



International Organization for Standardization



International Accreditation Forum

Datum: 25 kolovoz 2005

ISO 9001 Auditing Practices Group Smjernice o:

Auditiranje Sustava upravljanja temeljenih na elektronici (EBMS)

1. Uvod

Rastuća ovisnost organizacija o elektronskim medijima za funkcioniranje i kontrolu njihovih sustava upravljanja zahtijeva od certifikacijskih/registracijskih tijela i njihovih auditora novi pogled na nove pristupe kako bi osigurali djelotvornost audita. Trebaju redefinirati načine procjene postupaka i uz njih vezanih dokumenata (uključujući zapise) kako bi potvrdili usklađenost s kriterijima audita.

Ovaj dokument je razvijen kako bi pružio općenita uputstva za provedbu audita sustava upravljanja koji su ili u potpunosti temeljeni na elektronici ili imaju visok stupanj dokumentacije u elektronskom obliku. On također pruža uputstva za certifikacijska/registracijska tijela koja mogu koristiti kao dodatak normalnim aktivnostima planiranja i priprema koje treba obaviti prije audita.

Ovaj document je usmjeren na one zahtjeve ISO 9001 gdje postoji mogućnost uporabe elektronskih dokumenata, zapisa itd., i također tamo gdje se pristup takvim dokumentima/zapisima može kontrolirati elektronskim sustavom.

Ovaj dokument je namijenjen auditorima sustava upravljanja koji imaju široko i raznoliko praktično iskustvo vezano uz sustave upravljanja temeljene na elektronici (EBMS) – tj. sustave upravljanja koji ovise o elektronskim dokumentima, podacima i programskoj podršci za njihov normalan rad. No, pisan je na način koji će omogućiti razumijevanje i korištenje i onima koji imaju ograničeno iskustvo s računalima i EBMS.

Bez obzira radi li se o trećoj strani certifikacijskom tijelu, akreditacijskom tijelu ili internoj funkciji audita, organizacija koja provodi audit ("organizacija koja auditira") je odgovorna za osiguravanje djelotvornosti postupka auditiranja za EBMS. Ovaj dokument primijenjuje upute pružene u ISO 19011, i predlaže pristupe koje mogu koristiti auditori ISO 9001 i ostalih standarda sustava upravljanja kako bi utvrdili usklađenost sa navedenim standardom. Auditori i organizacije koje auditiraju trebaju napraviti prilagodbe potrebne za

osiguravanje odgovarajućeg pristupa dok provode korake postupka audita kako je navedeno u ISO 19011.

Treba se napomenuti kako sposobnost auditiranja EBMS se ne smije gledati kao izgovor za smanjenje trajanja auditiranja, nego kao sredstvo za optimiziranje djelotvornosti audita.

Nije namjera ovog dokumenta pružanje uputstava za auditiranje kontrola vezanih uz sigurnost informacija unutar EBMS. Oni zainteresirani za daljnje kontrole povezane sa sigurnosti informacija usmjeravaju se prema ISO/IEC 17799 koji je obimna norma za ta pitanja.

2. Pokretanje audita i planiranje

Tijekom faze pokretanja audita (stupanj 1 audita) organizacija koja auditira treba odrediti strukturu organizacije koju auditira, kao i do koje je mjere njezin sustav upravljanja temeljen na elektronicima. Organizacija s više lokacija i centraliziranim EBMS-om, ili virtualna organizacija traže različite planove i postupke auditiranja, nego organizacija s jednom lokacijom ili fizička organizacija.

Organizacija koja auditira i auditirani trebaju se dogovoriti kako će auditori pristupiti i koristiti EBMS. To može uključivati razmatranje:

- Omogućavanje članovima grupe auditora upoznavanje auditiranog EBMS-a (uključujući određivanje odgovarajućeg vremena u planu audita za to upoznavanje)
- Politika auditirane organizacije vezano uz uporabu njezine informacijske tehnologije
- Uputstva za pristup, kao i obvezne sigurnosne dozvole za pristup, pertinent organizacijski dokumenti i zapisi
- Sigurnosni postupci za osiguranje da će auditori zaštititi povjerljivost elektronskih dokumenata i zapisa tijekom i poslije audita.

Organizacija koja auditira treba osigurati da unutar njezine grupe auditora postoji dovoljno znanja i vještina za provođenje djelotvorne procjene EBMS.

3. Procjena dokumentacije

Ovisno o tome da li auditirani može omogućiti pristup dokumentaciji putem aplikacija temeljenih na webu ili putem elektronske pošte, organizacija koja provodi audit može provesti dio ili cijelu procjenu dokumentacije izvan lokacije audita: on-line ili preuzimanjem elektronske dokumentacije dostavljene elektronskom poštom.

