNUAL LOSS EXPECTANCY (ALE)
Miloš Petronijević, Ana Janković

21. **ULOGA STEJKHOLDERA U UPRAVLJANJU RIZIKOM** 38
ROLE OF STAKEHOLDERS IN MANAGING RISK
Miloš Petronijević, Ana Janković

22. **KINESTATIČKI KONCEPT UPRAVLJANJA ZNANJEM I TQM–om: STUDIJA SKUČAJA** 39
KINESTATIC CONCEPT OF MANAGING WITH KNOWLEDGE AND TQM: CASE STUDY
Srđan Nikezić

23. **BSC KAO SISTEM MENADŽMENTA PERFORMANSAMA U ORGANIZACIJAMA** 40
BSC AS SZSTEM OF MANAGEMENT PERFORMANCES IN ORGANIZATIONES
Predrag Pravdić

24. **E-LIDERSTVO KAO REZULTAT MENADŽMENTA** 41
E-LEADERSHIP AS A RESULT OF MANAGEMENT
Predrag Pravdić

25. **KVALITETOM DO LIDERSTVA U DANAŠNJEM SVETU** 42
ACHIEVING LEADERSHIP IN TODAY'S WORLD BY QUALITY
Predrag Pravdić

26. **SAVREMENI PRINCIPI U KVALITETU ORGANIZACIJA** 43
MODERN PRINCIPLES IN QUALITY OF ORGANIZATIONS
Predrag Pravdić

27. **PRAKTIČNI PRIMJER PRIMJENE KONCEPTA „VLASNIŠTVO NAD PROCESIMA" KAO KOORDINISANA AKTIVNOST U VOĐENJU LUKE KOTOR** 44
PRACTICAL EXAMPLE OF APPLICATION OF THE CONCEPT "OWNER OF THE PROCESS" AS COORDINATED ACTIVITY TO DIRECT AND CONTROL OF PORT OF KOTOR
Pavle K. Popović

28. **RAZVOJ I INPLEMENTACIJA SOFTVERA ZA UPRAVLJANJE DQMS-A** 45
DEVELOPMENT AND IMPLEMENTATION OF SOFTWARE FOR MANAGING DQMS
Aleksandar Đorđević

29. **PROCESNI MODEL ORGANIZACIJE PRIVATNE ZAŠTITE U SVIJETU OUTSOURCINGA PREMA ISO 9001:2008** 46
PROCESS ORGANIZATION MODEL OF PRIVATE SECURITY IN LIGHT OF OUTSOURCING ACCORDING TO ISO 9001:2008
dr. Ivan Nađ, dr. Zdenko Adelsberger, dr. Krešimir Buntak

30. **KORIŠĆENI KVALITET REZULTATA PROCESA** 47
QUALITY OF USE
Branko Popović, Vitomir Bošković, Igor Nikodijević

31. **REALIZOVANJE I PROJEKTOVANJE U SISTEMU 6 SIGMA** 48
FOURTH STAGE IN SIX SIGMA
Branko Popović, Dragan Miletić, Igor Nikodijević

32. **UPRAVLJANJE POTROŠNJOM ODLIVAKA OTPORNIH NA HABANJE** 49
DEMAND MANAGEMENT CASTING ABRASION RESISTANT
Aleksandar Jovičić

33. KVALITET KAO DETERMINANTA RASTA IZVOZA POLJOPRIVREDNO –PREHRAMBENIH PROIZVODA REPUBLIKE SRBIJE **50**
QUALITY AS A DETERMINANT OF GROWTH IN EXPORTS OF AGRI-FOOD PRODUCTS OF REPUBLIC OF SERBIA
Raško Stefanović, Zoran Broćić

34. UNAPREĐENJE DIZAJNA OPREME ZA RECIKLAŽU ELEKTRONSKOG OTPADA **51**
DESIGN IMPROVEMENTS OF EQUIPMENT FOR ELECTRONIC WASTE RECYCLING
Lozica Ivanović, Danica Josifović, Blaža Stojanović, Andreja Ilić

35. PREVENTIVNIM MJERAMA DO POVEĆANJA SPOSOBNOSTI PROCESA **52**
WITH PREVENTIVE MEASURES TO PROCESS CAPABILITY IMPROVRMRNT
Radoslav Vučurević, Zdravko Krivokapić, Budimirka Marinković

36. PRILOG RECIKLIRANJU MATERIJALA U AUTO INDUSTRIJI I UGROŽAVANJE ŽIVOTNE SREDINE **53**
CONTRIBUTION TO RECYCLING MATERIALS IN AUTO INDUSTRY AND ENVIRONMENTAL THREAT
Snežana Vrekić

37. FKS NA POLJU KVALITETA **54**
FKS ON THE FIELD OF QUALITY
Novica Nešić, Zoran Simić

38. FAKTORI KOMPLEKSNOG ODRŽAVANJA U GRAĐEVINSKOJ MEHANIZACIJI **55**
FACTORS COMPLEX MAINTENANCE IN CONSTRUCTION MACHINERY
Dušan Đurović

39. MARKETING – KVALITET – ZADOVOLJSTVO KORISNIKA **56**
MARCETING – QUALITY – CUSTOMER SATISFACTION
Aleksandar Vujović, Zdravko Krivokpaić, Jelena Jovanović

40. MODEL KONKURENTNOSTI PREDUZEĆA U CENTRALNOJ SRBIJI **57**
COMPANY'S COMPETITIVENESS MODEL IN CENTRAL SERBIA
Aleksandra Kokić-Arsić, Slavko Arsovski, Jovan Milivojević, Ivan Savović, Katarina Kanjevac-Milovanović

41. EMC DIREKTIVA I KONKURENTNOST PROIZVODA **58**
EMC DIRECTIVE AND COMPETITIVNES
Katarina Kanjevac-Milovanović, Ivan Savović, Jovan Milivojević

