UDK 004.413.4

Matej Žderić, Ministarstvo unutarnjih poslova, Hrvatska
Davor Labaš, Ministarstvo unutarnjih poslova, Hrvatska, dlabas@fkz.hr

UPRAVLJANJE RIZICIMA SUKLADNO S ISO NORMAMA SIGURNOSTI – PODRUČJE INFORMACIJSKE SIGURNOSTI, SIGURNOSTI NA RADU I SIGURNOSTI HRANE

Sažetak

Standardi su prisutni u društvu već tisućama godina. Razvijali su se i napredovali kako je napredovalo i društvo. U moderno vrijeme gotovo je nemoguće zamisliti društvo u kojem ne postoje standardi jer su standardi zamjetni u gotovo svakom aspektu društva, te društvo bez njih ne bi moglo funkcionirati. Od posebne su važnosti standardi u području sigurnosti jer nam oni mogu pomoći da umanjimo vjerojatnost pojave i utjecaj neželjenih događaja poput hakerskih napada, ozljeda na radu i trovanja hranom. Radom su obuhvaćena tri standarda iz područja sigurnosti, standard ISO 27001 u području informacijske sigurnosti, standard ISO 45001 u području sigurnosti na radu i standard ISO 22000 u području sigurnosti hrane. Deskripcijom i elaboracijom, u radu su obuhvaćene glavne smjernice i aktivnosti, te su komparacijom izdvojene glavne posebnosti i sličnosti načina upravljanja rizikom u ovim specifičnim sustavima sigurnosti. Također, opisan je odnos i povezanost ovih „specijalističkih" područja upravljanja rizikom s mogućnostima općeg, generičkog pristupa upravljanju rizikom u organizaciji u skladu s normom ISO 31000 – upravljanje rizikom.

Ključne riječi: ISO standard 27001, ISO standard 45001, ISO standard 22000, upravljanje rizikom, ISO standard 31000.

1. UVOD

Upravljanjem rizicima želi se utjecati na učinkovitost organizacija u svim njihovim procesima i aktivnostima. Aktivnosti na upravljanju rizicima trebaju biti razmjerne razini rizika u organizaciji i usklađene s vrstom i specifičnostima područja u kojem se želi ostvariti svrha i cilj upravljanja rizicima. Svrha je upravljanja rizikom poboljšanje organizacije izvedbe neke aktivnosti ili više povezanih aktivnosti u procesu, a cilj je upravljanja rizicima da se provođenjem mjera utječe na vjerojatnost pojave rizika, da se smanji njegov učinak na način da se rizik eliminira ili zadrži na prihvatljivoj razini.

U ovome radu bit će prikazane glavne smjernice i aktivnosti u upravljanju rizikom u tri standarda na različitim područjima, ali pod zajedničkim nazivnikom „sigurnost“. Radom se nastoji prikazati glavne smjernice kojima organizacije putem izgradnje i održavanja sustava upravljanja sigurnošću na proaktivan i reaktivan način mogu upravljati rizikom u specifičnim područjima primjene standarda i to: standarda ISO 27001 u području informacijske sigurnosti, standarda u području sigurnosti na radu, ISO 45001 i standarda u području sigurnosti hrane ISO 22000.

Prema Hrvatskom zavodu za norme (u daljnjem tekstu: HZN), normom ili standardom smatra se dokument donesen konsenzusom i odobren od privatnog tijela, koji za opću i višekratnu uporabu daje pravila, upute ili značajke za djelatnosti ili njihove rezultate s ciljem postizanja najboljeg stupnja uređenosti u danome kontekstu. Norme bi se trebale temeljiti na provjerenim znanstvenim, tehničkim i iskustvenim rezultatima i morale bi biti usmjerene promicanju najboljih prednosti za društvo (HZN, 2018). Standardi i standardizacija prisutni su u društvu već tisućama godina, te su se razvijali i napredovali kako je napredovalo i društvo. U moderno vrijeme gotovo je nemoguće zamisliti društvo u kojem ne postoje standardi jer su standardi zamjetni u gotovo svakom aspektu društva, te društvo bez njih ne bi moglo funkcionirati; od korištenja interneta koji je reguliran internetskim protokolima do nošenja odjeće i cipela koje su regulirane standardima poput veličine. Od posebne su važnosti standardi u području sigurnosti jer nam oni mogu pomoći u nastojanju da umanjimo vjerojatnost pojave i utjecaj od neželjenih događaja poput hakerskih napada, ozljeda na radu i trovanja hranom.

