MSc Jovana Petrović Bureau Veritas
MSc Vanja Kukrika, Tekon Tehnokonsalting
Prof dr Milan Kukrika Beogradski univerzitet

Menadžment rizicima neusklađenosti

office@fqce.org.rs

Compliance risk management

Abstract

This paper presents a process for managing compliance risks. All systems during their lifecycle, no matter how simple, will generate compliance implications that need to be managed. A process designed to detect and prevent regulatory compliance failures is vital, however such an effective process cannot succeed without development of a strong compliance risk management culture.

Sažetak

Svrha ovog rada je da se organizacijama omogući da, kao deo ukupne infrastrukture upravljanja, implementiraju Sistem za menadžment zaštitom podataka o ličnosti (PIMS) koji je usklađen sa zahtevima relevantne zakonske regulative i najbolje prakse.

Keywords: personal information, personal information management system (PIMS), Monitoring and reviewing the PIMS, ISO/IEC 27001, Information technology — Security techniques — Information security management systems — Requirements, ISO/IEC 29100:2011 Information technology - Security techniques – Privacy framework
Keywords: *compliance, compliance obligation, ISO 19600, non-compliance,*
Ključne reči: *usklađenost, obaveze za usklađenost, ISO 19600, neusklađenost,*

Ključne reči: podaci o ličnosti, Sistem za menadžment zaštitom podataka o ličnosti (PIMS), Monitoring i preispitivanje PIMS-s, ISO/IEC 27001:2013 Informacione tehnologije — Tehnike bezbednosti — Sistemi menadžmenta bezbednošću informacija — Zahtevi, ISO/IEC 29100:2011 Informaciona tehnologija - Tehnike sigurnosti - Okvir privatnosti

1. Uvod

Poslovni imperativ u 21. veku postaje veština vođenja poslovanja vodeći pri tome računa da se ne prekrše slovo i duh zakona. Ako vaš poslovni uspeh podrazumeva da zapošljavate sve više ljudi, poslujete sa više zemalja, prodajete veći asortiman proizvoda, širite bazu vaših kupaca itd…, posledica može da bude povećavanje verovatnoće da će neko negde učiniti nešto čime ćete prekršiti normativni okvir koji je organizacici nametnut. Principi i praksa objašnjeni u ovom radu će vam pomoći da identifikujete gde je najverovatnije da se to dogodi, i da na osnovu toga uspostavite potrebne promene kako bi se smanjili šanse da budete izloženi posledicama rizika neusklađenosti.

Compliance Compliance risk is the risk of financial or reputational loss that can result from lack of awareness or misunderstanding of, ambiguity in, or reckless indifference to, the way law and regulation apply to your business, its relationships, processes, products and services.

Rizik neusklađenosti je rizik od finansijskog gubitka ili gubitka reputacije koji mogu nastati kao rezultat nedostatka svesti ili nerazumevanja, dvosmislenosti ili ignorisanja uticaja na poslovanje zbog kršenja prihvaćenih normativnih obaveza.

Većina poslovnih organizacija na žalost ne pridaje pravi značaj rizicima neusklađenosti i mogućnostima preventivnog delovanja na njegovom eliminisanju ili ublažavanju. Procenjuje se da direktni finansijski troškovi rizika neusklađenosti prevazilaze 200 milijardi $ godišnje samo u sektoru finansijskih usluga. Naknadni indirektni troškovi zbog gubljenja reputacije ih višestruko prevazilaze.

Očigledno je da postoji jasna potreba da se poboljša razumevanje uzroka rizika neuskađenosti sa ciljem da se poslovne organizacije motivišu da investiraju u projekte identifikovanja i upravljanja rizicima neusklađenosti proaktivno, pre nego što su gubici nastali.

Problem je u tome što su pravnici naučeni da reaguju reaktivno. Za advokatske firme je lakše i finansijski mnogo isplativije da se angažuju kada se rizik neusklađenosti već dogodio sa nastojanjem da umanje nastalu štetu (suđenja, parnica, zahteva za odštetom, plaćanja kazni i sl.).

S druge strane, za poslovne organizacije mnogo veća korist bi bila ako bi se odgovarajuća sredstva i napori investirali u proaktivno otkrivanje uzroka rizika neusklađenosti I njihovog eliminisanja ili značajnog umanjivanja, pre nego što uopšte dođe do posledica

2. Preispitivanje rizika neusklađenosti i predlaganje načina da se on umanji

Polazna tačka za prokativni menadžment rizikom neusklađenosti je da se prouče sve značajne interakcije poslovnih procesa sa normativnim okvirom i da se jasno utvrdi razlika između izvora rizika i njegovih posledica.

Postoje dva osnovna principa za razumevanje rizika neusklađenosti:

1. Prvi princip glasi da normativna obaveza sama po sebi ne predstavlja rizik. Normativne obaveze se nameću da bi se osiguralo da se zainteresovane strane osećaju maksimalno zaštićenim. Te obaveze su podložne promenama i i morate biti u stanju da im se prilagodite. Pri tom je najvažnije da napravite kvalitetnu analizu svih ključnih poslovnih transakcija gde postoji potencijal da pojedinci koji donose poslovne odluke dođu u sukob sa slovom ili duhom zakona.
2. Drugi princip je da se za definisanje rizika neusklađenosti obavezno koristi pravna terminologija. Svaki ne-pravni termin može imati za posledicu da se u nekom trenutku ospori odgovornost za primenu mera za eliminaciju ili ublažavanje rizika neusklađenosti.

