INTEGRIRANO UPRAVLJANJE RIZICIMA NA AERODROMU SARAJEVO

INTEGRATED RISK MANAGEMENT AT SARAJEVO AIRPORT

Nermin Zijadić MA - dipl. ing. saobr. i kom.
Međunarodni aerodrom Sarajevo d.o.o.
Sarajevo, Bosna i Hercegovina/*Bosnia and Herzegovina*
E-mail: nermin.zijadic@gmail.com

Prof. dr. sc Fadila Kiso
Fakultet za saobraćaj i komunikacije
Sarajevo, Bosna i Hercegovina/*Bosnia and Herzegovina*

UDK/*UDC*: 005.334:711.553.9
JEL klasifikacija/*JEL classification:* L15; L93
DOI: 10.30657/hdmk.2020.22
Pregledni članak/*Review*
Jezik/Language: Bošnjački/*Bosnian*

SAŽETAK

Upravljanje rizicima (prilikama) predstavlja osnovni izazov u radu organizacije. U savremenom poslovnom okruženje, punom promjena, opasnosti ali i prilika, kompanije koje slabo ili nikako ne upravljaju rizicima osuđene su na propast. U zrakoplovstvu, a onda i u poslovanju aerodroma koji su sve manje monopolne organizacije, a sve više tržišno orjentirane organizacije, upravljanje rizicima predstavlja imperativ. Ovo je dijelom zbog obaveze proistekle iz zakonske regulative, ali i dijelom obavezujućih standarda i sistema. Posebna složenost ispunjenju ovih zahtjeva predstavlja raznolikost i obim različitih metodologija i preporučenih tehnika kod procjene rizika.. Ako se posmatraju aerodromi, onda je to u minimumu 7 različitih domena koji zahtjevaju procjenu rizika.. Izdvojena procjena rizika i rad bez kolaboracije između različitih domena bio bi ogromno trošenje vremena i resursa, sa upitnim rezultatima. Sa druge strane jednostrana integracija sa samo jednom metodologijom, bez uvažavanja specifičnosti, ponekad i potrebe različitih metodologija, sigurno vodi u otuđenost samog procesa procjene rizika i ponovno sa upitnim rezultatima.

***Ključne riječi**: upravljanje rizicima, kvalitet, sigurnost, zaštita, cyber.*

1. UVOD

Historijski posmatrano, upravljanje rizikom je započeto sa upotrebom tržišnog osiguranja radi zaštite pojedinaca i kompanija od različitih gubitaka povezanih sa nezgodama. Drugi oblici upravljanja rizikom pojavili su se tokom pedesetih godina prošlog vijeka kada se tržišno osiguranje smatralo veoma skupim i nepotpunim radi zaštite od čistog rizika. Upotreba derivata kao instrumenata za upravljanje rizikom pojavila se tokom 1970-ih, a brzo se proširila tokom 1980-ih, jer su kompanije intenzivirale upravljanje finansijskim rizikom.

Međunarodna regulacija rizika započela je 1980-ih, a finansijske firme razvile su interne modele upravljanja rizikom i formule za izračunavanje kapitala kako bi se zaštitile od nepredviđenih situacija. Istovremeno, upravljanje rizicima postalo je od suštinske važnosti, uvedeno je integrisano upravljanje rizikom i stvorene su pozicije glavnih službenika za rizik.[1]

Također, počela se razvijati i nova poslovna filozofija tzv. razmišljanje zasnovano na riziku (RBT[2]). RBT zahtijeva od rukovodioca da kontinuirano procjenjuje pitanja koja utiču na rad i poslovanje organizacije i osigurava da postoje odgovarajući ciljevi, resursi i kontrole. RBT omogućava organizacijama da ulažu dinamične promjene u svoje ciljeve i fokusiraju se na ostvarenje tih ciljeva, istovremeno osiguravajući da postoje resursi za kontrolu promjena i nepredviđenih okolnosti.

Organizacija mora odrediti metodologiju za razmišljanje zasnovano na riziku s obzirom na obim i način poslovanja. Ova metodologija zahtijeva od organizacije da smanji rizike povezane s opasnostima na razumno prihvatljiv nivo.[3]

2. PREGLED RAZVOJA UPRAVLJANJA RIZICIMA U ZRAKOPLOVSTVU

Rizici i procesi upravljanja rizicima na aerodromu su inicijalno bili vezani za pojam sigurnosti. Ako se vratimo na historijski razvoj upravljanja rizicima onda je ovo i logičan put, znajući da su rizici usko vezani sa štetom i posljedicama štete i štetnog događaja. Kao prvi standard ili sistem koji je implementirao rizike u oblasti zrakoplovstva, pa onda i u oblasti rada aerodroma, pojavljuje se **sigurnost** (engl. *Safety*).

Ne ulazeći u vremenske okvire nastanka, može se reći da skoru u isto vrijeme kao i u sigurnosti, i u oblasti **zaštite** (engl. *Security*) u zrakoplovstvu se pojavljuje zahtjev za upravljanjem rizicima, često terminološki prepoznat kao procjena ugroženosti ili procjena uticaja.

Slijedeća oblast u zrakoplovstvu u kojoj može se prepoznati uspostavu sistema upravljanja rizicima je oblast **okolinskog upravljanja** (engl. Environment management system – EMS). Proces uspostave okolinskog upravljanja veže se više za spoljne uticaje i zahtjeve (zakonske, regulatorne, ugovorne i sl.), u odnosu na svjesnost i spremnost zainteresiranih strana u zrakoplovstvu za uvođenjem ovog sistema ili standarda. Slično kao i kod zaštite i ovdje se u prvom trenutku upravljanje rizicima terminološki uspostavlja kroz procjenu uticaja značajnih okolinskih aspekata koji mogu imati negativno dejstvo na okolinu.

Kada se posmatra rane faze sistema ili standarda **upravljanja kvalitetom** (engl. Quality management system – QMS), može se reći da nema eksplicitnog zahtjeva za upravljanje rizicima ili procjenom uticaja. Element u kome vidimo nagovještaje rizika su preventivne akcije. Prema ISO 9001:2000[4]: „Organizacija mora odrediti akciju radi eliminiranja uzroka potencijalnih neusklađenosti kako bi spriječila njihovo pojavljivanje."