Također, u posebnom poglavlju opisat će se osnovne značajke i ključni elementi norme ISO 31000 – upravljanje rizikom, koja pruža generalne smjernice za upravljanje rizikom u svim područjima sigurnosti.

1.1. Tema rada

Komparacijom i elaboracijom sustava upravljanja rizikom u različitim područjima sigurnosti koje reguliraju navedene norme, izdvojit će se one posebnosti ali i zajednički nazivnici koji znatno utječu na prilagođavanje procesa upravljanja rizikom posebnosti područja u kojem djeluju. Također, nastojat će se izdvojiti izravna povezanost „specijalističkih“ normi s općom, generičkom normom u području upravljanja rizikom ISO 31000.

Standarde je izdala Međunarodna organizacija za standardizaciju (engl. *International Organization for Standardization* - u daljnjem tekstu: „ISO“). Organizacija ‘’ISO’’ je neovisna, nedržavna, internacionalna organizacija čiji nastanak datira još iz 1964. godine, a sjedište joj je u Ženevi. Organizacija ujedinjuje 164 nacionalna tijela za standardizaciju, te putem stručnjaka iz raznih područja i njihovih ekspertiza razvija internacionalne standarde koje organizacije mogu primijeniti sa svrhom unaprjeđenja poslovanja.

2. PRAKTIČNI PRIMJERI ISO STANDARDA U PODRUČJU SIGURNOSTI

2.1. ISO 27000 - standardi u području informacijske sigurnosti

Informacija (podatak) je najvažnija valuta informacijskog doba (Calder, 2009:3). Informacije se također smatraju jednim od najvažnijih dijelova imovine (resursima) kojima organizacija raspolaže.

Porastom uporabe informacijske tehnologije u moderno doba, također su u porastu i prijetnje sigurnosti informacija i informacijskim sustavima raznih tvrtki. Porastom prijetnji od hakerskih napada, virusa i raznih drugih štetnih aplikacija kojima je svrha napraviti štetu informacijskom sustavu ili osobnom računalu, također je došlo do potrebe za razvijanjem i uspostavljanjem adekvatnih mjera i standarda informacijske sigurnosti. Jedna od najvažnijih zadaća organizacija u moderno doba jest uspostava djelotvornog sustava upravljanja informacijskom sigurnošću. Organizacija ''ISO'' razvila je seriju standarda i normi koje su mnoge međunarodne i domaće tvrtke primijenile na svoje poslovanje da bi unaprijedile razinu informacijske sigurnosti. U seriju standarda pod nazivom ISO 27000 uvršteni su desetci standarda koji se mogu rabiti kao vodič ili okvir za ustrojavanje djelotvornog ''sustava upravljanja informacijskom sigurnošću'' (engl. *Information security management System* u daljnjem tekstu: ISMS). Organizacija ''ISO'' i IEC (engl. *International Electrotechnical Comission*) zajedno su dio sustava za međunarodnu standardizaciju. Neke od najznačajnijih normi su sljedeće:

- ISO 27000: pregled normi iz serije 27000 te pojašnjenje tehničkih pojmova
- ISO 27001: sustav upravljanja informacijskom sigurnošću
- ISO 27002: kontrole i kodeks postupaka za upravljanje sigurnošću informacijskog sustava
- ISO 27003: vodič za implementaciju sustava informacijske sigurnosti
- ISO 27004: mjerenje i metrika učinkovitosti sustava informacijske sigurnosti
- ISO 27005: upravljanje rizicima informacijske sigurnosti
- ISO 27006: zahtjevi i dokumenti za postupak akreditiranja standarda.