42. MODELI PRIKUPLJANJA E-OTPADA **59**
MODELS OF COLLECTING E-WASTE
Bogdan Nedić

43. KVALITET PROCESA PROIZVODNJE DEMINERALIZOVANE VODE **60**
IMPROVEMENT OF QUALITY OF DEMINERALIZED WATER
Maja Angelovski, Jelena Čađenović Milovanović

44. ELEMENTI KORPORATIVNE KULTURE PODREĐENI KAPACITETU ZA OPORAVAK **61**
ELEMENTS OF CORPORATE CULTURE OFSUBORDINATED TO THE ORGANIZATIONAL RESILIENCE
Aleksandar Aleksić, Slavko Arsovski, Miladin Stefanović, Aleksandar Đorđević, Ivan Savović

45. **DEKOMPOZICIJA I METRIKA PROCESA PLANIRANJA NABAVKE** 62
DECOMPOSITION OF THE PROCUREMENT PLANNING PROCESS AND PROCESS METRIC
Snežana Nestić, Miladin Stefanović

46. **LIDERSTVO I KVALITET-STUDIJA SLUČAJA: TRAYAL KORPORACIJA** 63
LEADERSHIP AND QUALITIY-CASE STUDY: TRAYAL CORPORATION
Srđan Nikezić, Dragan Bataveljić

47. **KVALITET KROZ KONTRAPUNKT EFEKTIVNOG VERSUS TOKSIČKOG LIDERSTVA: STUDIJE SLUČAJA** 64
COUNTERPOINT THROUGH QUALITY EFFECTIVE VERSUS TOXIC LEADERSHIP: A CASE STUDY
Srđan Nikezić, Srđan Vladetić

48. **MEDICINSKI UREĐAJI, PRIMENA UPRAVLJANJA RIZIKOM NA MEDICINSKE UREĐAJE, VASKULARNI KALEMOVI** 65
MEDICAL DEVICES, THE APPLICATION OF RISK MANAGEMENT TO MEDICAL DEVICES, VASCULAR GRAFTS
Marko Rakić, Aleksandar Aleksić

49. **UNAPREĐENJE KVALITETA U JAVNOM SEKTORU PROJEKTNA FUNKCIJA U GRADSKOJ UPRAVI** 66
IMPROVING THE QUALITY IN PUBLIC SECTOR PROJECT MANAGEMENT FUNCTION IN THE CITY
Aleksandar Marić, Zoran Pavlović, Slavko Arsovski

50. **AUDITIRANJE PROCESA ZA UPRAVLJANJE RIZICIMA PREMA ISO 31000:2009** 67
PROCESS AUDITING FOR RISK MANAGEMENT BY 31000:2009
Zdenko Adelsberger

51. **KREIRANJE NOVE FILOZOFIJE I KULTURE KVALITETA** 68
CRETAE A NEW PHILOSOPHY AND CULTURE OF QUALITY
Jovan Milivojević, Aleksandra Kokić Arsić, Sonja Grubor, Ivan Savović, Katarina Kanjevac Milovanović

52. **SOCIJALNE INOVACIJE I DRUŠTVENA IZVRSNOST** 69
SOCIAL INNOVATIONS AND SOCIAL EXELLENCE
Jovan Milivojević, Ivan Savović, Sonja Grubor, Snežana Đokić Pešić, Nikola Tonić

53. **SISTEM MENADŽMENTA ZA BEZBEDNOST INFORMACIJA I MENADZMENT RIZIKA INFORMACIONIH SISTEMA U PREDUZEĆIMA** 70
THE MANAGEMENT SYSTEM FOR INFORMATION SECURITY AND RISK MANAGEMENT IN ENTERPRISE INFORMATION SYSTEMS
Predrag Pavdić, Marija Marković, Zoran Punoševac

7. Nacionalna konferencija o kvalitetu života 72

1. **INTEZITET KORIŠĆENJA REUSRSA BITNIH ZA ŽIVOT I OPSTANAK LJUDSKE VRSTE** 74
THE INTENSITY OF USE OF RESOURCES ESSENTIUAL FOR LIFE AND SURVIVEL OF HUMAN SPECIES
Jovan Milivojević, Aleksandra Kokić Arsić i Katarina Milovanović Kanjevac

2. **FILOZOFIJA KVALITETA ŽIVOTA I ODRŽIVOSTI LJUDSKE ZAJEDNICE** **75**
PHILOSOPHY LIFE OF QUALITY AND SUSTAINABILITY OF HUMAN SOCIETY
Jovan Milivojević, Aleksandra Kokić Arsić, Sonja Grubor, Ivan Savović i Katarina Milovanović Kanjevac

3. **NAUKA I TEHNOLOGIJE U FUNKSIJI KVALITETA ŽIVOTA** **76**
SCIENCE AND TECHNOLOGY IN FUNCTION OF THE QUALITY OF LIFE
Jovan Milivojević, Aleksandra Kokić Arsić, Sonja Grubor, Ivan Savović i Aleksandar Aleksić

4. **KVALITET ŽIVOTA I GLOBALNE KATASTROFE** **77**
QUALITY OF LIFE AND GLOBAL CATASTROPHE
Jovan Milivojević, Aleksandra Kokić Arsić, Sonja Grubor, Ivan Savović i Aleksandar Aleksić

5. **ZADOVOLJSTVO ŽIVOTOM – KLJUČNI ASPEKTI** **78**
LIFE SATISFACTION – KEY ASPECTS
Jovan Milivojević, Aleksandra Kokić Arsić, Sonja Grubor, Ivan Savović i Nikola Tonić

6. **KVALITET ČOVEKA I KVALITET ŽIVOTA –NAJVIŠI NIVO KVALITETA** **79**
QUALITY OF MAN AND QUALITY OF LIFE – HIGHEST LEVEL OF QUALITY
Ljilja Berežljev