Kao najmlađi standard početkom 2000-tih javlja se sistem za **upravljanje sigurnošću informacija** (engl. Information security management system – ISMS). Kao i kod sistema upravljanja kvalitetom, nema eksplicitnog zahtjeva za upravljanje rizicima ili procjenom uticaja. Element u kome se vidi nagovještaje rizika su preventivne akcije. Prema ISO 27001:2005[5]: „Organizacija mora odrediti akciju radi eliminiranja uzroka potencijalnih

---

[1] Georges Dionne, Risk Management: History, Definition, and Critique, First published: 21 October 2013.
[2] RBT (eng. *Risk Based Thinking*) – Razmišljanje zasnovano na riziku.
[3] https://www.nqa.com/medialibraries/NQA/NQA-Media-Library/PDFs/NQA-ISO-45001-Implementation-Guide.pdf, pristupljeno 07.12.2019 16:12.
[4] ISO 9001:2000 Quality management systems – Requirements.
[5] ISO 27001:2005 Information security management systems – Requirements.

neusklađenosti u odnosu na Information Security Management System (ISMS) zahtjeve, kako bi spriječila njihovo pojavljivanje".

U oblasti **zaštite na radu** (engl. *Occupational Health and Safety Standard - OHSAS*) najčešće imamo zakonski okvir koji uređuje ovu oblast, iako postoje i standardi i sistemi koji obuhvataju ovu oblast.[6] Najčešće poslodavac provodi mjere sigurnosti i zdravlja na radu poštujući načela procjene rizika, sprječavanja rizika, otklanjanja rizika na njihovom izvoru, kao i obavezu da vrši procjenu rizika za svako radno mjesto i utvrđuje poslove sa povećanim rizikom. Procjena rizika na mjestu rada treba da sadrži opis procesa rada sa procjenom rizika od povreda ili oštećenja zdravlja na mjestu rada u radnoj okolini i mjere za otklanjanje ili smanjivanje rizika na najmanju moguću mjeru u cilju poboljšanja sigurnosti i zdravlja na radu.[7]

U oblasti finansija razlikuje se: **internu reviziju** i **finansijsko upravljanje i kontrola** (FUK)[8]. Za internu reviziju karakteristično je da se izrađuju strateški i godišnji planova interne revizije baziranih na procjeni rizika. Finansijsko upravljanje i kontrola se zasniva na sistemu internih kontrola baziranim na rizicima.

3. ZAHTJEVI ZA UPRAVLJANJE RIZICIMA PRIMJENJIVI NA AERODROM SARAJEVO

U nastavku teksta biće izloženi osnovni zahtjevi koji su primjenljivi na procjene rizika za aerodrom:

QMS[9]

Polazeći od obaveze primjene europske norme EC 73/2010 ADQ, koja ima za predmet uređivanje oblasti aeronautičkih podataka i informacija, aerodromski operator po prvi put dobiva obavezu implementacije sistema upravljanja kvalitetom kroz ovu regulativu.

Sistem upravljanja kvalitetom ima zadatak da kroz: Politiku kvaliteta, Program osiguranja kvaliteta, Priručnike i procedure daje podršku u kreiranju, proizvodnji, pohranjivanju, upotrebi, obradi, transferu i distribuciji aeronautičkih podataka i aeronautičkih informacija.

Po prvi put se uvodi i preciznije određenje koji sistem upravljanja kvalitetom se može primijeniti, na način da „EN ISO 9001 certifikat, izdat od strane odgovarajuće akreditacijske organizacije, smatraće se zadovoljavajućim dokazom usklađenosti"[10]. Na osnovu ove mogućnosti, ISO 9001 postaje opće prihvaćeni sistem upravljanja kvalitetom u zrakoplovstvu, pa time primjenljiv i za aerodrome.

Zahtjev za upravljanje rizicima se izvodi iz ISO 9001:2015, tačka 6.1 Mjere za obradu rizika i prilika.[11] Posebno je potrebno naglasiti uvođenje i ove „pozitivne" komponente – prilika, čime se omogućuje ukupno sagledavanje konkretnih situacija.

---

[6] Kao jedan od najčešćih standarda pojavljuje se ISO 18001:2007 (OHSAS), odnosno standard ISO 45001:2018, koji je zamijenio OHSAS.

[7] EC 391/1989, kao i Zakon o sigurnosti i zaštiti na radu F BiH.

[8] FUK (eng. *FMC – Financial Management and Control*) – Finansijsko upravljanje i kontrola.

[9] QMS (engl. *Quality Management System*) – Sistem upravljanja kvalitetom.

[10] Regulation EC 73/2010 of the European Parliament and of the Council of 26 January 2010 laying down requirements on the quality of aeronautical data and aeronautical information for the single European sky.

[11] ISO 9001:2015 Quality management systems – Requirements.

Sigurnost

Sistem upravljanja sigurnošću (engl. Safety Management System – SMS) postavlja upravljanje rizicima kao jedan od ključnih mehanizama upravljanja sistemom. Upravljanje rizicima se sastoji iz: [12]

1. Identifikacije opasnosti;[13]
2. Sigurnosne procjene rizika i ublažavanja posljedica.

Identifikacija opasnosti je kombinacija reaktivnih, proaktivnih i prediktivnih metoda.

Sigurnosna procjena rizika i ublažavanje posljedica su posebni procesi koji osiguravaju analizu, procjenu i kontrolu sigurnosnih rizika koji su u vezi sa identificiranim opasnostima.

Često se miješaju područja primjene i nadležnosti između: sigurnosti u oblasti zrakoplovstva – safety i zaštite na radu – OHSAS. Da li je opasnost bitna za sigurnost u zrakoplovstvu ili zaštite na radu zavisi od potencijala opasnosti ili predvidivih posljedica ili rizika. Svaki rizik koji može imati uticaja (bilo direktno ili indirektno) na operativnu sigurnost zrakoplova ili opreme, proizvoda i usluga koji se odnose na zrakoplovnu sigurnost treba smatrati relevantnim za sigurnost u zrakoplovstvu. Opasnost koja ima čisto posljedice na zdravlje i radnu sposobnost radnika (znači bez ikakvog uticaja na zrakoplovnu sigurnost) treba odvojeno rješavati kroz OHSAS.[14]

Sigurnosni rizici povezani sa složenim opasnostima koje istovremeno utiču na zrakoplovnu sigurnost kao i na zdravlje i radnu sposobnost radnika mogu se upravljati kroz odvojene (paralelne) postupke. Alternativno, integrirani sistemi za smanjenje rizika u oblasti sigurnosti u zrakoplovstvu i u oblasti zaštite na radu mogu se koristiti za rješavanje takvih složenih opasnosti. Primjer složene opasnosti je udar groma u zrakoplov kada je zrakoplov u tranzitu na aerodromu. Inspektor OSHAS ovu opasnost može smatrati „opasnost na radnom mjestu“. Inspektor za zrakoplovnu sigurnost ovo posmatra kao opasnost od oštećenja zrakoplova i opasnost po putnike. Budući da posljedice nisu iste, potrebno je uzeti u obzir njihovo odvojeno upravljanje.