U nastavku je predložena metodologija menadžmenta rizikom neusklađenosti:

Korak 1. Artikulisati koje gubitke želite da sprečite

Postoje dve vrste gubitka koje bi proaktivni menadžment rizikom neusklađenosti trebalo da pokuša da spreči:

1. direktni finansijski gubitak (na primer velike novčane kazne ili troškovi sudskih sporova i parničenja) i
2. indirektni poslovni gubitak zbog narušavanja ugleda (koji može da utiče na vrednost brenda i potencijalno na dugoročnu održivost vašeg poslovanja).

Korak 2. Objasniti koje aktivnosti mogu da dovedu do pojave rizika neusklađenosti.

Pojava rizika neusklađenosti je direktna posledica ljudskog ponašanja koje može dovesti do gubitka. Tri moguća ponašanja koji mogu dovesti do gubitka su:

1. nerazumevanje načina na koji se normativni okvir primenjuje
2. nejasnoće u zakonu
3. namerno ignorisanje posledica kršenja nomativnog okvira od strane pojedinaca koji donose poslovne odluke

Korak 3. Odrediti oblasti u kojima se rizik neusklađenosti manifestuje

Da bi se olakšalo operativno upravljanje rizikom neuskađenosti trebalo bi definisati odgovarajuće kategorije (oblasti ili područja primene) u kojima se on može manifestovati:

1. *Zakonodavno-regulatorni rizik* - rizik da se poslovne aktivnosti ne sprovode i u skladu sa zakonom i propisima.
2. *Rizik neispunjavanja relevantnih zahteva i očekivanja relevantnih zainteresovanih strana* - Rizik da poslovna organizacija ne ispunjava svoju obavezu brige prema klijentima, životnoj sredini, njenim akterima i na tržištu. U građanskom pravu ovi rizici su pokriveni konceptom "građanska dužnost".
3. *Ugovorni rizik* - rizik da poslovna organizacija ne ispunjava ugovorne obaveze. Ovo je obično najveći izvor redovnog gubitka.
4. *Rizik vođenja sporova:* ovom katergorijom se namerno ograničava obim rešavanja rizika za postupke koje će se preduzimati ako i kada dođe do spora. Osnovni uzrok spora je bilo loše upravljanje drugom vrstom rizika (ugovornih rizika, na primer) ili spekulativni potraživanja od treće strane.

Korak 4. Napraviti analizu poslovnog uticaja

Na žalost, mnoge organizacije primenjuju menadžment rizicima neusklađenosti na pogrešan način jer izbegavaju da primene procesni pristup, nego se odmah definiše sistem procedura i odgovornosti svih lica u organizaciji za postizanje usklađenosti.
Posledice ovakvog pristupa velike pošto stalno rastu nepotrebni operativni troškovi za pravljenje, kontrolu i proveru beskorisne dokumentacije. Time je narušen i ugled osnovnog koncepta menadžmenta rizicima neusklađenosti, pošto su ga u praksi mnogi shvatili isključivo kao konfuzan skup procedura koje služe isključivo da se zadovolje naoko besmisleni zahtevi zainteresovanih strana.

Umesto toga bi trebalo implementirati odgovarajući proces čija svrha je da se popišu sve obaveze organizacije u pogledu ispunjavanja zakonskih, ugovornih i drugih obaveza, kao i relevantnih zahteva relevantnih zainteresovanih strana i da se izvrši procena stepena usklađenosti.

Rezultati uspešne implementacije ovog procesa su:
1. Dokumentovana informacija o relevantnim obavezama na usklađenost i kako to utiče na organizaciju
2. Definisan proces za identifikaciju, pristup i ažuriranje zapisa i informacija koje se odnose na ispunjavanje obaveza na usklađenost
3. Dokumentovani zapisi koji pokazuju stepen usklađenosti u odnosu na svaku od navedenih obaveza.
4. Dokazi o tome da su ti zapisi preispitani tako da organizacija može da dokaže svoj status usklađenosti.

Korak 5. Primeniti odgovarajuće mere za eliminaciju ili eliminisanje rizika neusklađenosti

Mere za eliminaciju ili eliminisanje rizika neusklađenosti podrazumevaju primenu pisane politike usklađenosti i pratećih procedura. Ove mere se uspostavljaju da pruže razumno uveravanje da su rizici za postizanje ciljeva ograničeni na prihvatljiv nivo definisan u procedurama za menadžment usklađenošću. Kontrole moraju biti odgovarajuće, a troškovi za njihovo uvođenje ne smeju prevazići očekivanu korist od njihovog uvođenja.