7. **MENADŽMENT TOTALNOG KVALITETA (MTK) U SISTEMU OBRAZOVANJA – KREATIVAN PRISTUP** **80**
TOTAL QUALITY MANAGEMENT (ICC) IN THE EDUCATION SYSTEM – A CREATIVE APPRAOCH
Ljilja Berežljev

8. **UNAPREĐENJE SNABDEVANJA VODOM SEOSKIH DOMAĆINSTAVA U OKOLINI GRADA KRAGUJEVCA** **81**
IMPROVEMENT OF WATER SUPPLY OF VILLAGE HOUSEHOLDS NEAR THE CITY OF KRAGUJEVAC
Slibodan Savić, Snežana Živanović Katić i Saša Jovanović

9. **NEKE MOGUĆNOSTI POVEĆANJA ENERGETSKE EFIKASNOSTI ZATVORENOG BAZENA SPORTSKOG CENTRA PARK U KRAGUJEVCU** **81**
POSSIBILITIES TO INCREASE ENERGY EFFICIENCY OF THE INDOOR SWIMMING POOL AT THE SPORT CENTRE PARK IN KRAGUJEVAC
Aleksandra Vulović, Nikola Jovanović, Slobodan Savić i Dušan Gordić

10. **UNAPREĐENJE SNABDEVANJA VODOM SEOSKIH DOMAĆINSTAVA U OKOLINI GRADA KRAGUJEVCA** **82**
IMPROVEMENT OF WATER SUPPLY OF VILLAGE HOUSEHOLDS NEAR THE CITY OF KRAGUJEVAC
Aleksandra Vulović, Nikola Jovanović, Slobodan Savić i Dušan Gordić

11. **PRISTUP DEFINISANJU OPTIMALNOG TEHNOLOŠKOG PORTFOLIA ZA RECIKLAŽU ELV** **83**
AN APPROACH TO DEFINE OPTIMAL TECHNOLOGIES PORTFOLIO OF ELV RECYCLING
Slavko Arsovski, Danijela Tadić, Sonja Grubor, Aleksandar Đorđević

12. **IZVORI ZAGAĐENJA VODENOG EKOSISTEMA NA REGIONALNOM NIVOU OTPADOM OD AUTO INDUSTRIJE** **84**

SOURCES OF POLLUTION OF WATER ECOSYSTEMS ON DISTRICT LEVEL WASTE OF AUTO INDUSTRY
Srećko Ćurčić, Sandra Milunović, Dragan Filipović

13. **RAZVOJ SISTEMA ZA PRAĆENJE PORTFOLIA TEHNOLOGIJA RECIKLAŽE ELV** **85**
DEVELOPMENT OF MONITORING SYSTEM FOR ELV PORTFOLIO RECYCLING TECHNOLOGIES
Zora Arsovski, Slavko Arsovski, Aleksandra Kokić-Arsić, Aleksandar Đorđević

14. **PRISTUP PRAČENJU I IZMENAMA PORTFOLIJA TEHNOLOGIJA RECIKLAŽE ELV** **86**
AN APPROACH TO MONITOR AND CHANGE THE TECHNOLOGY PORTFOLIO OF ELV RECYCLING
Slavko Arsovski, M. Pavlović, Miodrag Lazić, Aleksandar Đorđević

15. **PRISTUP PRAČENJU I IZMENAMA PORTFOLIJA TEHNOLOGIJA RECIKLAŽE ELV** **87**
AN APPROACH TO MONITOR AND CHANGE THE TECHNOLOGY PORTFOLIO OF ELV RECYCLING
Ivan Savović, Aleksandra Kokić-Arsić, Katarina Kanjevac-Milovanović, Aleksandar Đorđević

16. **MERENJE PERFORMANSI ZDRAVSTVENOG SISTEMA** **88**
MEASURING THE PERFORMANCE OF HEALTH SYSTEMS
Ivan Savović, Zorica Savović, Aleksandra Kokić-Arsić, Rajko Šofranac

AUDITIRANJE ISMS PREMA NORMAMA ISO 27007 I ISO 27008

AUDITING OF ISMS ACCORDING TO ISO 27007 AND ISO 27008

mr Zdenko Adelsberger[1)], dr Krešimir Buntak[2)]
Dejan Adelsberger[3)]

Rezime: *Upravljanje informacijskom sigurnošću (ISMS) je jedno od najpropulzivnijih područja razvoja sistema upravljanja. Često izdavanje novih normi, praktički svake godine barem jedna do dvije nove norme, ukazuju da se to područje intenzivno razvija i u ISO projekcijama u području ISMS bit će najviše normi, u glavnom u obliku preporuka. U tu kategoriju svakako spadaju novoobjavljene norme ISO 27007:2011 i ISO 27008:2011. Obadvije norme se odnose na proces provođenja provjere (audita) ISMS i to posebno za zahtjeve norme ISO 27001, a posebno za provjeravanje kontrola iz aneksa A norme ISO 27001. U okviru rada kritički se obrađuju pristupi provjeri ISMS-a prema preporukama normi ISO 27007 i ISO 27008 te analizira njihov značaj za kvalitetno i ujednačeno provođenje procesa provjere.*
Ključne riječi: *provjera, informacijska sigurnost, ISMS, ISO 19011, ISO 27007, ISO 27008*

Abstract: *Information security management (ISMS) is one of the most propulsive areas of development management system. Frequently issuing new standards, virtually every year at least one or two new standards, indicate that this area is intensively developed in ISO projections and in the ISMS will be the highest number of standards, mainly in the form of recommendations. In this category the newly published ISO 27007:2011 and ISO 27008:2011 belong. Both standards relating to the process of carrying out checks (audits), ISMS, especially for the requirements of ISO 27001, and in particular for checking the controls in Annex A standard ISO 27001. This paper will show how to audit ISMS according to standards ISO 27007 and ISO 27008, and how to analyze their significance and consistent implementation of the review process.*
Key Words: *audit, information security, ISMS, ISO 19011, ISO 27007, ISO 27008*