ISO 27001 standard sadrži 14 poglavlja u kojima se nalaze odrednice za izgradnju sustava upravljanja informacijskom sigurnošću. U ''Aneksu A'' koji je dodatak ISO 27001 standardu, sadržani su kontrolni ciljevi i kontrole koje imaju svrhu identifikacije, smanjenja i upravljanja cijelog niza prijetnji informacijama s kojima se organizacija koristi u svakodnevnom poslovanju. Ovaj standard predstavlja veliku pomoć organizaciji u zaštiti cijelog informacijskog sustava, te osigurava koherentnost aktivnosti organizacije s važećom zakonskom regulativom, također podiže razinu pouzdanosti sustava u slučaju katastrofe.

Kako bi se ostvarila zaštita informacijskog sustava, koherentnost i veća pouzdanost sustava ISO 27001, standard primjenjuje ''procesni pristup'' na implementiranje, rukovanje, nadzor, pregled, održavanje i unaprjeđenje u organiziranju sustava upravljanja informacijskom sigurnošću. Procesnim pristupom smatra se primjena sustava procesa unutar

organizacije, zajedno s identifikacijom i interakcijom između tih procesa, kao i njihovim upravljanjem. Procesnim pristupom za upravljanje informacijskom sigurnošću nastoji se potaknuti korisnike da prepoznaju **važnost**: prepoznavanja potrebe uspostavljanja sigurnosne politike i ciljeva informacijske sigurnosti; implementacije i korištenja kontrola za upravljanje rizicima informacijske sigurnosti unutar organizacije; kao i za cjelokupne rizike vezane za poslovanje; nadzora učinkovitosti i performansi sustava upravljanja informacijskom sigurnošću; konstantnog unaprjeđivanja sustava. Ukratko, procesom se smatra transformacija uloženog u učinak (*inputa* u *output*), te je za to potreban niz koraka ili aktivnosti koje rezultiraju planiranim ciljem. Učinak jednog procesa u većini slučajeva postaje *input* za drugi proces (Russel, 2018:9).

Važnost procesnog pristupa očituje se i kroz faze upravljanja informacijskom sigurnošću koje se temelje na uporabi Demingovog ''PDCA'' modela za upravljanje kvalitetom (engl. *Plan-Do-Check-Act-* u daljnjem tekstu „PDCA"), a on se primjenjuje na cjelokupni sustav upravljanja informacijskom sigurnošću (slika 2), ali i na svaki pojedini element sustava (slika 1); odnosno, strukturiranje svih procesa u sustavu upravljanja informacijskom sigurnošću. Svaki proces u sustavu upravljanja informacijskom sigurnošću, to jest svaki sigurnosni *zahtjev* ili *očekivanje* podvrgnut će se „PDCA" modelu koji obuhvaća nužne aktivnosti i procese koji su dijelovi faze upravljanja informacijskom sigurnošću što će naposljetku rezultirati kontroliranim aspektom informacijske sigurnosti. *Primjer* takvog zahtjeva može biti da propusti informacijske sigurnosti ne izazovu znatnu financijsku štetu organizaciji; takav zahtjev će se potom podvrgnuti „PDCA" modelu odnosno nužnim aktivnostima koje takav model propisuje. *Primjer* je očekivanja – da, u slučaju nekog ozbiljnog incidenta u organizaciji, primjerice hakiranja u računalni sustav organizacije, postoje ljudi koji su specijalno izučeni za postupanje u takvim situacijama.

Britvić (2013) navodi faze upravljanja informacijskom sigurnošću:

