



PLANIRANJE I PROVOĐENJE PROCESA AUDITIRANJA SUSTAVA UPRAVLJANJA POMOĆU PROGRAMA AUDIT MAN

Dejan Adelsberger, Zdenko Adelsberger, Krešimir Buntak¹

Rezime: *Proces auditiranja sukladno danim normama konceptijski nije doživio velike promjene. Ono što se mijenja je tehnologija uz pomoću koje se može organizirati i provoditi proces audita. Ovaj rad prikazuje mogućnost auditiranja različitih sustava upravljanja kao što su ISO 9001, ISO 14001, ISO 18001, ISO 27001, ISO 31000 i dr. pomoću programa AUDIT MAN koji je baziran na WEB tehnologiji i omogućuje planiranje i provođenje audita, te izradu kompletne dokumentacije vezane za proces auditiranja.*

Ključne riječi: *sustavi upravljanja, auditiranje, program AUDIT MAN, moderne tehnologije*

1. UVOD

Danas se auditiranje sustava upravljanja može provoditi na tri različita načina: samostalni sustav upravljanja ili kombinirani sustav upravljanja, odnosno kako se obično naziva šingrirani sustav upravljanja. Kada govorimo o samostalnom sustavu upravljanja tada najčešće govorimo o jednom sustavu kao što je ISO 9001, ISO 14001, ISO/IEC 20000, ISO/IEC 27001, itd. Kod kombiniranog sustava upravljanja u jednoj organizaciji ima dva ili više sustava upravljanja u nekoj kombinaciji kao npr. ISO 9001 + ISO 14001, ili ISO 9001 + ISO/IEC 27001, ili ISO 9001 + ISO/IEC 20000 + ISO/IEC 27001 itd. Za svaki sustav upravljanja ako se želi certificirati postoji odgovarajuća norma (ISO 9001, ISO 14001, itd.). Svaka ta norma ima niz zahtjeva koje se mora ispuniti ako se želi dobiti certifikat. No kada se želi certificirati tzv. šingrirani sustav ne postoji međunarodna norma prema kojoj se može izvršiti takvo auditiranje i certificiranje. Mada certifikacijske kuće izdaju certifikate za integrirane sisteme, i to na temelju zahtjeva u ISO 9001, praktički to nije moguće. Naime, ISO 9001 u svom preambulu navodi u kojim slučajevima se može primijeniti ta norma. Prema samoj definiciji namijenjene norme ISO 9001 ona je neprijemljiva kao skup zahtjeva za integraciju sistema i da se na temelju nje izdaje neki certifikat. Zbog toga je prikladniji naziv kombinirani sustav upravljanja koji ima sve značajke integracije više sistema upravljanja, ali ne prema nekoj formalnoj normi, već prema logičkom i funkcionalnom objedinjavanju na nivou poslovnih procesa koji su jedinstveni za svaki sustav upravljanja. Međutim, postoji nacionalna norma BS PAS 99:2006 koja je namijenjena za certificiranje integriranih sistema, ali nije važeća u međunarodnim okvirima. Ona je primjenljiva samo u zemljama koje su pripadale ujedinjenom kraljevstvu GB. Osnovni princip integracije sistema upravljanja u okviru PAS:99:2006 sastoji se u identifikaciji istih zahtjeva i objektivnom postojanju jedinstvenih procesa u svim sistemima upravljanja. Zatim se ti jedinstveni procesi obrađuju u potpunosti u skladu sa najzahtjevnijom normom i formalno se uključuju u dokumentaciju nekog sistema upravljanja što normalno u ISO 9001. Svi ostali sistemi upravljanja se onda samo pozivaju (referenciraju) na tu jedinstvenu proceduru i/ili radnu uputu. Što znači najzahtjevniji zahtjev kod implementacije neke standardne procedure? Dobar primjer može biti