1. UVOD

Potrebne provjere (auditiranja) ISMS-a vežu se u prvom redu za ispunjenje zahtjeva standarda ISO/IEC 27001:2005. U navedenom standardu se u poglavlju 6 – Interne provjere ISMS definira obaveza provođenja provjera u cilju da se u planiranim intervalima ustanovi da ciljevi kontrola, kontrole, procesi i procedure uspostavljenog ISMS-a:

a) Zadovoljavaju zahtjeve ovog međunarodnog standarda, kao i relevantne zakone i propise,
b) Zadovoljavaju prepoznate zahtjeve informacijske sigurnosti,
c) Utvrđivanju da li je implementacija provedena učinkovito i održavana, te
d) Da li se ciljevi izvršavaju kako se od njih očekuje.

Način provođenja provjera se temelji na implementaciji procesa provjere koji je opisan u standardu ISO 19011:2011. U okviru ovog standarda se definira da je provjera (audit) sistematičan, nezavisan i dokumentiran proces za dobivanje dokaza provjere i njegovo objektivno vrednovanje da bi se utvrdio stupanj do kojeg su ispunjeni kriteriji provjere. Pri tome se napominje da se interne provjere obično nazivaju "provjere prve strane" i obavlja ih sama organizacija, ili se obavljaju u njeno ime u svrhu preispitivanja koje vrši rukovodstvo i za ostale interne potrebe (npr. za potvrđivanje efektivnosti sistema menadžmenta ili za dobivanje informacija za poboljšavanje sistema menadžmenta, itd.). Interne provjere za organizaciju mogu predstavljati temelj za samo-ocjenjivanje o usuglašenosti. U mnogim slučajevima, nezavisnost se pokazuje time što auditor nije odgovoran za aktivnosti koje se auditiraju. Pored toga, navedeni standard kaže, eksterne (vanjske) provjere obuhvaćaju ono što se obično naziva "provjera preko druge strane" i "provjera preko treće strane". Provjere preko druge strane obavljaju strane koje imaju interesa u organizaciji, kao što su korisnici ili druge osobe u njihovo ime. Provjere preko treće strane obavljaju eksterne, nezavisne organizacije, kao one koje obavljaju certifikaciju, odnosno certifikacijske kuće.

Kada se vrši zajedničko provjeravanje dva ili više sistema upravljanja iz različitih područja (npr. kvaliteta - QMS, zaštita okoliša - EMS, sigurnost i zdravlje na radu – OHSAS, informacijske sigurnosti – ISMS, itd.), prema ISO 19011:2011 to se naziva "kombinirana provjera", odnosno kombinirani audit.

Kada dvije ili više organizacija za audit surađuju na provjeri iste provjeravane organizacije,

1) mr Zdenko Adelsberger, Bluefield d.o.o., Zagreb, HR, mail: zadelsbe@zg.t-com.hr
2) dr Krešimir Buntak, Tehničko veleučilište Varaždin, mail: kresimir.buntak@inet.hr
3) Dejan Adelsberger, Bluefield d.o.o., Zagreb, HR, mail: dejan@bluefield.hr

to ISO 19011:2011 naziva "zajednička provjera", odnosno „zajednički audit“.

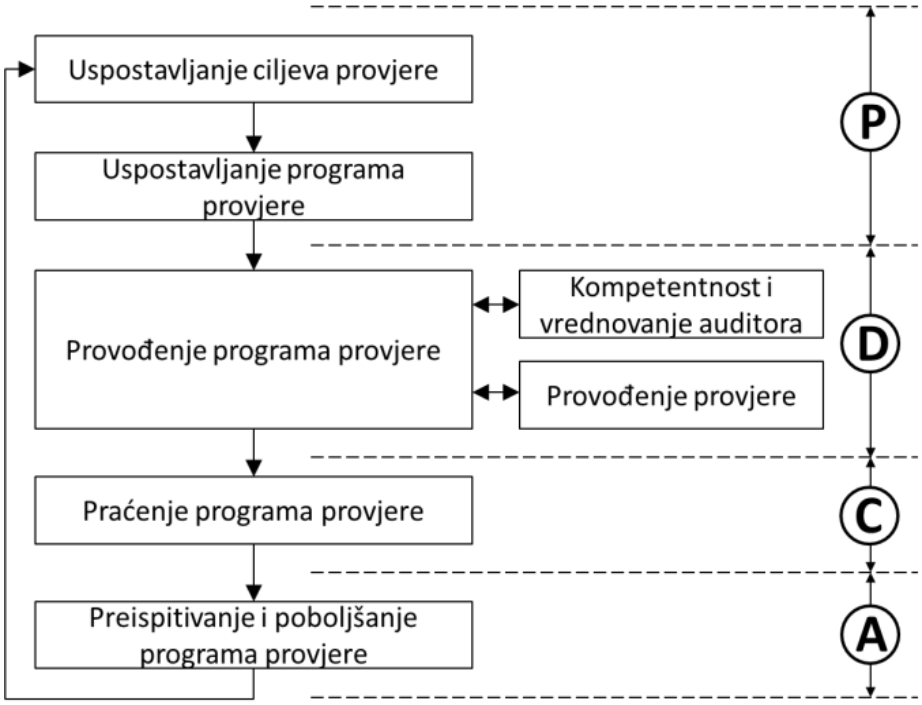
Prema gore navedenom, ISO 19011:2011 definira generički proces za planiranje, provođenje i naknadno postupanje s provjerama svih vrsta. Zavisno od organizacije koja provodi provjeru i svrhe za koju se provodi provjera, načini tehnički provedbe pojedinih procesnih koraka provjere razlikuju se u većoj ili manjoj mjeri.