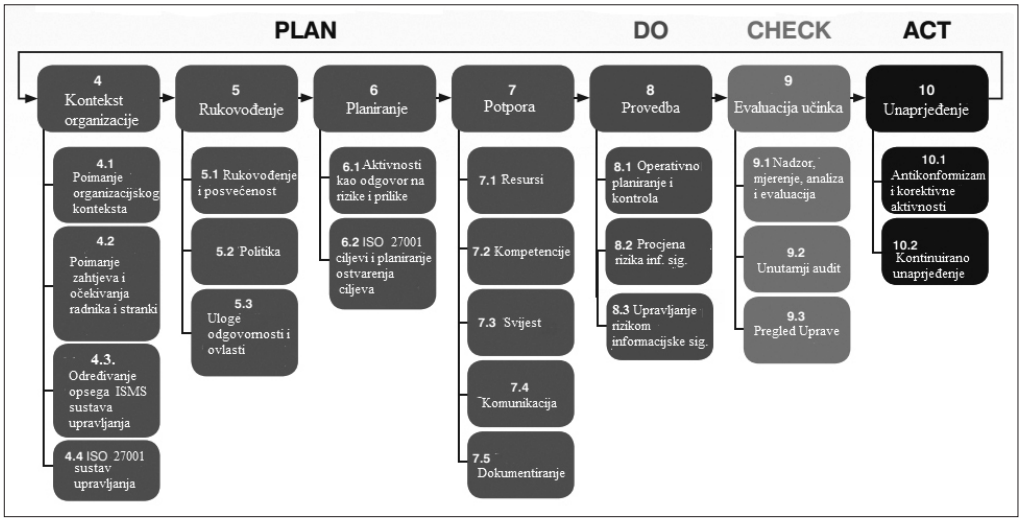
- Plan: faza planiranja (uspostava sustava za upravljanje informacijskom sigurnošću), uspostavljanje sigurnosne politike, ciljeva, procesa i postupaka koji su važni za upravljanje rizicima i unaprjeđenje informacijske sigurnosti. Faza planiranja služi organizaciji pri odabiru primjerenih mjera sigurnosti;
- Do: faza implementacije (upravljanje sustavom informacijske sigurnosti), implementacija i upravljanje sigurnosnom politikom, kontrola procesa i procedura. Sve što je isplanirano prilikom faze planiranja, provodi se u ovoj fazi;
- Check: faza provjere (nadzor i ispitivanje sustava informacijske sigurnosti), provodi se procjena i gdje je svrsishodno mjerenje procesnog nastupa protiv sigurnosne politike, ciljeva i praktičnog iskustva. U ovoj se fazi menadžmentu na preispitivanje dostavljaju izvješća s rezultatima. Svrha je ove faze provjera funkcioniranja informacijske sigurnosti i ispunjava li postavljene ciljeve;
- Act: faza djelovanja (poboljšanje sustava informacijske sigurnosti); svrha je ove faze poduzimanje preventivnih i korektivnih radnji na temelju rezultata koje je ustupio menadžment kako bi se osiguralo kontinuirano unaprjeđenje informacijske

sigurnosti. U ovoj se fazi nastoje poboljšati svi nedostaci informacijske sigurnosti koji su zamijećeni u prethodnoj fazi.

Slika 1. Prikaz PDCA ciklusa ISO 27001
Izvor: (Bogati, 2011:114)

Faze upravljanja sigurnošću trebaju se kontinuirano provoditi kako bi se umanjili rizici za povjerljivost, cjelovitost i dostupnost informacija (Britvić, 2013:4, prema „ISO", 2010.).

Bogati (2011) smatra da PCDA ciklus nikada ne završava nego se njegove aktivnosti ciklički ponavljaju kako bi se osigurala ažurnost sustava upravljanja sigurnošću informacijskog sustava.



Slika 2. PDCA model primijenjen na cjelokupni ISMS
Izvor: (prilagođeno prema Russell, 2018:8)

Planiranje je jedan od ključnih elemenata svakog sustava upravljanja, i prvi dio PDCA ciklusa koji se rabi da bi se odredile aktivnosti koje će dati odgovor na pitanje kako će funkcionirati sustav upravljanja. Propisuje preventivne aktivnosti, to jest dužnost organizacije da planira aktivnosti i postupa s prilikama i prijetnjama definiranim u kontekstu organizacije.