Zaštita

U oblasti zaštite – security, obaveza procjene rizika utvrđena je u ICAO Annex-a 17.[15]

Osnovni razlog je prihvatanje modernih mehanizama kroz procjenu rizika, a radi provođenje mjera i procedura u zaštiti civilnog zrakoplovstva od akata nezakonitog ometanja i djelovanja, pri čemu se ne ide u pravcu tehničkih detalja.[16]

Pomoću novorazvijene EU regulative, a u čijem fokusu je procjena rizika, zbog poboljšanja zaštite posebno su se razvijale[17]:

- Frekvencije i načini nadgledanja i patroliranja, odobrenih od strane nadležnih vlasti,
- Potencijalno problematični putnici (INAD),
- Roba i pošta označena kao visoko rizična.

---

[12] ICAO Annex 19 Safety Management.

[13] Prema ICAO Doc 9859 Safety Management Manual: Sigurnosni stručnjaci općenito definiraju opasnost kao stanje ili objekt koji može uzrokovati smrt, ozljede osoblja, oštećenje opreme ili konstrukcija, gubitak materijala ili smanjenje sposobnosti obavljanja propisane funkcije. U svrhu upravljanja rizikom sigurnosti u zračnom prometu, termin opasnost trebao bi biti fokusiran na one uslove koji mogu izazvati ili doprinijeti nesigurnom radu zrakoplova ili opreme u zrakoplovu, proizvodima i uslugama vezanim za sigurnost zrakoplova.

[14] ICAO Doc 9859 Safety Management Manual.

[15] ICAO Annex 17 Security.

[16] EC 300/2008 Common rules in the field of civil aviation security.

[17] EC 2015/1998 Detailed measures for the implementation of the common basic standards on aviation security.

Kao posebno važna izdvaja se EU regulativa za zaštitu mreža i informacijskih sistema (NIS)[18]. Formira se Europska agenciju za zaštitu mreže i informacija (European Network and Information Security Agency - ENISA[19]) sa zadatkom pružanja podrške i aktiviranja strateške saradnje između država članica u pogledu zaštite mrežnih i informacijskih sistema. Ključno je da sve države članice imaju minimalne mogućnosti i strategiju koja osigurava visoku razinu zaštite mrežnih i informacijskih sistema na svom području. Osim toga, ovi zahtjevi i informacije trebaju se primjenjivati na operatore osnovnih usluga i na pružatelje digitalnih usluga kako bi se promovirala kultura upravljanja rizikom i osiguralo prijavljivanje najtežih incidenata.

Cyber

Kao posebna važna oblast u savremenom poslovanju u svim domenima u oblasti zrakoplovstva uvodi se cyber opasnost ili cyber risk. Ovaj problem je mnogo kompleksniji i izlazi van okvira isključive zaštite – security i savremeni istraživači ovaj pojam više vežu kao zajedničku domenu: security, safety i operacija.

Transponiranjem zahtjeva iz oblasti cyber opasnosti u provedbeno zakonodavstvo o sigurnosti zrakoplovstva u cijeloj EU osigurava se da odgovarajuća tijela uspostave i provode postupke za razmjenu, ako je to primjereno i na praktičan i pravodoban način, relevantnih informacija radi pružanja pomoći drugim nacionalnim vlastima i agencijama, operatorima aerodroma, zračnim prijevoznici i drugim subjektima koji provode procjene sigurnosnog rizika u vezi sa svojim operacijama.[20]

Radno okruženje civilnog zrakoplovstva brzo se i značajno mijenja s primjenom novih naprednih tehnologija i komunikacijskih sistema prelazeći s ručnih procesa na efikasnije, automatizirane procese.

Operatori u zrakoplovstvu, uključujući operatore zrakoplova, operatore aerodroma, pružatelje usluga zračne navigacije itd. moraju identifikovati kritične informacione sisteme (softvera i hardvera) koji se koriste u njihovim operacijama, a koji mogu uključivati, ali nisu ograničeni na: [21]

a) sistemi za kontrolu pristupa i nadzor nad alarmom;
b) sistemi za procesuiranje putnika, prtljaga i robe[22];
c) sistemi za usklađivanja broja putnika i prtljaga (engl. *passenger and baggage reconciliation systems*);
d) sistemi za provjeru (engl. *screening*) i/ili sistemi za otkrivanje eksploziva, bilo da su umreženi ili rade u samostalnoj konfiguraciji;
e) regulirani agenti i/ili poznate baze podataka pošiljatelja;
f) sistemi upravljanja zračnim saobraćajem (ATM);
g) sistemi za rezervaciju putnika i sistemi za prijavu putnika;
h) sistemi za video nadzor (CCTV[23]);
i) zapovjedni, upravljački i dispečerski sistemi za zaštitu.

Kao obavezujući element postavlja se procjena opasnosti i rizika da bi se utvrdila ranjivost sistema i vjerovatnoća napada.

---

[18] EC 2016/1148 Measures for a high common level of security of network and information systems across the Union.

[19] ENISA (engl. *European Network and Information Security Agency*) – Europska agenciju za sigurnost mreže i informacija.

[20] EC 2019/1583 Detailed measures for the implementation of the common basic standards on aviation security, as regards cybersecurity measures.

[21] ICAO Doc 8973 Aviation Security Manual.

[22] DCS (engl. *Departure Control Systems*) – Sistemi za procesuiranje putnika, prtljaga i robe.

[23] CCTV (engl. *Closed-Circuit TeleVision*) – Sistemi za video nadzor.

EMS

Aerodromski operator nema eksplicitni zahtjev za uvođenjem sistema upravljanja okolinom, ali oni operatori koji su uveli ovaj standard zahtjev za upravljanje rizicima se izvodi iz ISO 14001:2015, tačka 6.1 Mjere za obradu rizika i prilika.[24]

ISMS

Ovo je prvi ISO standard koji je primijenio zajedničku visoku strukturu standarda (engl. *High level structure*), kojim se omogućava integracija više implementiranih ISO standarda u organizaciji sa zajedničkom osnovnom strukturom. Prema ISO 27001:2013, tačka 6.1 Mjere za obradu rizika i prilika uspostavlja se zahtjev za upravljanje rizicima i prilikama.[25] Važno je na ovom mjestu napomenuti da se u nastavku ovog zahtjeva upućuje na pitanja definirana u tački 4.1 ovog standarda, a praktično se radi o razumijevanju organizacije i njenog konteksta. U napomeni u ovom paragrafu se precizira da je utvrđivanje ovih pitanja definisano sa uspostavljanjem eksternog i internog konteksta organizacije razmatranog u tački 5.3 standarda ISO 31000:2009. Ovim smo praktično došli do izbora mogućeg sistema (standarda) za procjenu rizika i prilika.

OHSAS

Trenutno važeći Zakon u Federaciji BiH[26], nema jasnu i moderno definiranu metodologiju procjene rizika. U Članu 27. definiraju se radna mjesta sa posebnim uslovima rada, gdje postoje povećani rizici od povređivanja, nastanka profesionalnih oboljenja i oštećenja zdravlja radnika.