Premda standard ISO 19011:2011 ima kategoriju upute, odnosno neobaveznosti primjene, predstavlja izraz najbolje prakse i općenito prihvaćeni proces za provođenje provjere. Na njega se referenciraju svi drugi ISO standardi koji traže bilo kakav oblik provjere, pa je u najmanju ruku nezamislivo ne držati se njega za planiranje i provedbu provjere. Kako u pojedinim sistemima upravljanja može biti značajnih specifičnosti koje se ne pojavljuju u nekim drugim nameće se stav da i provjere ne moraju biti iste. Upravo je to slučaj sa sistemom upravljanja informacijskom sigurnošću ISMS, koji je toliko specifičan i sveobuhvatan te nizom nezaobilaznih područja da opći generički proces za provjere nije dovoljan. U tom cilju za provođenje provjere ISMS-a objavila su se dva nova standarda ISO/IEC 27007:2011 i ISO/IEC TR 27008:2011.

U nastavku će se prikazati glavne značajke standarda ISO 19011, te specijalnih standarda ISO 27007 i ISO 27008, kao i uputa na razlike i značaj provođenja provjera prema ova dva posljednja.

2. PROVJERE TEMELJENE NA ISO 19011:2011

Međunarodni standard ISO 19011:2011, kako je već rečeno, je uputa za provjeravanje sistema upravljanja, a uključuje principe provjeravanja, upravljanje programima provjere i provođenje provjera, kao i upute za vrednovanje kompetentnosti pojedinaca uključenih u proces provjeravanja, ali i osobe za upravljanje programima provjere, auditore i timove auditora. Standard je primjenljiv na sve vrste organizacija koje imaju potrebu provedbe internog ili eksternog audita. Blok shema organizacije procesa za provjeru prema ISO 19011:2011 prikazana je na slici 1.



Slika 1 - Blok shema procesa provjere prema ISO 19011:2011

Sadržaj standarda ISO 19011:2011 prikazan je u tablici 1. Iz njega je vidljivo da se u samom standardu obrađuju sve relevantne teme vezane za uspostavljanje, provođenje i poboljšanje procesa audita. U okviru standarda se definira i minimalna potrebna dokumentacija kojom se dokazuje pristup i provođenje aktivnosti vezanih za auditiranje.

Kod certifikacijskih kuća standard ISO 19011:2011 služi kao uputa za generiranje glavnog (Core) poslovnog procesa provjere partnerske strane, a kod internih provjera spomenuti standard je osnova za generiranje pomoćnog procesa, odnosno obavezne procedure internih provjera, a koja se nalazi kao eksplicitni zahtjev u svim ISO certifikacijskim standardima.

Tablica 1. Sadržaj standarda ISO 19011:201

Predgovor
Uvod
1. Predmet i područje primjene
2. Normativne reference
3. Termini i definicije
4. Principi provjeravanja
5. Menadžment programom provjere
5.1 Opće odredbe
5.2 Uspostavljanje ciljeva programa provjere
5.3 Uspostavljanje programa provjere
5.4 Provođenje programa provjere
5.5 Praćenje programa provjere
5.6 Preispitivanje i poboljšavanje programa provjere
6. Provođenje provjere
6.1 Opće odredbe
6.2 Iniciranje provjere
6.3 Pripremanje aktivnosti provjere
6.4 Provođenje aktivnosti provjere
6.5 Priprema, odobravanje i distribucija izvještaja o provjeri
6.6 Završetak provjere
6.7 Obavljanje naknadne provjere
7. Kompetentnost i vrednovanje auditora
7.1 Opće odredbe
7.2 Utvrđivanje potrebne kompetentnosti auditora da ispuni program provjere
7.3 Uspostavljanje kriteriji za vrednovanje auditora
7.4 Izbor odgovarajuće metode za vrednovanje auditora
7.5 Provođenje vrednovanja auditora
7.6 Održavanje i poboljšavanje kompetentnosti auditora
Prilog A (informativan) Uputa i ilustrativni primjeri za znanje i vještine auditora za specifične discipline
Prilog B (informativan) Dodatne upute za auditore za planiranje i provođenje provjere
Bibliografija

Procesom provjere prema ISO 19011:2011, bez obzira u koju svrhu i za koji sistem upravljanja se primjenjuje, upravlja se preko PDCA kruga, što je jasno prikazano na slici 1.

Bitna razlika između najnovije revizije ISO 19011:2011 i prethodne iz 2002 godine je u tome što je standard i formalno proglašen primjenljiv za sve sisteme upravljanja, a ne samo za sisteme upravljanja kvalitetom i zaštitom okoliša kako je bilo ranije. Ostale promjene u novoj reviziji su korektivne prirode, odnosno preciznijih postavki.

3. PROVJERE ISMS-A TEMELJENE NA ISO/IEC 27007:2011 I ISO/IEC 27008:2011

Kao što je već rečeno, informacijski sistem, odnosno sistem za upravljanje sigurnošću informacija se u praksi pojavljuje kao jedan od najsloženijih i sistema upravljanja. Uz to, za njega postaje sve više svijesti da je jedan od ključnih sistema upravljanja za sve ostale. Naime, informacija kao resurs postoji u svakoj organizaciji, u svakom sistemu upravljanja (QMS, EMS, OHSAS, FSMS, itd.) informacija je eksplicitno navedena kao ključan resurs. U svim sistemima upravljanja navode se zahtjevu u području upravljanja resursima: očuvanje resursa u svakom aspektu, te pravilna upotreba resursa. Kada se govori o informacijama kao resursu, tada se pod informacijom smatraju svi podaci koji u nekom kontekstu imaju neku vrijednost za vlasnika i/ili korisnika informacije. Prema ISO 27001:2005 postoje tri aspekta informacijske sigurnosti, i to:

- očuvanje tajnosti informacije (do informacije i njene upotrebe mogu doći samo ovlašteni korisnici)
- očuvanje cjelovitosti informacije (informacija u formi i sadržaju se ne smije promijeniti bez znanja vlasnika informacije, što uključuje i metode i postupke obrade informacija), i
- osiguranje dostupa do informacije (do informacije moraju moći doći svi ovlašteni korisnici tamo gdje i kada im treba u prihvatljivom obliku).