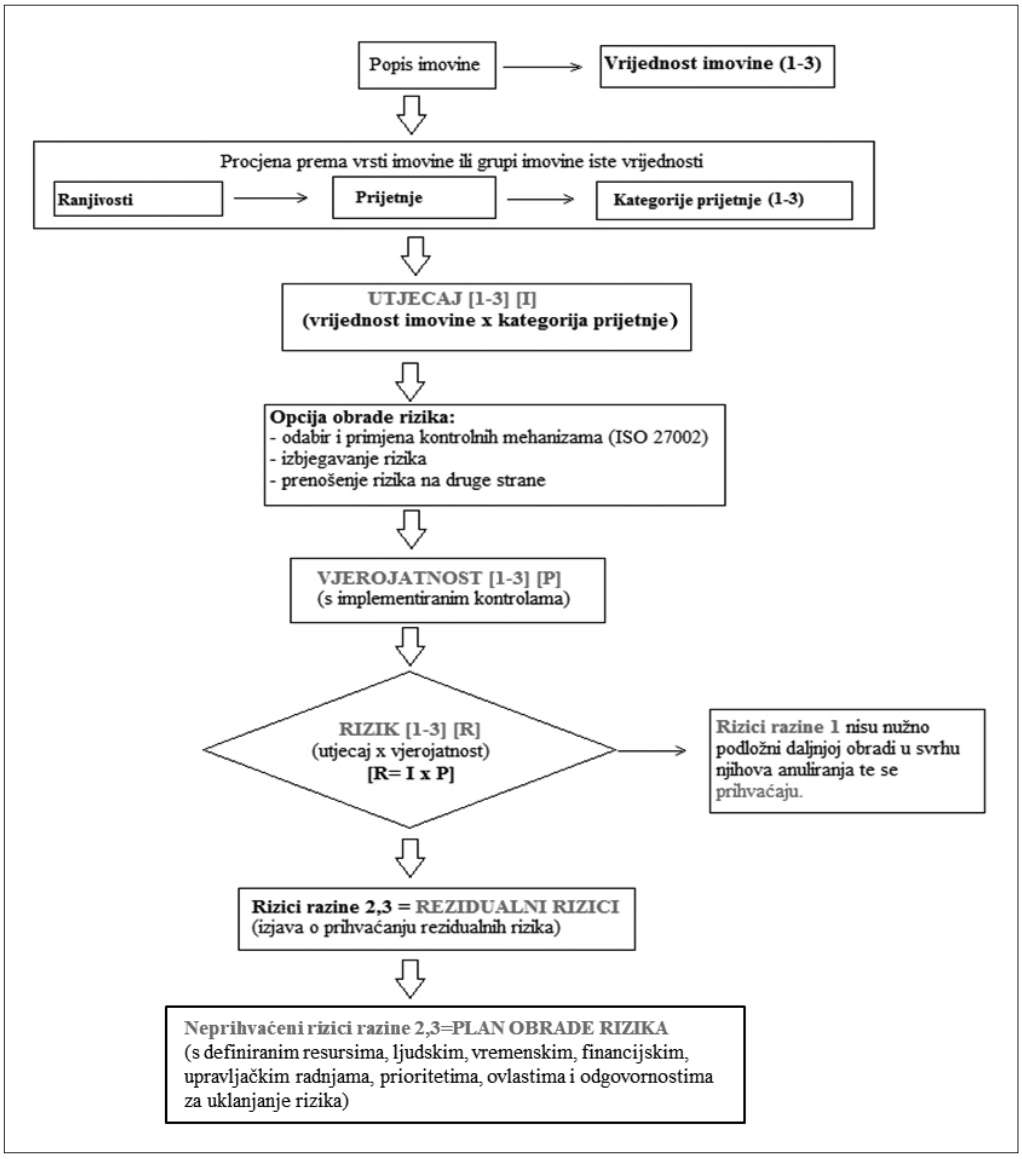
Kao dio poglavlja planiranja, procjena rizika u ovome koraku treba utvrditi prijetnje i ranjivosti organizacije. Sukladno s time potrebno je prepoznati ranjivosti svakog dijela imovine koja podržava kritične informacije organizacije. Takve ranjivosti u interakciji s prijetnjama mogu dovesti do nepoželjnih učinaka na kritične informacije i podatke. Prema ISO 27000, rizik je učinak neizvjesnosti ciljeva, odnosno djelovanje nesigurnosti na ciljeve organizacije, te najčešće predstavlja kombinaciju vjerojatnosti nekog događaja i utjecaja, odnosno posljedice tog događaja u slučaju realizacije prijetnji koje iskorištavaju neku od ranjivosti imovine (ISO/IEC 27000:2018(en)).