U prijedlogu novog zakona[27], koristi se EU regulativa 391/89, koja sadrži opće principe u vezi prevencije profesionalnih rizika, sigurnosti i zdravlja na radu i eliminacije rizika koji mogu izazvati nesretne slučajeve. Poslodavac treba da provodi mjere sigurnosti i zdravlja na radu poštujući opća načela prevencije:

a) procjene rizika,

b) sprječavanja rizika,

c) otklanjanja rizika na njihovom izvoru.

Interna revizija

Na početku treba napraviti jasnu razliku između interne kontrole (posmatrano kroz FUK) i interne revizije. Interna (unutarnja) revizija je naknadni nadzor, prije svega funkcioniranja sistema internih kontrola i ostvarenja poslovanja u skladu s usvojenim ciljevima.[28]

Kada se posmatra integralno sistem javne interne finansijske kontrole, vidi se da se sastoji iz:

– finansijskog upravljanja i kontrole (FUK),

– interne revizije,

– centralne harmonizacijske jedinice.

Interni revizori ovlašteni su vršiti sistematičan pregled i procjenu upravljanja rizikom i internih kontrola. Interni revizori procjenjivat će adekvatnost i efikasnost sistema finansijskog upravljanja i kontrole u smislu:

1. Identifikacije rizika, ocjene rizika i upravljanja rizikom od uprave organizacije;

---

[24] ISO 14001:2015 Environmental management systems – Requirements with guidance for use.

[25] ISO 27001:2013 lnformation security management systems – Requirements.

[26] *Zakon o zaštiti na radu* – „Službeni list SRBiH“, broj 22/90.

[27] NACRT *Zakon o sigurnosti i zaštiti na radu F BiH*.

[28] Boris Tušek i Sanja Sever, Uloga interne revizije u povećanju kvalitete poslovanja poduzeća u Republici Hrvatskoj (Empirijsko istraživanje), Zbornik Ekonomskog fakulteta u Zagrebu, Vol. 5, 2007.

2. Ispunjavanja zadataka i postizanja definiranih ciljeva organizacije;
3. Ekonomične, efikasne i djelotvorne upotrebe resursa;
4. Usklađenosti sa uspostavljenim politikama, procedurama, zakonima i regulativama;
5. Čuvanja sredstava organizacije od gubitaka kao rezultata svih vidova nepravilnosti;
6. Integriteta i vjerodostojnosti informacija, računa i podataka, uključujući procese internog i eksternog izvještavanja.[29]

FUK

Rizik je vjerovatnoća da će se desiti neki događaj koji može da utiče na ostvarivanje ciljeva. Upravljanje rizicima se definiše kao cjelokupan proces utvrđivanja, procjenjivanja i praćenja rizika za ostvarenje ciljeva, kao i preduzimanje potrebnih aktivnosti, posebno kroz sistem finansijskog upravljanja i kontrole, u svrhu smanjenja rizika.[30]

To je ciklus koji se kontinuirano odvija, a obuhvata utvrđivanje rizika, procjenu njihove vjerovatnoće i uticaja, preduzimanje mjera kao odgovor na rizike, dokumentovanje podataka o najznačajnijim rizicima i praćenje i izvještavanje o rizicima.

Preduslov za upravljanje rizicima je utvrđivanje ciljeva na različitim nivoima. Razvijen sistem upravljanja rizicima zahtijeva uspostavljanje kontrolnih aktivnosti koje su usmjerene ne samo na osiguranje zakonitosti, već i na realizaciju postavljenih ciljeva.

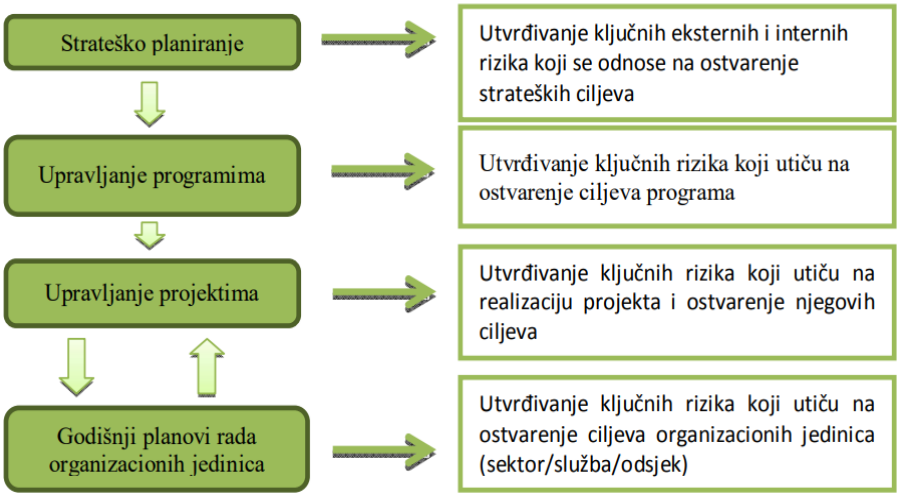
Upravljanje rizicima obuhvata aktivnosti vezane za razvoj procesa upravljanja, posebno planiranja i donošenja odluka, što uključuje:

- Utvrđivanje rizika u odnosu na ciljeve iz strateških i operativnih planova,
- Programa, projekata i aktivnosti, te poslovnih procesa,
- Procjenjivanje vjerovatnoće nastanka rizika i njihovih uticaja,
- Utvrđivanje načina postupanja po rizicima koji su neprihvatljivi,
- Dokumentovanje podataka o rizicima u registre rizika,
- Izvještavanje o najznačajnijim rizicima i aktivnostima u upravljanju rizicima,
- Mogućnost donošenja strategije upravljanja rizicima.

Sistem internih finansijskih kontrola, u skladu sa međunarodnim standardima za internu kontrolu zahtijeva da upravljanje rizicima postane sastavni dio postojećih procesa planiranja i upravljanja. Da bi upravljanje rizicima postalo sastavni dio procesa planiranja i donošenja odluka neophodno je da svaka institucija vrši procjenu rizika prilikom izrade planskih dokumenata (strateških, operativnih i finansijskih planova).

[29] *Zakon o internoj reviziji u javnom sektoru u Federaciji Bosne i Hercegovine.*
[30] Ministarstvo finansija BiH: Priručnik za finansijsko upravljanje i kontrolu.

Slika 1. Ključna područja za utvrđivanje rizika



Izvor: Ministarstvo finansija BiH: Priručnik za finansijsko upravljanje i kontrolu.