5.Zaključak

Odvijanje procesa iniciranih od strane čoveka znači i poštovanje niza zakona (kako onih koje propisuje struka, tako i onih koje propisuje društvo), ugovornih obaveza, standarda, pravila (koja se moraju poštovati već i iz zahteva dobre prakse) kao i nadzor i kontrolu od strane ovlašćenih osoba. Stoga su zakoni, standardi, pravila, nadzor i kontrola za sve poslovne procese apsolutna obaveza.

Usklađenost sa različitim nivoima zahteva i ograničenja je kritična aktivnost za svaku poslovnu organizaciju. Skoro je nemoguće izaći na kraj sa svim nametnutim zahtevima sa ograničenim ljudskim i finansijskim resursima, naročito ako su ti zahtevi međusobno konfliktni.

Menadžment rizicima neusklađenosti postaje sve složeniji zbog sve većeg broja zakona, propisa i standarda i drugih tipova ograničenja koja se uvode ili modifikuju svake godine. Sa toliko mnogo pravila koje bi trebalo poštovati velike organizacije imaju teškoća da procene nivoe usklađenosti sopstvenih poslovnih procesa sa normativnim okvirom i da procene njihov uticaj na realizaciju poslovnih ciljeva.

Menadžment rizicima neusklađenosti obuhvata identifikovanje, procenu i kontrolu nad potencijalnim događajima i situacijama koje mogu imati suprotan efekat na poslovanje organizacije, sa zadatkom da pruži razumno uveravanje da će uz poštovanje postavljenih zahteva poslovni ciljevi biti ostvareni.

Većina organizacija koristi reaktivni pristup menadžmentu rizicima neusklađenosti i reaguje tek nakon otkrivenih grešaka i plaćenih kazni, umesto da se proaktivnim pristupom spreči njihovo pojavljivanje.
U ovom radu je predložena odgovarajuća metodologiju za menadžment rizicima neusklađenosti koja odgovara na sledeća pitanja:

- Kako da se uspostavi sledljivost između postavljenih zahteva i poslovnih procesa i ciljeva organizacije?
- Na koji način poslovne organizacije mogu da konstantno nadgledaju nivo usklađenosti svojih poslovnih procesa?
- Kako objediniti odgovore na sve zahteve koji mogu da budu i međusobno konfliktni, pošto ih postavljaju sukobljene zaineresovane strane?
- Kako da organizacija odredi prioritete dokazivanja usklađenosti, s obzirom na ograničena sredstva koja su im na raspolaganju?

Literatura

1. COUNCIL OF THE EUROPEAN UNION, Regulation (EU) 2016/679, on the protection of natural persons with regards to the processing of personal data and on the free movement of such data.
2. Kukrika V.: Izbor i analiza standarda pogodnih za implementaciju Sistema za menadžment zaštitom podataka o ličnosti, diplomski rad Fakultet organizacionih nauka, oktobar 2014.
3. Kukrika M, Kaljević Z., Delić Z., Kukrika V.: Predlog metodologije za objektivnu procenu stepena usaglašenosti sa zahtevima standarda sistema menadžmenta, Nedelja kvaliteta 2014, Beograd, mart 2014
4. Milan Kukrika, Zoran Kaljević, Zoran Delić, Vanja Kukrika: Procesni referentni model na osnovu zahteva ANEX-a SL, Kvalitet & Izvrsnost 3-4/2014
5. Milan Kukrika, Vanja Kukrika: Značaj primene sistema za menadžment usaglašenošću sa normativnim okvirom,Kvalitet & Izvrsnost 1-2/2014
6. ISO/IEC 17021:2011, Conformity assessment — Requirements for bodies providing audit and certification of management systems
7. ISO 9000:2015, Quality management systems — Fundamentals and vocabulary
8. ISO 19011:2011, Guidelines for auditing management systems
9. ISO/IEC 20000-2:2012 Information technology – Service management - Part 2: Guidance on the application of service management systems.
10. ISO/IEC 27000:2016 Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary
11. ISO/IEC 27001, Information technology — Security techniques — Information security management systems — Requirements
12. ISO/IEC 27002, Information technology — Security techniques — Code of practice for information security controls
13. ISO/IEC 27005:2011, Information technology — Security techniques — Information security risk management
14. ISO/IEC 27006:2011, Information technology — Security techniques — Requirements for bodies providing audit and certification of information security management systems
15. ISO/IEC 27007:2011, Information technology — Security techniques — Guidelines for information security management systems auditing
16. ISO/IEC TR 27008:2011, Information technology — Security techniques — Guidelines for auditors on information security controls
17. ISO/IEC 27009:2016 Information technology -- Security techniques -- Sector-specific application of ISO/IEC 27001 -- Requirements
18. ISO/IEC 29100:2011 Information technology - Security techniques – Privacy framework
19. ISO 31000:2009, Risk management - Principles and guidelines
20. ISO/IEC 29190 Information technology - Security techniques - Privacy capability assessment model

21. BIP 0012, Data Protection: Guide to practical implementation
22. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data
23. Zakon o zaštiti podataka o ličnosti ("Sl.glasnik RS" 97/08,104/09-dr.zakon 68/12-odluka us 107/12)