Ovisno o tehničkim i sigurnosnim faktorima, može se dogoditi da nije izvedivo provesti cjelokupnu procjenu EBMS-a organizacije on-line ili putem prijenosa dokumenata e-poštom, prije dolaska na lokaciju audita. U tim slučajevima, pripremne aktivnosti za audit koje zahtijevaju procjenu elektronskih dokumenata moraju se odvijati na lokaciji auditiranog tijekom audita prvog stupnja.

4. Aktivnosti koje se provode na lokaciji

Pristup auditu za sustave upravljanja temeljene na elektronicima ovisiti će najviše o tome koliko je dokaza potrebnih za utvrđivanje usklađenosti u obliku elektronskih zapisa.

Tijekom provođenja aktivnosti na lokaciji, auditorov put tipično uključuje fizičko lociranje postupaka koji se auditiraju. No, kod EBMS vrijeme potrebno za potvrđivanje dokaza za

određivanje da li su zahtjevi ispunjeni može biti potrošeno na računalnoj radnoj stanici koja se ne mora nalaziti blizu promatranog stvarnog postupka.

Kada su računalne radne stanice u udaljenim prostorima koji nisu dostupni na lokaciji stvarnog procesa, stvarno vrijeme auditiranja na fizičkoj lokaciji postupka može biti smanjeno. No, cjelokupno vrijeme procjene ne mora biti smanjeno, s obzirom da se procjena elektronskih dokaza može provesti prije i/ili poslije potvrđivanja postojanja fizičkih postupaka.

U slučaju kada je povezana računalna radna stanica postavljena na udaljenom mjestu, posebnu pažnju mora se posvetiti vremenu potrebnom za kretanje do i od fizičke lokacije postupka.

Kada postupak ovisi o ljudskoj intervenciji, auditor treba procijeniti postupke primijenjene za interakciju između fizičkih postupaka i elektronskih medija kako bi se osigurala točnost povezanih informacija. .

5. Auditiranje kontrole elektronskih dokumenata

Elektronski dokumenti koji uspostavljaju politike i postupke sustava upravljanja mogu biti u različitim oblicima datoteka ovisno o programskim aplikacijama koje se koriste u organizaciji za stvaranje tih dokumenata. Oblici elektronskih datoteka uključuju tekst, html, pdf, itd. Oblici tablica i baza podataka su također elektronski dokumenti podložni elemnetima kontrole tijekom auditiranja sustava upravljanja.

S obzirom na relativnu jednostavnost korisničkog stvaranja elektronskih tablica i baza podataka, auditori moraju ustanoviti da se politike koje upravljaju kontrolama koje se odnose na dokumentaciju sustava upravljanja općenito, odnose i na elektronske dokumente putem odgovarajućih postupaka.

Organizacije moraju upotrijebiti odgovarajuće i djelotvorne postupke unutar elektronskog okruženja za osiguravanje odgovarajuće procjene, odobravanja, objavljivanja i raspačavanja dokumentacije sustava upravljanja. Sve mora biti u skladu s metodama za razvoj i izmjenu elektronskih dokumenata.

U mnogim slučajevima mjere kontrole dokumentacije mogu također biti standardni elementi programske aplikacije korištene za njihovo stvaranje. Stoga auditori trebaju razumjeti te kontrole specifične za program do te mjere da se one koriste kao temelj usklađenosti s primjenjenom normom sustava upravljanja.

S obzirom na veću mogućnost izmjena, usklađivanja, preoblikovanja i na druge načine poboljšavanja dokumenata unutar elektronski temeljenog sustava upravljanja, auditori trebaju posvetiti posebnu pažnju elementima kontrole kao što je razina identifikacije i revizije dokumenata.

Kako elektronski mediji pogoduju povećanom broju izmjena dokumenata, auditori trebaju ustvrditi kako su kontrole koje se koriste za upravljanje zastarjelim dokumentima obuhvaćene politikama i postupcima kontrole dokumentacije organizacije.

Auditori trebaju potvrditi da EBMS documentatcija postoji kako bi osigurala usmjerenje korisnicima vezano uz funkcionalne i kontrolne aspekte vezane uz elektronske dokumente. Uz to, "točka korištenja" zahtjevi vezani uz primjenjive norme sustava upravljanja će se tipično djelomično razmatrati unutar politike pristupa dokumentaciji te organizacije. Auditori

trebaju razumjeti politike i postupke organizacije vezano uz privilegije korisnika kako to postaje važan razlog za pravilno razumijevanje procesa unutar organizacije.