¹Dejan Adelsberger, Bluefield d.o.o., Zagreb, HR, dejan@bluefield.hr

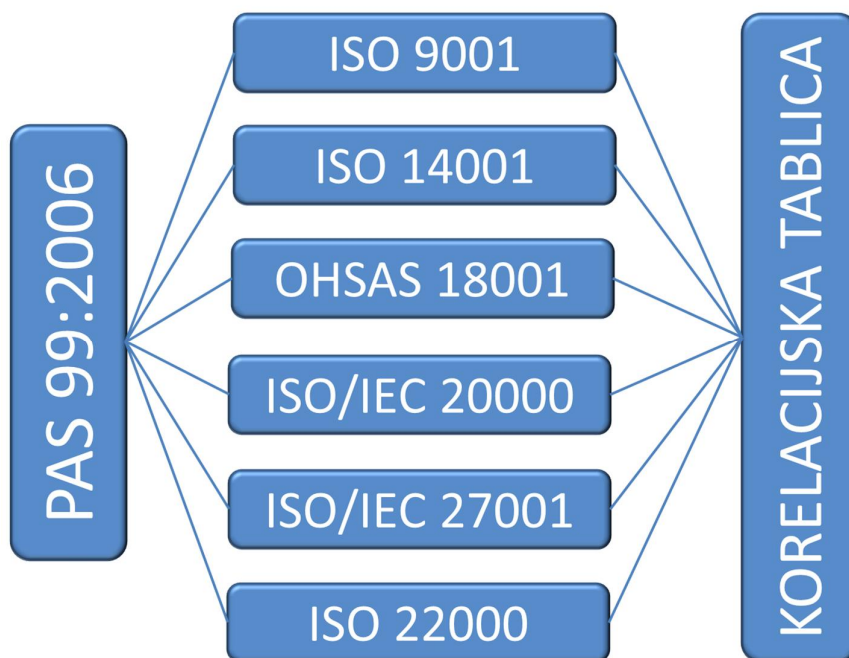
²Mr.sc. Zdenko Adelsberger, Bluefield d.o.o., Zagreb, HR, zadelsbe@zg.t-com.hr

³Dr.sc. Krešimir Buntak, Državni zavod za mjeriteljstvo, Zagreb, HR, kresimir.buntak@dzm.hr

procedura za upravljanje dokumentacijom. Ona se zahtjeva u svim sistemima upravljanja, ali samo ISO/IEC 27001:2005 zahtjeva klasifikaciju informacija, a time i dokumenata na kojima se nalaze informacije. To znači, ako se taj zahtjev proširi na sve sisteme upravljanja dobije se jedinstvena procedura za upravljanje dokumentacijom koja je relevantna za sve sisteme upravljanja.

Prilikom auditiranja samostalnog sustava problem je relativno jednostavan. Auditiranje se vrši samo prema jednom standardu sa jednim ili više auditora iz istog područja upravljanja. Kod auditiranja kombiniranog sustava pojavljuje se potreba za auditorima različitog znanja i specijalnosti u različitim područjima koja se auditiraju. Ovdje već može doći do komplikacija u postupku provođenja audita jer osim što se treba voditi računa o različitim područjima treba se voditi računa i o zajedničkim dijelovima koji su zajednički za sve sustave kod kombiniranog sustava.

Program AUDIT MAN je namijenjen za auditiranje pojedinačnih sustava upravljanja kao i kombiniranih sustava upravljanja u skladu sa standardom PAS 99:2006 kao što je prikazano na slici 1. Ovdje se PAS:99:2006 koristi samo kao jako dobar pristup integraciji sistema upravljanja, mada se na međunarodnom nivou ne koristi kao skup zahtjeva za integraciju.



Slika 1. Prikaz integriranog sustava pomoći standarda PAS 99

2. AUDIT MAN

Program AUDIT MAN kao softversko rješenje pokriva sva područja u procesu auditiranja kao i što se radi kod šru nogō auditiranja. U postupku auditiranja postoje različite faze obavljanja posla kao što je prikazano na slici 2.



Slika 2. Korištenje programa AUDIT MAN u fazama auditiranja

Iz slike 2. može se vidjeti da se najveći dio posla u procesu auditiranja može napraviti korištenjem programa AUDIT MAN.

Osnovne značajke programa AUDIT MAN:

- Web sučelje
- Izvođenje na različitim platformama (Windows™, Linux, Android™, iOS™) osobno računalo, prijenosno računalo, tablet računalo, mobilni telefon
- Rad u off-line načinu
- Uvoz/izvoz podataka
- Vi-ekorisnički rad
- Vi-jezičnost
- Pristup klijenta do svojim podataka
- Sigurnost
- Kriptirana baza
- Strogo određena pravila pristupa i korištenja
- Usklađenost sa standardom ISO 19011

U fazi izrade plana auditiranja potrebno je prvo odabrati koje se sustave nad kojima će se provoditi audit, potom odabir auditora koji će sudjelovati u procesu auditiranja kao i definiranje vremenskih rokova za provođenje audita. Na slici 3. dan je prikazano kako to izgleda u programu AUDIT MAN.