Šegudović navodi, da se iz perspektive informacijske sigurnosti rizik (R) za određeni resurs procjenjuje procjenom njegove vrijednosti (engl. *asset value* – AV), ranjivosti tog resursa (engl. *vulnerability* – V), prijetnji koje mogu iskoristiti te ranjivosti (engl. *threat*), vjerojatnosti realizacije prijetnji (engl. *probability*) i posljedici ili negativnom utjecaju koji se mogu dogoditi ukoliko se prijetnja realizira. Izraženo matematičkom formulom možemo reći da je rizik jednak funkciji prethodno navedenih varijabli (R= f (AV,V,T,P,I)). U konačnici svrha je procjene rizika da u prvome redu prepozna rizike, a potom da ih razvrsta i vrednuje. Uprava organizacije mora u skladu s rezultatima procjene rizika poduzeti potrebne radnje, to jest mora odrediti prioritete upravljanja informacijskim sigurnosnim rizicima i na rizike primijeniti prikladne kontrole. Za objektivnost i valjanost procesa procjene rizika potrebno je zadovoljiti kriterije jednoznačnosti, objektivnosti, pouzdanosti i repetabilnosti (Šegudović, 2006:6).

Prvi korak u fazi upravljanja rizikom odluka je organizacije o tome je li određeni rizik prihvatljiv ili nije, a potom je za svaki rizik koji je utvrđen u fazi procjene rizika potrebno donijeti plan obrade rizika. Plan obrade rizika mora sadržavati zadatke i odgovornosti, imena sudionika, prioritete uprave i druge podatke.

Sukladno s Planom obrade rizika moguće je donijeti nekoliko odluka u odnosu na način postupanja s rizikom, a to su:

- smanjenje rizika - primjenom odgovarajućih kontroli koje su uvrštene u normu ISO 27001, a pobliže opisane u normi ISO 27002,
- prihvaćanje rizika - rizik je moguće prihvatiti u određenim slučajevima, ali razlog prihvaćanja mora biti obrazložen i dokumentiran,
- izbjegavanje rizika - sprječavanje i prevencija aktivnosti koje bi izazvale rizik,
- prijenos rizika - delegiranje rizika na druge osobe, organizacije, suradnike (dobavljače, osiguranje) (Russell, 2013:19).



Slika 3. Primjer metodologije procjene rizika
Izvor: (Hofer, 2014:160)

Nakon donošenja odluke o načinu postupanja s rizikom postavljaju se ciljevi informacijske sigurnosti i implementiraju kontrole. Navedene kontrole i ciljevi uvršteni su unutar Aneksa A norme ISO 27001. Međutim, organizacija nije striktno vezana uz propisane kontrole, te ih može sama identificirati i izraditi. Nadalje, standardom je propisano da ciljevi moraju biti određeni i iskomunicirani na svim razinama organizacije, usklađeni s politikom

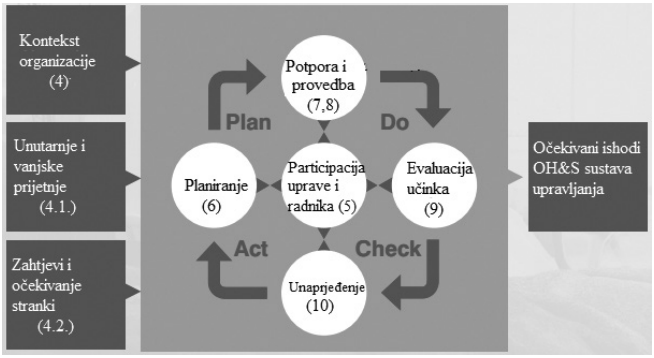
informacijske sigurnosti i mjerljivi. Ukratko, ciljevima se mora dati odgovor na pitanje što je potrebno učiniti, kada, kojim resursima, tko je za njih odgovoran i kako ih evaluirati.