Vanjska elektronska komunikacija s dobavljačima, kupcima i drugim zainteresiranim stranama može uključivati razmjenu podataka. Kako ti vanjski dokumenti mogu sadržavati ključne parametre koji određuju funkcioniranje organizacijskih postupaka, auditori trebaju potvrditi stupanj do kojeg su ti dokumenti službeno uključeni i kontrolirani unutar elektronski temeljenog sustava upravljanja.

6. Auditiranje kontrole elektronskih dokumenata

Elektronski zapisi sastoje se od podataka o rezultatima postupaka u kombinaciji s elektronskim formatima koji sadržavaju te podatke. Ti elektronski formati su u rasponu od jednostavnih tabličnih dokumenata do kompleksnijih baza podataka.

Auditori trebaju biti svjesni kako elementi kontrole koje uspostavi organizacija za elektronske oblike nisu obvezno isti kao oni koji se primjenjuju na elektronske zapise. Na primjer, ako uzmemo "identifikaciju", pojam se odnosi na nomenklaturu same elektronske forme. Kada se "identifikacija" odnosi na elektronski zapis, to se odnosi na jedinstvenu uporabu elektronske forme za tu grupu podataka.

Auditori trebaju procijeniti metode koje organizacija koristi za prikupljanje podataka, kako bi osigurali da postupci unosa podataka daju dovoljno povjerenja u njihovu točnost.

Kada se procjenjuju kontrole organizacije vezano uz pohranu zapisa, auditori moraju ustvrditi da li organizacije razumiju svoj kapacitet pohrane naprama:

- Brzine stvaranja zapisa,
- Politike čuvanja zapisa i uz to vezanih vremenskih okvira,
- Brzinu odbacivanja zapisa,

Pošto ti faktori mogu utjecati na pravilno funkcioniranje EMBS.

Kako baza znanja i izvedba organizacije mogu biti u potpunosti sadržani u elektronskim dokumentima, auditori trebaju procijeniti pristup organizacije osiguravanju informacija sadržanih u elektronskim sredstvima. Za više informacija o sigurnosti informacija pogledajte ISO / IEC 17799.

7. Organizacijski izvori

Kako organizacije prelaze na korištenje EMBS, funkcija IT postaje vitalna. Auditori trebaju utvrditi da li je organizacija osigurala odgovarajuće IT resurse (uključujući infrastrukturu) kako bi osigurali da EBMS funkcionira kontinuirano i djelotvorno.

Auditori također trebaju utvrditi da li je organizacija odgovarajuće odredila stupanj interakcije, podrške i uključanja IT osoblja u pitanja povezana uz uspostavu, dokumentiranje, primjenu i održavanje EBMS.

Kao dio utvrđivanja određivanja odgovarajućih resursa, auditori trebaju procijeniti kako se organizacija odnosi prema kompetencijama koje treba imati osoblje koje upravlja hardverom i programskom podrškom potrebnom za vođenje EBMS.

Tijekom uspostavljanja EBMS, uobičajeno je da postoje paralelni sustavi (papirni i elektronski) dok se korisnici ne naviknu na korištenje elektronskog sustava. U tim slučajevima auditor treba potvrditi postupke organizacije koji osiguravaju da je EBMS stvarno asimiliran i korišten od strane zaposlenika.

Složenost IT infrastructure organizacije će varirati, ovisno o prirodi i složenosti poslovanja. Auditori trebaju provjeriti politike i postupke održavanja sustava organizacije za njezinu IT platformu. Isto tako, auditori trebaju ustvrditi kako se organizacija odnosi prema incidentima pada sustava, pošto će oni utjecati na uobičajeno funkcioniranje sustava. Auditori trebaju ustvrditi da li organizacija posjeduje formalne zaštitne sustave i da li se ti povremeno provjeravaju i testiraju da su odgovarajući.

U odnosu na računalnu podršku, auditori trebaju provjeriti kontrole postavljene za unutrašnju programsku podršku, vanjsku programsku podršku, licenciranje programa, kao i ažuriranje programa. Pošto se na programsku podršku može gledati kao na dinamične elektronske dokumente, upute pružene za auditiranje dokumenata su također primjenjive i na njih.

Do koje mjere organizacija koristi programsku podršku za svoj EBMS, auditori trebaju procijeniti djelotvornost aplikacija i njihov odnos prema lelementima sustava upravljanja definiranim u primjenjivim kriterijima.

Pošto faktori iz okoliša mogu utjecati djelotvornost IT platforme, organizacija treba poduzeti mjere za zaštitu od takvih događaja. To može biti od odgovarajućih prostora i kućišta do potrebe za neprekinutim dovodom struje (UPS). Auditor treba procijeniti da li organizacijske kontrole uzimaju u obzir takve aspekte kao što je održavanje sustava, vlaga, temperature, itd., do stupnja kada isti utječu na djelovanje EBMS-a.