Edit audit plan details

Partner: Star consulting Ltd
 Start of audit: 01/11/2011
 End of audit: 15/11/2011
 Audit representative: Mark Irvin

Systems for audit

Standard	Name
ISO/IEC 27001:2005	Information technology -- Security techniques -- Information security management systems -- Requirements
ISO 9001:2008	Quality management systems -- Requirements

Audit team

Standard	Auditor	Function	Organization / Director / Address
ISO/IEC 27001:2005	Scheiber Erich	Lead auditor	Star consulting Ltd
ISO/IEC 27001:2005	Irjajc Nikola	2nd auditor	5th Avenue
ISO/IEC 27001:2005	Adelsberger Dejan	Observer	New York
ISO 9001:2008	Adelsberger Dejan	Lead auditor	
ISO 9001:2008	Irjajc Nikola	2nd auditor	

Audit / Assessment plan

Type of audit: Mark Irvin
 Start of audit: 01.11.2011
 End of audit: 15.11.2011

Systems for audit: ISO/IEC 27001:2005, ISO 9001:2008

Date	Start time	End time	Clause	Topic	Auditor	Location	Contact
05.11.2011	08:00	15:00	5.1	Management commitment	Scheiber Erich		Mark Irvin
05.11.2011	08:00	15:00	5.1.a	Management shall provide evidence of its commitment to the establishment, implementation, operation, monitoring, review, maintenance and improvement of the ISMS by:	Scheiber Erich		Mark Irvin
05.11.2011	08:00	15:00	5.1.b	establishing an ISMS policy;	Scheiber Erich		Mark Irvin
05.11.2011	08:00	15:00	5.1.c	ensuring that ISMS objectives and plans are established;	Scheiber Erich		Mark Irvin
05.11.2011	08:00	15:00	5.1.c	establishing roles and responsibilities for information security;	Scheiber Erich		Mark Irvin
05.11.2011	08:00	15:00	A.9.2.4	Equipment maintenance	Scheiber Erich		Mark Irvin
05.11.2011	08:00	15:00	5	Control			
05.11.2011	08:00	15:00	5.1.a	Equipment shall be correctly maintained to ensure its continued availability and integrity			
05.11.2011	08:00	15:00	5	Management responsibility			
05.11.2011	08:00	15:00	5.1.a	Ensuring sufficient resources to establish, implement, operate, monitor, review, maintain and improve the ISMS (see 5.2.1);			
05.11.2011	08:00	15:00	5.2	Resource management			

Topics

Details	Date	Location
7 - Management review of the ISMS	Company headquarter	Company headquarter

Details: ISO/IEC 27001:2005

Date	Start time	End time	Clause	Topic	Auditor	Location	Contact
05.11.2011	08:00	15:00	7.3.d	Resource needs.			
05.11.2011	08:00	15:00	7.3.e	Improvement to how the effect			
05.11.2011	08:00	15:00	5.1	Management commitment	Scheiber Erich		Mark Irvin
05.11.2011	08:00	15:00	5.1.a	establishing an ISMS policy;	Scheiber Erich		Mark Irvin
05.11.2011	08:00	15:00	5.1.b	ensuring that ISMS objectives and plans are established;	Scheiber Erich		Mark Irvin
05.11.2011	08:00	15:00	5.1.c	establishing roles and responsibilities for information security;	Scheiber Erich		Mark Irvin
05.11.2011	08:00	15:00	5.1.c	Equipment maintenance	Scheiber Erich		Mark Irvin

Slika 3. Izrada plana auditiranja pomoću programa AUDIT MAN

Slika 3. prikazuje odabir sustava za auditiranje, odabir auditora za pojedini sustav kao i definiranje funkcije u pojedinom sustavu, definiranje tema kao i vremenika odvijanja audita te izgled kako izgleda na ispisu na papir. Prednost koju nudi program AUDIT MAN je ta –to nakon definiranja plana audita korisnik odnosno auditirana strana može dobiti plan audita direktno na e-mail u PDF formi ili mu se može omogućiti direktan pristup programu kako bi zajedno sa auditorima mogao sudjelovati u definiranju plana audita –ime se dobiva na vremenu i gudi se potreba za naknadnim usklađivanjem.