2.2. ISO 45001 - standard u području zdravlja i sigurnosti na radu

ISO 45001 (ISO, 2018) je novi standard izdan od organizacije ''ISO'' 12. ožujka 2018. godine. Svrha je ISO 45001 standarda osiguranje sigurne radne okoline, povećanje učinkovitosti i zadovoljstvo zaposlenika organizacije, identificiranje i kontroliranje zdravstvenih i sigurnosnih rizika, smanjivanje potencijalnih rizika od nezgoda i manji broj dana bolovanja zaposlenika, te osiguranje usklađenosti sa zakonskim propisima te cjelokupno unaprjeđenje poslovanja organizacije. Norma ISO 45001 navedeno postiže uspostavom ''sustava upravljanja zaštitom zdravlja i sigurnosti na radu'' (engl. *Occupational Health and Safety Management System u daljnjem tekstu:* OH&S), to jest, uspostavlja se funkcionalni organizacijski okvir, koji se može primijeniti na svaku organizaciju bez obzira na veličinu, vrstu poslovanja i lokaciju s ciljem upravljanja i kontinuiranog poboljšanja zdravlja i sigurnosti na radu unutar određene organizacije. ISO 45001 standard je kompatibilan te se može primijeniti na organizaciju zajedno s drugim standardima ''ISO'' organizacije poput ISO 9001 (upravljanje kvalitetom), ISO 14001 (upravljanje okolišem) i ISO 27001 (upravljanje informacijskom sigurnošću).

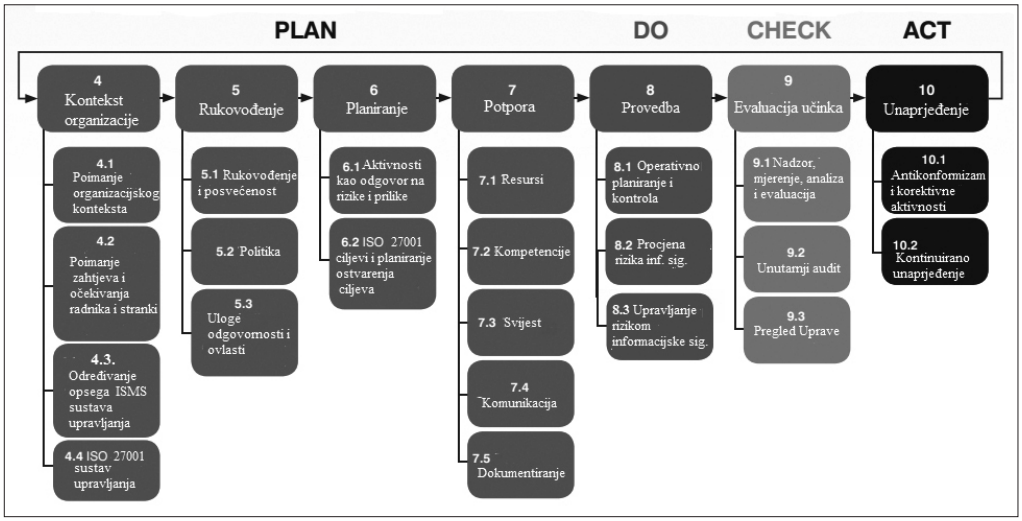
ISO 45001 standard jest dokument od 81 stranice, podijeljen u deset poglavlja u kojima je na detaljan način opisano kako implementirati standard u organizaciju, te stvoriti djelotvoran sustav upravljanja sigurnošću na radu. ISO 45001 također primjenjuje „PDCA" model kao ključan element sustavnog pristupa kojim se omogućava kontinuirano unaprjeđenje sustava upravljanja sigurnošću na radu kroz utvrđivanje djelotvornih rješenja, procjenu rezultata i implementiranje tih rješenja. „PDCA" model može se primijeniti na cjelokupni sustav upravljanja organizacije (slika 5), ali i na svaki pojedini element tog sustava (slika 4). Iz perspektive ISO 45001 standarda, PDCA model odnosi se na:

- Plan: shvaćanje konteksta organizacije kao i rizika i prilika zdravlju i sigurnosti na radu. Uspostava ciljeva, procesa i resursa nužnih za ostvarenje pozitivnih rezultata u području sigurnosti na radu;
- Do: implementiranje procesa poput participacije zaposlenika, identificiranja prijetnji i spremnosti na hitne slučajeve;
- Check: nadzor, mjerenje i evaluacija aktivnosti i procesa sigurnosti na radu;
- Act: kontinuirano unaprjeđenje sustava kroz poduzimanje aktivnosti poput pronalaska incidenata i neusklađenosti, te poduzimanje aktivnosti u skladu s rezultatima audita (Constantine, 2018).