8. Unutarnja i vanjska komunikacija elektronskim putem

Kako raste jednostavnost uporabe elektronske komunikacije, kao i njezina rasprostranjenost, organizacije trebaju osigurati da dokumentirani sustav upravljanja pokriva ta pitanja, koliko je potrebno, kako bi osiguralo konzistentnost korištenja za zadovoljavanje zahtjeva njihovog EBMS-a, i primjenjive norme sustava upravljanja.

Kada se intranet, e-pošta i instant poruke koriste za zadovoljavanje zahtjeva EBMS-a, auditori trebaju utvrditi da li politike i postupci pokrivaju uvjete pod kojima se ta sredstva mogu koristiti. Dodatno, ako se rezultati unutarnje elektronske komunikacije koriste za zadovoljavanje kriterija audita, tada se auditori moraju uvjeriti da se primjenjuju politike i postupci za kontrolu zapisa.

Kada se organizacija oslanja na svoju IT infrastrukturu za elektronsku komunikaciju s korisnicima (npr. Za e-kupovinu), dobavljačima (e-nabava), vanjske lokacije i druge zainteresirane strane, auditor treba potvrditi da su metodologija, politike i postupci za te komunikacije i vezane transakcije formalno obrađeni unutar EBMS-a.

9. Sustavi upravljanja više lokacija

Organizacije koje posluju na više lokacija (ili sa središnje lokacije prema satelitskim lokacijama) uglavnom održavaju komunikaciju i razmjenjuju politike, postupke i podatke s različitim lokacijama putem elektronskih sredstava, kao što je internet, ekstranet, e-pošta i instant poruke.

Kada se IT platforma i njezine pridružene programske aplikacije koriste za razmjenu informacija koje potpadaju pod kriterije audita, auditori trebaju razmjeti različite načine komunikacije koje primjenjuje organizacija do te mjere koja je potrebna za utvrđivanje da li EBMS zadovoljava kriterije audita.

Auditori trebaju utvrditi da li kontrole nad sustavom upravljanja više lokacija su odgovarajuće obrađene i uspostavljene unutar politiks i postupaka organizacije.

10. Kompetencije auditora

Pouzdanost postupka audita za EBMS će ovisiti o sposobnosti auditora da razumiju trendove u informacijskim tehnologijama kako se organizacije sve više oslanjaju na programsku podršku za praćenje i kontroliranje svojeg poslovanja.

Organizacije koje auditiraju trebaju poduzeti potrebne mjere, uključujući obuku, kako bi pokrili opće i pojedinačne potrebe svojih auditora vezano uz:

- **Opće trendove u Informacijskim tehnologijama koji mogu utjecati na djelovanje sustava upravljanja**
- **Pitanja specifična za audit za svaki zadani audit koji treba provesti**

Kako su inovacije i promjene u IT sektoru relativno česte u usporedbi s promjenama kriterija audita, auditori i organizacije koje auditiraju su izazvane potrebom imanja praktičnog razumijevanja povezanih trendova i kako oni mogu biti primjenjivi i korišteni unutar EBMS-a.

U svjetlu inovacija koje utječu na djelovanje EBMS-a, organizacije koje auditiraju trebaju odrediti da li grupa auditora koja provodi audit ima potrebno iskustvo da bi bila djelotvorna prilikom audita ili je potrebno angažirati tehničkog stručnjaka za provođenje audita kao pomoć grupi.

Za daljnje informacije o ISO 9001 Auditing Practices Group, molimo pročitajte članak: *Introduction to the ISO 9001 Auditing Practices Group (Upoznavanje s ISO 9001 Grupom za postupke auditiranja)*

Povratne informacije od korisnika upotrijebiti će ISO 9001 Auditing Practices Group kako bi procijenili da li treba razvijati dodatne smjernice ili će biti samo potrebno revidirati postojeće. Komentare i primjedbe na članke i prezentacije možete poslati na slijedeću e-mail adresu: charles.corrie@bsi-global.com.

Ostali dokumenti ISO 9001 Auditing Practices Group mogu se skinuti s web stranica:

www.iaf.nu

www.iso.org/tc176/ISO9001AuditingPracticesGroup

Odricanje od zahtjeva

Ovaj članak nije bio predmet postupka podrške od strane ISO, ISO tehničke komisije 176 ili Međunarodnog akreditacijskog foruma (IAF).

Informacije sadržane u njemu namijenjene su za obrazovnu i komunikacijsku svrhu. ISO 9001 Auditing Practices Group ne preuzima odgovornost za eventualne pogreške, nedostatke ili druge odgovornosti koje mogu nastati davanjem ili kasnijom uporabom takvih informacija.