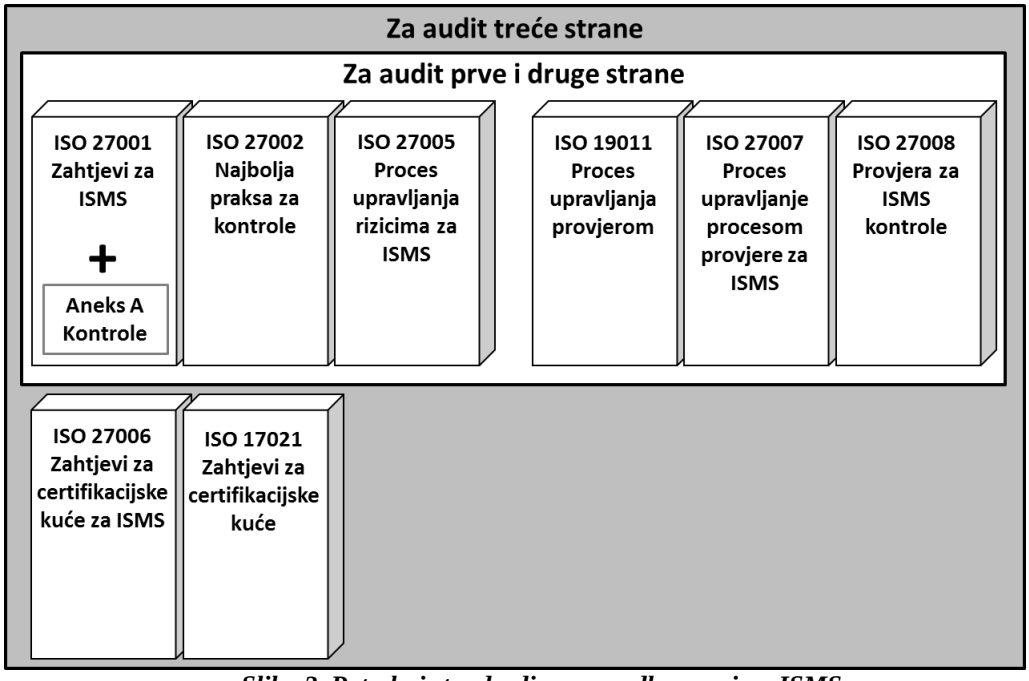
Obično se u području informacijske sigurnosti to označava kao očuvanje C-I-A ili CIA, gdje je CIA akronim od engleskih riječi: Confidentiality,

Integrity i Availability (u prijevodu označavaju tajnost, cjelovitost i dostupnost).

Prema definiciji se pod sistemom upravljanja informacijskom sigurnošću (ISMS) podrazumijeva dokumentirani proces koji uz pomoć resursa i pravila osigurava ispunjenje zahtjeva očuvanja aspekata informacijske sigurnosti CIA. Taj proces, za ostvarenje planiranih ciljeva, zahtjeva u organizaciji niz novih organizaciono-funkcionalnih pristupa, najčešće i nove resurse, ali obavezno niz novih znanja i vještina te podizanja svijesti o informacijskoj sigurnosti svih sudionika. Zbog toga, osim časnih izuzetaka, u svim firmama gdje trema implementirati ISMS, ako se želi stvarna korist od njega, treba provesti mnoge aktivnosti donijeti vrlo stručna rješenja. To predstavlja u pravilu vrlo naporan rad i bez apsolutne podrške vrhovne uprave je ne provediv postupak sa rezultatima koji u cjelini ne zadovoljavaju. Zbog toga se za provođenje certifikacije ISMS-a i priznavanje efikasno uspostavljenog sistema informacijske sigurnosti mora pristupiti poštujući sve ono što je značajno i važno za ostale sisteme upravljanja plus niz dodatnih stručnih analiza i provjera. Ta specifičnosti nisu eksplicitno navedene u standardu ISO 19011:2011 (mada ih niti ne isključuju). U tom cilju su i objavljena dva nova standarda ISO/IEC 27007:2011 (Guidelines for information security management systems auditing) i ISO/IEC 27008:2011 (Guidelines for auditors on information security controls).

Objavljivanje dva standarda za provođenje provjere ISMS-a je posljedica razlike standarda ISO 27001:2005 i ostalih standarda sa zahtjevima. Naime, ISO/IEC 27001:2005 ima dva dijela. U glavnom dijelu su navedeni svi zahtjevi koje se mora ispuniti ako se želi certifikat, a dodatak A je normativni , što znači obavezan za primjenu kod implementacije ISMS-a. To ga čini različitim od ostalih certifikacijskih standarda, koji nemaju takav noramativni, već samo neobavezne informativne dodatke. Normativni dodatak A (Control objectives and controls) daje popis sigurnosnih područja (11) sa definiranim ciljevima (39) i kontrolama (133) kojima se ti ciljevi mogu ostvariti. Pod pojmom kontrola se podrazumijeva sigurnosna mjera ili protumjera s kojom se smanjuje razina rizika informacijske sigurnosti. Ne provođenje neke od kontrola zahtjeva da korisnik eksplicitno objasni u pisanoj formi zašto ne koristi kontrolu, i to za svaku ne korištenu kontrolu posebno.