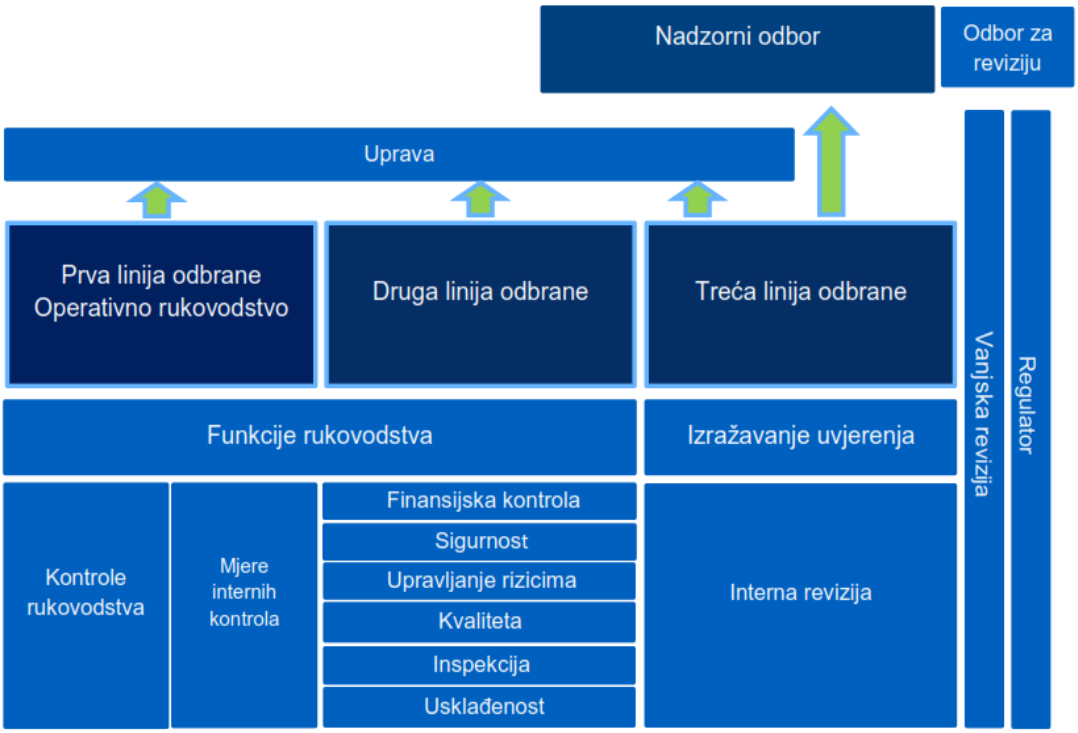
U modelu "Tri linije odbrane", interne kontrole koje uspostavlja operativno rukovodstvo smatraju se ***prvom linijom odbrane*** u upravljanju rizikom, jer je operativno rukovodstvo vlasnik rizika i direktno upravlja njime, a usto je odgovorno i za poduzimanje korektivnih mjera za otklanjanje nedostataka u funkcioniranju procesa i kontrola.[31]

Različite funkcije koje su u organizaciji uspostavljene u cilju upravljanja rizikom i funkcije za nadzor usklađenosti smatraju se ***drugom linijom odbrane*** i razlikuju se u zavisnosti od specifičnosti same organizacije, resora i nadležnosti (Tipične funkcije "druge linije" najčešće uključuju: funkciju upravljanja rizikom, funkciju usklađenosti koja vrši nadzor nad specifičnim rizicima neusklađenosti sa zakonom i pozitivnim propisima, kontroling – kao funkciju za nadzor finansijskih rizika i pitanja finansijskog izvještavanja).

Treću liniju odbrane predstavlja nezavisno uvjeravanje – interna revizija koja rukovodstvu osigurava značajno uvjeravanje u vezi efektivnosti procesa upravljanja, upravljanja rizikom i internih kontrola, uključujući i način na koji prva i druga linija odbrane ostvaruju ciljeve upravljanja rizikom i funkcioniranja internih kontrola. Interna revizija svoje uvjeravanje zasniva na visokom nivou nezavisnosti i objektivnosti koji nije moguć u funkcijama druge linije odbrane.

[31] Federalno Ministarstvo finansija: Priručnik za finansijsko upravljanje i kontrolu u javnom sektoru FBiH

Slika 2. Model "Tri linije odbrane"



Izvor: Federalno Ministarstvo finansija: Priručnik za finansijsko upravljanje i kontrolu u javnom sektoru FBiH

FUK se definira kao sveobuhvatan sistem internih kontrola koji uspostavljaju i za koji su odgovorni rukovodioci korisnika, a kojim se upravljajući rizicima osigurava razumno uvjeravanje da će se u ostvarivanju ciljeva budžetska i druga sredstva koristiti pravilno, ekonomično, efikasno i efektivno.[32]

4. USPOSTAVA SISTEMA UPRAVLJANJA RIZICIMA NA AERODROMU SARAJEVO

U nastavku teksta biće izloženi osnovni elementi uspostavljenih sistema procjene rizika za različite domene (oblasti) na Aerodromu Sarajevo.

QMS

Metodološki okvir za procjenu rizika u ovoj domeni je ISO 31000:2018. Proračun rizika se vrši na osnovu ocjene faktora rizika u odnosu na uspostavljene kriterije.

Matematski rizik se izračunava na osnovu formule:

$$R = U \cdot V = \frac{O_{\text{pasnost}} \cdot I_{\text{složenost}} \cdot P_{\text{osljedice}}}{O_{\text{tpornost}}} \cdot V_{\text{jerovatnost}} \qquad (1)$$

EMS

Metodološki okvir za procjenu rizika u ovoj domeni je ISO 31000:2018. Proračun rizika se vrši na osnovu ocjene faktora rizika u odnosu na uspostavljene kriterije.

[32] *Zakon o finansijskom upravljanju i kontroli u javnom sektoru FBiH.*

U domeni okolinskog upravljanja, rizici će se promatrati sa:

- Aspekta Zrak,
- Aspekta Voda,
- Aspekta Tlo.

Matematski rizik se izračunava na osnovu formule:

$$R = U \cdot V = \frac{O_{\mathbf{p}asnost} \cdot I_{\mathbf{z}loženost} \cdot P_{\mathbf{o}sljedice}}{O_{\mathbf{t}pornost}} \cdot V_{\mathbf{j}erovatnost} \quad (2)$$

ISMS

Metodološki okvir za procjenu rizika u ovoj domeni je ISO 31000:2018. Proračun rizika se vrši na osnovu ocjene faktora rizika u odnosu na uspostavljene kriterije.