Suglasnost partnera za plan audita može se odraditi direktno kroz program –ime se omogućava sljedeća faza u procesu auditiranja a to je izrada lista za provjeru (check lista). Program AUDIT MAN sam na osnovu plana audita izrađuje liste za provjeru sa automatskim dodjeljivanjem fleljenog auditora, vremena auditiranja, kao i osobe zadužene na auditiranoj strani.

Izgled popunjavanja liste za provjeru dan je na slici 4. iz koje se može vidjeti da osim –to se ispunjava da li je ispunjen neki od zahtjeva moguće je tako napisati nesukladnosti, obveze kao i vlastita započinjanja auditora. Kompletna lista za provjeru može se i ispisati na papir ili u PDF datoteku. Nakon izrade i popunjavanja liste za provjeru potrebno je napisati izvještaj sa audita koji se također piše kroz sam program AUDIT MAN.

Check list

Partner: Star consulting Ltd [Close]

Start of audit: 01/11/2011 End of audit: 15/11/2011

Audit representative: Mark Irvin

ISO/IEC 27001:2005 ISO 9001:2008

Details: ISO/IEC 27001:2005

Clause	Topic	True	False	Nonconformity	Note	Remark
5.1.e	providing sufficient resources to establish, in			Nonconformity	Obligations	Remark
5.2	Resource management					
5.2.1	Provision of resources The organization sha					This is the
5.2.1.a	establish, implement, operate, monitor, revix					
5.2.1.b	ensure that information security procedures					This should be obliga
5.2.1.c	identify and address legal and regulatory reX					
5.2.1.d	maintain adequate security by correct applic					
5.2.1.e	carry out reviews when necessary, and to re			Text of nonconf	Test	Hier könnten die Nach
5.2.1.f	where required, improve the effectiveness o					
5.2.2	Training, awareness and competence The of					
5.2.2.a	determining the necessary competencies for					
5.2.2.b	providing training or taking other actions (e.					
5.2.2.c	evaluating the effectiveness of the actions t					
5.2.2.d	maintaining records of education, training, s					

Complies Does not comply Nonconformity Note Remark

Tag all Untag all Reset selected Print

Clause	Topic	True	False	Nonconformity	Note	Remark
5.2.1.b	ensure that information security procedures support the business requirements;					This should be obligation.
5.2.1.c	identify and address legal and regulatory requirements and contractual security obligations;			X		
5.2.1.d	maintain adequate security by correct application of all implemented controls;					
5.2.1.e	carry out reviews when necessary, and to react appropriately to the results of these reviews; and					Text of nonconformity.
5.2.1.f	where required, improve the				Test	Hier könnten die

Slika 4. Popunjavanje liste za provjeru i ispis na papir

Pisanjem izvještaja se završava rad u jednoj fazi certificiranja. AUDIT MAN nudi mogućnost automatskog izvještavanja prema listi za provjeru odnosno prema postavljenim obvezama koje trebaju biti ispunjena kako se na sljedećem auditu mogla obratiti pozornost na te postavljene obveze. Nudi se i mogućnost prilagodba vezana za vrstu audita bilo da je nadzorni, predcertifikacijski ili certifikacijski koji također mogu biti povezani i kontrolirani kao takvi.

3. ZAKLJUČAK

Program AUDIT MAN je kompletno rješenje bazirano na web tehnologiji koja omogućava izvođenje na bilo kojoj platformi kao što su Windows™, Linux, Android™, iOS™ itd. Mogućnost i takozvanog off-line na inačica omogućava i korištenje u područjima bez pokrivenosti mreže. AUDIT MAN omogućava pravovremeno i kompletno praćenje klijenta u procesu auditiranja bilo da je u pitanju auditiranje jednog sustava, kombiniranog ili integriranog sustava.

LITERATURA

1. ISO 19011:2002, Guidelines for quality and/or environmental management systems auditing
2. Integrated Management PAS 99:2006, The British Standards Institution
3. Jelen Bill, Dowell Dwayne K., *Excel For Auditors: Audit Spreadsheets Using Excel 97 Through Excel 2007 (Excel For Professionals Series)*, HolyMacro! Books, 2006
4. Verschoor Curtis C., *Audit Committee Essentials*, Wiley, 2008
5. Pickett K. H. Spencer, *The Essential Handbook of Internal Auditing*, Wiley, 2005