Za provedbu provjere ISMS-a bilo koje strane potreban je niz standarda kojih se trebaju pridržavati i primjenjivati kako tijela koje provode provjeru, tako i auditori. Na slici 2. su prikazani standardi koji su potrebni za provedbu provjere ISMS.



Slika 2. Potrebni standardi za provedbu provjere ISMS-a

Standard ISO 27001 je obvezujući za organizaciju koja želi provesti certifikaciju svog ISMS-a, a ISO 27006 i ISO 17021 su obvezujući standardi za certifikacijske kuće koje se žele akreditirati za certifikaciju ISMS.

Važno je naglasiti da je standard ISO/IEC 27007:2011 u potpunosti usklađen sa standardom

ISO 19011:2011. Objektivno se standard ISO/IEC 27007:2011 ne može koristiti ako korisnik nema i tekst standarda ISO 19011:2011. Naime, na niz mjesta u ISO/IEC 2707:2011 stoji tekst „Primijenite uputu iz ISO 19011:2011, Klauzula x.y.z“. No, na niz mjesta gdje se traži neka specifičnost vezana za provjeru ISMS-a u standardu se nalazi dodatna uputa ili preporuka koja se može shvatiti kao zahtjev. Tako npr. može se pokazati za ilustraciju mogu poslužiti tablica 2.

Tablica 2. Primjer usporedbe teksta standarda ISO 19011:2011 i ISO/IEC 27007:2011

Sadržaj ISO 19011:2011
…
7.2.4 Postizanje kompetentnosti auditora Znanje i vještine auditora mogu se steći korištenjem kombinacije slijedećeg: – zvaničnog obrazovanja/obuke i iskustva koje doprinosi razvoju znanja i vještina auditora u sistemu menadžmenta za discipline i oblasti koje namjerava da provjerava; – programa obuke koji obuhvaćaju generičko znanje i vještine auditora; – iskustva na relevantnoj tehničkoj, menadžerskoj ili profesionalnoj poziciji, uključujući prakse u prosuđivanju, donošenju odluka, rješavanju problema i komuniciranju sa rukovoditeljima, profesionalcima, kolegama, korisnicima i ostalim zainteresiranim stranama; – iskustva stečenog u provođenju provjere pod nadzorom auditora u istoj disciplini.
7.2.5 Vođe tima auditora
…
Sadržaj ISO 27007:2011
…
7.2.4 Postizanje kompetentnosti auditora Primijenite uputu iz ISO 19011:2011, Klauzula 7.2.4. Pored toga primijenite i slijedeće ISMS specifičnosti.
7.2.4.1 IS 7.2.4 Postizanje kompetentnosti auditora ISMS auditori trebaju imati znanje i vještine za informacijske tehnologije i informacijsku sigurnost, što dokazuju pomoću relevantnih certifikata, a pored toga bi trebali biti u stanju razumjeti pojedine poslovne zahtjeve. ISMS auditorima radno iskustvo bi trebalo također pridonijeti razvoju njihovih znanja i vještina u području ISMS.
7.2.5 Vođe tima auditora
…

Takvih i sličnih dodataka u ISO/IEC 27007:2011 u odnosu ima ISO 19011:2011 ima niz. Neki od tih dodataka su vrlo obimni i otežavaju provjeru ISMS-a, ali primjena tih specifičnosti osigurava bolju i realniju ocjenu provjeravanog ISMS-a.

Dodatna značajka standarda ISO/IEC 27007:2011 je Aneks A koji daje vrlo precizne upute kako praktički provesti provjeru ISMS. Taj dodatak standardu ima 9 dijelova u kojima su prikazane specifičnosti provjere ISMS-a. Ti dijelovi su prikazani u tablici 3.

Tablica 3. Dijelovi aneksa A standarda ISO/IEC 27007:2011

A.1. ISMS opseg, politika i pristup procjeni rizika
A.2. Identifikacija rizika, analiza i evaulacija, identifikacija opcija obrade rizika
A.3. Odabir kontrolnih ciljeva i kontrola, odobrenje za preostale rizike, autorizacija izjave o primjenljivosti (SoA)
A.4. Implementacija i funkcioniranje ISMS-a
A.5. ISMS nadzor i izvještavanje
A.6. ISMS održavanje i poboljšanje
A.7. ISMS dokumentacija
A.8. Odgovornost menadžmenta
A.9. Interna provjera ISMS i upravina ocjena ISMS

Svaki taj dio aneksa ima definiranu strukturu koja ima oblik prikazan u tablici 4.

Tablica 4. Struktura dodatka A u ISO/IEC 27007:2011 za provjeru nekog dijela ISMS-a

A.x naziv dijela za provjeru ISMS-a	
Kriteriji provjere	Popis zahtjeva koji se moraju zadovoljiti u konkretnom dijelu
Relevantni standardi	Popis svi relevantnih standarda i točaka u njima koje su vezane za provjeru konkretnog dijela
Praktična uputa za provedbu provjere	Detaljan opis kao provesti i sve relevantne napomene vezane za najbolju praksu provjere zahtjeva vezanih za konkretan dio provjere ISMS.

Prema zahtjevima definiranim u ISO/IEC 27001:2005 za uspostavu i certifikaciju ISMS-a nije predviđen priručnik, što se eksplicitno zahtjeva npr. kod implementacije sistema upravljanja kvalitetom prema ISO 9001:2008. To bi moglo značajno usložiti, odnosno produžiti provjeru ISMS-a, pa većina certifikacijskih kuća prije provođenja provjere prvog stupnja (First Stage Audit) pošalju korisniku upitnik sa detaljnim pregledom zahtjeva prema ISO/IEC 27001:2005 u kojega korisnik za svaki zahtjev mora upisati referencu na dokument (ili dokumente) s kojima se

dokazuje ispunjenje nekog zahtjeva, ili objašnjenje zašto neki od zahtjeve nisu ispunjeni.