U domeni sistema upravljanja sigurnošću informacijama, rizici će se promatrati sa:

- Aspekta Povjerljivost (Confidentiality),
- Aspekta Cjelovitost (Integrity),
- Aspekta Dostupnost (Availability)

Matematski rizik se izračunava na osnovu formule:

$$R = U \cdot V = \frac{O_{\mathbf{p}asnost} \cdot I_{\mathbf{z}loženost} \cdot P_{\mathbf{o}sljedice}}{O_{\mathbf{t}pornost}} \cdot V_{\mathbf{j}erovatnost} \quad (3)$$

Safety

Metodološki okvir za procjenu rizika u ovoj domeni je ISO 31000:2018. Proračun rizika se vrši na osnovu ocjene faktora rizika u odnosu na uspostavljene kriterije.

U domeni sistema upravljanja sigurnošću, rizici će se promatrati sa:

- Aspekta povrede uposlenika i oštećenja sredstava,
- Aspekta wildlife managementa.

Matematski rizik se izračunava na osnovu formule:

$$R = U \cdot V = \frac{O_{\mathbf{p}asnost} \cdot I_{\mathbf{z}loženost} \cdot P_{\mathbf{o}sljedice}}{O_{\mathbf{t}pornost}} \cdot V_{\mathbf{j}erovatnost} \quad (4)$$

Security

Rizik se može definirati kao stepen neizvjesnosti u ispunjenju zadanog cilja ili učinka (efekta) na ciljeve ili jednostavno kao umnožak vjerojatnosti da će se napad izvršiti, posljedica tog napada i ranjivosti koje mogu doprinijeti da se taj napad uspješno izvrši.

Matematski rizik se izračunava na osnovu formule:

$$R = U \cdot V = R_{\mathbf{a}njivost} \cdot P_{\mathbf{o}sljedice} \cdot V_{\mathbf{j}erovatnost} \quad (5)$$

FUK

Opis rizika je završetak procesa utvrđivanja rizika i početak procjene rizika. Utvrđene rizike je potrebno opisati na način da opis rizika obavezno sadrži informacije:

1. Uzrocima rizika (odgovara kriteriju ozbiljnost opasnosti za metodologiju prema ISO 31000:2018);
2. Posljedicama rizika (odgovara kriteriju posljedice opasnosti za metodologiju prema ISO 31000:2018).

Ako se želi imati objektivniju procjenu rizika, potrebno je dodati u opis rizika:

3. Pokazatelje rizika – postojeća saznanja koja ukazuju da su određene situacije rizične;
4. Faktore rizičnosti – karakteristike, događaji, okolnosti, trendovi koji mogu povećati vjerovatnost i uticaj rizika.

Procjena rizika uključuje procjenu uticaja i vjerovatnosti nastanka rizika.

Procjena uticaja su kriteriji po kojim se vrši ocjenjivanje uticaja. Najčešće je to nizak, srednji i visok uticaj.

Procjena vjerovatnosti su kriteriji po kojim se vrši ocjenjivanje vjerovatnosti. Najčešće je to niska, srednja i visoka vjerovatnost.

Ukupna izloženost riziku

Ukupna izloženost riziku predstavlja umnožak procijenjene razine uticaja rizika i procijenjene razine vjerovatnosti nastanka rizika.

$$R = U \cdot V \tag{6}$$

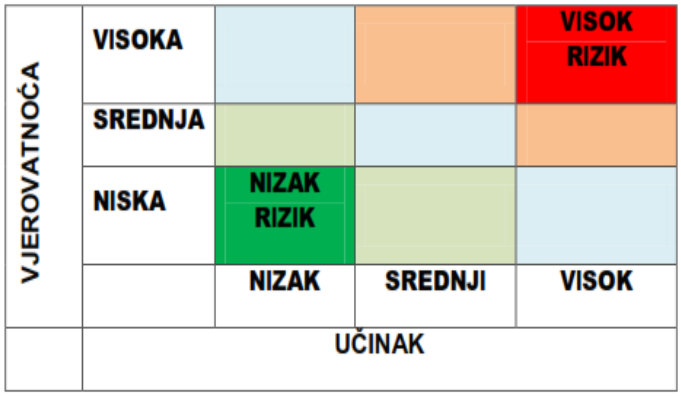
Interna revizija

Procjena rizika koju vrše interni revizori je način za procjenu slabih tačaka sistema. Cilj je izvršiti kategorizaciju slabih tačaka sistema prema rangu rizika. Rizici se često utvrđuju kroz razgovore sa rukovodiocima i zaposlenim, putem upitnika, kao i na osnovu iskustva i diskusija između samih revizora. Rukovodilac interne revizije ove aktivnosti treba predočiti rukovodiocu organizacije i predložiti ih na odobrenje.[33]

Nakon što se utvrde, rizike je potrebno procijeniti kako bi ih rangirali, utvrdili prioritete i dobili informacije za donošenje odluka o onim rizicima na koje se treba usmjeriti.

Procjena rizika je u suštini zasnovana na subjektivnoj ocjeni, uz korištenje različitih tehnika kako bi analiza bila sistematičnija i u određenoj mjeri objektivnija. Ove tehnike su potkrijepljene procjenom koju revizori donesu po pitanju prioriteta i učestalosti revizija i pomažu u identificiranju oblasti koje nose veliki rizik, koji se inače ne može identificirati na drugi način.

Slika 3. Matrica vjerovatnoće i učinka



Izvor: Metodologiju rada interne revizije u javnom sektoru u Federaciji Bosne i Hercegovine.

U primjeni ove metodologije procjene rizika, razmatraju se učinak koji proizlazi iz neostvarivanja ciljeva sistema i vjerovatnoća neuspjeha sistema.

Rezultat odluka se zapisuje u jednu od devet raspoloživih pozicija matrice, a to pokazuje da li se radi o sistemu visokog, srednjeg ili niskog rizika.

[33] *Metodologiju rada interne revizije u javnom sektoru u Federaciji Bosne i Hercegovine*.

5. ISKUSTVA I NAUČENE LEKCIJE IZ POJEDINAČNIH IMPLEMENTACIJA UPRAVLJANJA RIZICIMA NA AERODROMU SARAJEVO

Iskustva implementacije **QMS**, **EMS**, **ISMS** i **Safety** su pokazala ispravnost građenja zajedničke osnove tj. metodologije procjene rizika. Prije usvajanja zajedničke metodologije, procjena rizika se zasnivala na individualnoj procjeni pojedinih zaduženih radnika. Obično je ova procjena bila na početku poslovne godine, gdje su se utvrđivale značajne opasnosti ili značajni aspekti, vršena procjena rizika te su se provodile mjere i programi za ublažavanje posljedica ovakvih rizika.

Sa sigurnošću se može reći da ovaj proces nije bio zastupljen u cijeloj organizaciji, posebno ne na svim nivoima organizacije. Posljedica je bilo potpuno nerazumijevanje i osjećaj nepotrebnog ili stranog uticaja, često prihvaćen sa otvorenim neprijateljstvom. Procjena rizika nije bila sistematična, nisu se posmatrali događaji i okolnosti iz svakodnevnog života, nisu se sistematično prijavljivali događaji koji su imali ili posljedice ili su mogli dovoditi do određenih opasnosti.