Za razliku od ISO 27007 koji je nadopuna na ISO 19011 u podruju ISMS, standard ISO/IEC 27008:2011 je potpuno novi dodatak za provjeru ISMS-a i jedini kao takav u usporedbi sa svim ostalim sistemima upravljanja, odnosno, tako nešto drugi sistemi upravljanja nemaju predviđeno za provjeru. Standard ISO/IEC TR 27008:2011 koji ima naziv: Uputa za provjeru kontrola informacijske sigurnosti je u biti tehnički izvještaj (TR) kojemu je namjena tehnička provjera usklađenosti kontrola informacijskog sistema s utvrđenim standardima organizacijske informacijske sigurnosti. Ovaj TR odnosi se na sve vrste i veličine organizacija, uključujući i javna i privatnih poduzeća, državna poduzeća kao i neprofitne organizacije, a daje mišljenja o tehničkoj usklađenosti na temelju provjere. Ovaj TR nije namijenjen za upravljanje provjerama sistema (auditima). Sadržaj standarda ISO/IEC TR 27008:2011 prikazan je u tablici 5.

Tablica 5. Sadržaj standarda ISO/IEC TR 27008:2011

Predgovor
Uvod
1. Opseg
2. Normativne reference
3. Nazivi i definicije
4. Struktura ovog tehničkog izvješća
5. Pozadina
6. Recenzija pregleda kontrola informacijske sigurnosti
6.1 Pregled procesa
6.2 Resourcing
7. Pregled metoda
7.1 Pregled
7.2 Metoda pregleda: ispitivanje
7.3 Metoda pregleda: intervju
7.4 Metoda pregleda: test
8. Aktivnosti
8.1 Pripreme
8.2 Izrada plana
8.3 Provođenje recenzije
8.4 Analize i izvješćivanja
Dodatak A (informativno) praktična uputa tehničkog pridržavanje provjere
Dodatak B (informativno) inicijalno prikupljanje informacija (osim IT)
B.1 Ljudski resursi i sigurnost
B.2 Politike
B.3 Organizacija
B.4 Fizička i sigurnost okoliša
B.4.1 Da li su lokacije sigurne za informacije?
B.4.2 Da li su lokacije sigurne za ICT? (aspekti zaštite okoliša)
B.4.3 Da li su lokacije sigurne za ljude?
B.5 Upravljanje incidentima
Bibliografija

U samom standardu se vrlo detaljno opisuje pristup, tehnike i metode provjere implementiranih kontrola ISMS-a organizacije. Tu provjeru mogu u biti raditi kompetentni auditori, odnosno stručnjaci koji imaju znanja, vještine i iskustva u praktičnoj primjeni planiranih aktivnosti te resursa potrebnih za implementaciju i provođenje konkretne kontrole.

4. Zaključak

Planiranje i provođenje provjere ISMS-a je jedan od najsloženijih vrsta provjera sistema upravljanja jer zahtjeva ne samo dobro poznavanje zahtjeva certifikacijskog standarda ISO 27001, već i niza drugih uputa, sa velikim stručnim znanjem i praktičnim iskustvom auditora i područjima tehničke realizacije sigurnosti informacija. Poseban je naglasak na područje znanja i vještina u području IT-a. Za razliku od menadžera ISMS, za kojega nije bitno kojeg je općeg i stručnog obrazovanja ako ima menadžerska znanja i vještine, za auditora je stvar potpuno drugačija. Auditor mora biti izuzetno dobar poznavalac IT tehnologije i informacijskih sistema. To stvara u praksi dosta problema. Tako npr. u koliko se želi napraviti kvalitetan interni audit, može se pokazati da organizacije uopće nemaju ili imaju nedovoljno stručnog kadra koje ima koristi obučiti za interne auditore ISMS-a, a da ne dođe do sukoba interesa i nestručnih (čitaj beskorisnih) provjera. Obuke u firmama po principu „bilo-koga“ za interne auditore u trajanju 2-3 dana i to bez formalne kvalifikacije posebno u IT području je objektivno formalizam koji ne doprinosi objektivnoj ocjeni ISMS-a, a time i uvjerenju da ISMS zadovoljava osnovnu funkciju i smisao: očuvanje CIA, odnosno, aspekata informacijske sigurnosti. Što se tiče certifikacijskih kuća koje su akreditirane za certifikaciju ISMS-a one su u stanju osigurati kompetentne auditore koji mogu obaviti kvalitetnu provjeru ISMS-a. U svakom slučaju, za provjeru ISMS-a svi auditori moraju izuzetno dobro baratati zahtjevima, uputama i imati dovoljno prakse za sve elemente definirane kroz standarde prikazane na slici 2, ali i niza drugih koji nisu tu navedeni.

Literatura

[1] ISO/IEC 27000:2009 Information technology — Security techniques — Information security management systems — Overview and vocabulary
[2] ISO/IEC 27001:2005 Information technology — Security techniques —

Information security management systems — Requirements
[3] ISO/IEC 27002:2005 Information technology — Security techniques — Code of practice for information security management
[4] ISO/IEC 27005:2011 Information technology — Security techniques — Information security risk management
[5] ISO/IEC 27006:2007 Information technology — Security techniques — Requirements for bodies providing audit and certification of information security management systems
[6] ISO/IEC 27007:2011 Information technology — Security techniques — Guidelines for information security management systems auditing
[7] ISO/IEC TR 27008:2011 Information technology — Security techniques — Guidelines for auditors on information security controls
[8] ISO 19011:2011 Guidelines for auditing management systems
[9] ISO/IEC 17021:2011 Conformity assessment -- Requirements for bodies providing audit and certification of management systems