Sa druge strane, zaduženi radnici za procjene rizika i upravljanje sistemima, držali su procjenu rizika skrivenom i na određen način „mističnim“ dijelom njihovog posla za šta su mislili da su bili školovani i kompetentni. Jedini koji su bili njima interesantni su bili najviše rukovodstvo. Izlažući njima rizike i opasnosti, u stvari su gradili svoje posebno mjesto i ulogu u organizaciji. Na ovaj način još više je dolazilo do otuđenja procjene rizika u organizaciji.

U ovoj fazi potpuno je nepoznat pozitivni element procjene rizika, tj. prilike. Ne posmatra se niti analizira interni i eksterni kontekst organizacije, pa se samim time ne vide prijetnje i prilike.

Sa uspostavljanjem zajedničke (principijelno slične) metodologije za ova četiri standarda, uspostavljen je proces integracije procjene rizika. U najosnovnijem obliku, a tiče se procjene operativnih rizika, dnevna događanja i promjene prije svega internog karaktera, a u posebnim slučajevima i eksternog karaktera, zaživljavaju. Događaji, incidenti i ozbiljne situacije sistematski se zabilježavaju, procjenjuje se potencijalna opasnost i na osnovu ovog vrši se procjena rizika prema oblastima. Obično se procjena vrši u radnim grupama u kojim učestvuju i specijalisti iz posmatrane oblasti. Kreiraju se stvarni akcioni planovi, pokreću korektivne mjere i uspostavljaju planovi za tretman prepoznatih rizika.

Rezultati koji se postižu su više nego očigledni, a najbolji pokazatelji efikasnosti su smanjenje i nestanak uzroka neusklađenosti, što posebno konstatuju zrakoplovne kompanije koje obavljaju letove sa Aerodroma Sarajevo. Značajna karakteristika je da nije kupljena „high tec“ aplikacija, upravljanje se vrši na jednostavnim bazama podataka u obliku tabela koje u potpunosti zadovoljavaju potrebe u praksi. Kao najvažnija stvar kod ponovljenih opasnosti je analiza prethodnih istih događaja, mjere koje su poduzimane, a ovim ponavljanjem ukazuju da nisu bile efikasne te iznalaženje novih rješenja, što u biti predstavlja proces stalnog poboljšanja.

U osnovi, ovakvim pristupom počinje zaživljavati poslovna praksa rada – razmišljanje/upravljanje zasnovano na rizicima.

Važno je napomenuti da se kroz procese i procesne liste, prepoznaju ciljevi procesa, prepoznaju se glavni rizici u procesima, a sve vezano za posmatrani vremenski period. Operativni ciljevi uspostavljeni u procesima su u liniji sa strateškim ciljevima koji se definiraju u trogodišnjem planu poslovanja, a koji predstavlja strateški plan Aerodroma Sarajevo.

U ovom periodu procjena rizika **interne revizije** i procjena rizika **zaštite – security** provode se odvojeno. Nema jasnih rezultata (nedostatak je očigledan na nižim nivoima, izvjesno postoje sastanci i analize na nivou najvišeg rukovodstva), pa time nema niti pokretanja

jasnih i mjerljivih mjera koje se poduzimaju za rješavanje opasnosti. **FUK** i **zaštita na radu** nisu implementirane, tako da se ove procjene rizika i ne provode.

Aerodrom Sarajevo generira veliki broj **projekata** koje izvodi ili samostalno ili angažovanjem spoljnih kompanija i pojedinaca. Veoma mali broj projekata je praćen sa procjenom rizika i upravljanjem rizicima. Za ovaj mali broj projekata koji imaju zastupljenu procjenu rizika, primijenjena je metodologija ISO 21500:2012.[34]

U 2019. godini se redefinisalo upravljanje rizicima u oblasti zaštite – security, tako da je ovo postala peta oblast za integrirano upravljanje rizicima na Aerodromu Sarajevo.

6. INTEGRIRANO UPRAVLJANJE RIZICIMA I PROMJENE SA NOVOM VERZIJOM STANDARDA ISO 31000:2018

Prema ISO 31000:2009, 3. Principi, Upravljanje rizicima je integralni dio svih organizacijskih procesa. Upravljanje rizikom nije samostalna aktivnost koja je odvojena od glavnih aktivnosti i procesa organizacije. Upravljanje rizikom dio je odgovornosti rukovodstva i sastavni je dio svih organizacijskih procesa, uključujući strateško planiranje i sve procese upravljanja projektima i promjenama.[35,36]

Ovako definisana integriranost daje potrebu uključenosti upravljanja rizicima u svakodnevnm životu organizacije.

U standardu ISO 31000:2018, 5.3 Integracija, po prvi put se eksplicitno traži da upravljanje rizicima predstavlja stalni zadatak za sve uposlenike. Upravljanje rizikom treba da bude dio svrhe organizacije, upravljanja, vođstva i posvećenosti, strategije, ciljeva i operacija, a ne odvojeno od njih.[37] Također, daje se akcenat na iterativnu prirodu upravljanja rizikom, uz napomenu da nova iskustva, znanje i analiza mogu dovesti do revizije elemenata procesa, radnji i kontrola u svakoj fazi procesa.

Za razliku od gore objašnjene integracije, integriranost upravljanja rizicima u različitim domenima, sa različitim metodologijama, a organizovano kao jedinstven, zajednički proces u svim dijelovima organizacije predstavlja drugu vrstu izazova.

Postavlja se vrlo jednostavan zadatak: Ako se ima jedan događaj, treba „proći“ kroz sve domene i vidjeti kakav je uticaj. Prolazeći kroz različite domene, treba se znati metodologiju za tu domenu te istu pravilno primjeniti na jedan događaj. U praksi se ovo pokazalo prilično kompleksno za pojedinačne procjene rizike, pa su se jako efikasnim pokazale radionice u kome su obavezno bili uposlenici koji su nosioci standarda i sisteme (npr. quality manager, environment manager, safety manager itd.). Na ovaj način smo praktično ostvarili integrirano upravljanje rizicima u različitim domenima.

Međutim, i dalje stoji činjenica da se na Aerodromu Sarajevo u jednom broju organizacionih jedinica veoma slabo ili nikako provodi upravljanje rizicima, da nedostaje ukupna svjesnost o upravljanju rizicima, posebno upravljanje rizicima u projektima.

7. ZAKLJUČAK

Upravljanje rizicima (prilikama) kao i nova poslovna filozofija – razmišljanje zasnovano na riziku, zahtijevaju od svih članove organizacije (na različitim nivoima i različite

[34] ISO 21500:2012 Guidance on project management.
[35] ISO 31000:2009 Risk management — Principles and guidelines.
[36] Ovako definisana integriranost u verziji standarda iz 2009 daje bolju sliku potrebe integriranosti upravljanja rizicima sa svim ostalim procesima.
[37] ISO 31000:2018 Risk management — Guidelines.

kompleksnosti) da kontinuirano procjenjuje pitanja koja utiču na rad, poslovanje organizacije i ostvarenje ciljeva.

Rizici i procesi upravljanja rizicima na aerodromu su inicijalno bili vezani za pojam sigurnosti, a u narednom periodu šire se na oblasti: zaštite, okolinskog upravljanja, upravljanja kvalitetom, upravljanja sigurnošću informacija, zaštite na radu, interne revizije, finansijskog upravljanja i kontrole i na kraju cyber.

Aerodrom Sarajevo je integrirao upravljanje rizicima u oblastima: upravljanja kvalitetom, okolinskog upravljanja, upravljanja sigurnošću informacija, upravljanja sigurnošću i upravljanja zaštitom. Događaji, incidenti i ozbiljne situacije sistematski se zabilježavaju, procjenjuje se potencijalna opasnost i na osnovu ovog vrši se procjena rizika prema oblastima. Obično se procjena vrši u radnim grupama u kojim učestvuju i specijalisti iz posmatrane oblasti. Kreiraju se stvarni akcioni planovi, pokreću korektivne mjere i uspostavljaju planovi za tretman prepoznatih rizika.

Prema ISO 31000 (verzije 2009 i 2018) upravljanje rizicima je integralni dio svih organizacijskih procesa i upravljanje rizicima predstavlja stalni zadatak za sve uposlenike. Upravljanje rizikom nije samostalna aktivnost koja je odvojena od glavnih aktivnosti i procesa organizacije. Upravljanje rizikom dio je odgovornosti rukovodstva i sastavni je dio svih organizacijskih procesa, uključujući strateško planiranje i sve procese upravljanja projektima i promjenama. Na Aerodromu Sarajevo nije u potpunosti zastupljena ovakva integriranost kada se posmatraju organizacione jedinice i procesi, nedostaje ukupna svjesnost o upravljanju rizicima, posebno upravljanju rizicima u projektima.

Summary:

INTEGRATED RISK MANAGEMENT AT SARAJEVO AIRPORT

Risk Management (Opportunities) and New Business Philosophy - Risk-based thinking require all members of the organization (at different levels and with different complexity) to continually evaluate issues that affect the organization's work, operations and goals. Risks and risk management processes at the airport were initially related to the concept of safety, and in the following period are expanding in the areas of: security, environmental management, quality management, information security management, occupational safety, internal audit, financial management and control and finally cyber. Sarajevo Airport has integrated risk management in the areas of: quality management, environmental management, information security management, security management and security management. Events, incidents and serious situations are systematically recorded, potential hazards assessed and risk assessed by area. Typically, assessments are made in working groups involving specialists in the field. Actual action plans are created, corrective action is taken, and plans are identified for the treatment of identified risks. According to ISO 31000 (2009 and 2018 versions), risk management is an integral part of all organizational processes and risk management is an ongoing task for all employees. Risk management is not an independent activity that is separate from the main activities and processes of the organization. Risk management is part of management responsibility and is an integral part of all organizational processes, including strategic planning and all project and change management processes. At Sarajevo Airport, such integration is not fully represented when looking at organizational units and processes, lacking overall awareness of risk management, especially project risk management.

Keywords: *Risk management, quality, security, protection, cyber.*

8. LITERATURA

1. Directive EC 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.
2. Directive EC 391/1989 of the European Parliament and of the Council of 12 June 1989 on the introduction of measures to encourage improvements in the safety and health of workers ar work.
3. Federalno ministarstvo finansija FBiH, Centralna harmonizacijska jedinica u Federaciji Bosne i Hercegovine, Metodologija rada interne revizije FBiH, Sarajevo, 2012.
4. Federalno ministarstvo finansija FBiH, Priručnik za finansijsko upravljanje i kontrolu u javnom sektoru FBiH.
5. Georges Dionne, Risk Management: History, Definition, and Critique, First published: 21 October 2013.
6. ICAO Annex 17 Security.
7. ICAO Annex 19 Safety Management.
8. ICAO Doc 8973 Aviation Security Manual.
9. ICAO Doc 9859 Safety Management Manual.
10. ISO 14001:2015 Environmental management systems – Requirements with guidance for use.
11. ISO 27001:2005 Information security management systems – Requirements.
12. ISO 27001:2013 lnformation security management systems – Requirements.
13. ISO 31000:2009 Risk management – Principles and guidelines.
14. ISO 31000:2018 Risk management – Guidelines.
15. ISO 9001:2000 Quality management systems – Requirements.
16. ISO 9001:2015 Quality management systems – Requirements.
17. Ministarstvo finansija i trezora BiH, Priručnik za finansijsko upravljanje i kontrolu.
18. NACRT Zakon o sigurnosti i zaštiti na radu F BiH.
19. Regulation EC 2015/1998 of the European Parliament and of the Council of 5 November 2015 laying down detailed measures for the implementation of the common basic standards on aviation security.
20. Regulation EC 2019/1583 of the European Parliament and of the Council of 25 September 2019 amending Implementing Regulation (EU) 2015/1998 laying down detailed measures for the implementation of the common basic standards on aviation security, as regards cybersecurity measures.
21. Regulation EC 300/2008 of the European Parliament and of the Council of 11 March 2008 on common rules in the field of civil aviation security and repealing Regulation (EC) No 2320/2002.
22. Regulation EC 73/2010 of the European Parliament and of the Council of 26 January 2010 laying down requirements on the quality of aeronautical data and aeronautical information for the single European sky.
23. Regulation EC 73/2010 of the European Parliament and of the Council of 26 January 2010 laying down requirements on the quality of aeronautical data and aeronautical information for the single European sky.
24. Službene novine Federacije BiH, broj 38/16, Zakon o finansijskom upravljanju i kontroli u javnom sektoru FBiH.
25. Službene novine Federacije BiH, broj 47/08, Zakon o internoj reviziji u javnom sektoru u Federaciji BiH.
26. Službene novine Federacije BiH, broj 65/18, Smjernice za upravljanje rizicima u javnom sektoru u Federaciji BiH.

27. Službeni list SRBiH, broj 22/90, Zakon o zaštiti na radu.
28. Tušek, B. i Sanja Sever, „Uloga interne revizije u povećanju kvalitete poslovanja poduzeća u Republici Hrvatskoj (Empirijsko istraživanje)“, Zbornik Ekonomskog fakulteta u Zagrebu, Vol. 5, 2007.
29. www.nqa.com/medialibraries/NQA/NQA-Media-Library/PDFs/NQA-ISO-45001-Implementation-Guide.pdf, (Pristupljeno 7.12.2019 16:12).