Slika 4. Prikaz PDCA ciklusa ISO 45001
Izvor: (preuzeto i prilagođeno prema Constantine, 2018:9)

Jedan je od temeljnih postulata ISO 45001 standarda ''razmišljanje utemeljeno na riziku'' (engl. *Risk Based Thinking* - u daljnjem tekstu: RBT). Pod ovim elementom smatra se konstantna potreba uprave organizacije da procjenjuje potencijalne prijetnje sigurnosti na radu, te u skladu s njima osigura potrebne resurse i primijeni potrebne kontrole. RBT se osim na unutarnje, primjenjuje i na vanjske elemente organizacije, primjerice na nabavku i utjecaj isporučene robe i usluge na sigurnost na radu (Constantine, 2018:8).



Slika 5. PDCA model primijenjen na OH&S sustavu upravljanja
Izvor: (prilagođeno prema Constantine, 2018:9)

ISO 45001 standard koncipiran je na način propisan Aneksom SL, što znači da slijedi istu strukturu kao i ISO 27001. Slijedom navedenog osnovni su postulati ovog standarda slični kao i u standardu ISO 27001. Tangen i Warris (2012) tvrde da je Aneksom određeno da se standardi sastoje od istih deset poglavlja, te se zahtijeva ujednačavanje naziva i definicija što rezultira lakšom integracijom više različitih sustava upravljanja u poslovanje jedne organizacije.

U fazi planiranja planiraju se aktivnosti (poglavlje 6.1. – slika 5) kao odgovor na rizike i prilike koje uključuju identifikaciju opasnosti i procjenu rizika i prilika te određivanje zakonskih i drugih zahtjeva. Identifikacija opasnosti kao jedna od ključnih aktivnosti koja određuje uspješnost sustava upravljanja sigurnošću na radu, primjenjuje *''hijerarhiju kontrola''* pri procjeni rizika, te pomaže organizaciji u razumijevanju i prepoznavanju opasnosti na radnome mjestu. Ova metoda identifikacije opasnosti i procjene rizika mora ispunjavati sljedeće kriterije:

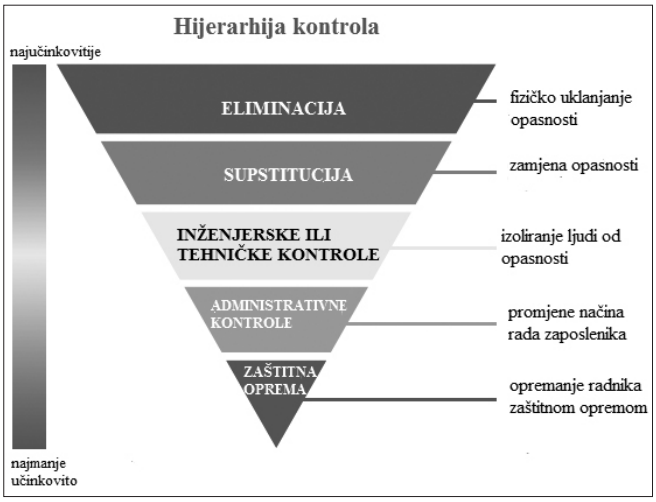
- mora omogućiti identifikaciju opasnosti i procjenu rizika za sve elemente organizacijske strukture (radnik, radni zadatak, sredstva za rad i radno okruženje), kao i identificirati i procijeniti sve rizike za sigurnost na radu vezane uz aktivnosti organizacije;
- mora se uskladiti s vrstom aktivnosti organizacije (nije ista metoda za identifikaciju opasnosti primjerice u uredskom poslovanju organizacije i proizvodnoj aktivnosti).

Nakon identifikacije opasnosti s ciljem ublažavanja rizika, planiraju se aktivnosti. Zadaća procjene rizika s propisanom odgovornošću rukovoditelja sadržana je u dokumentu organizacije *„Strateški plan sigurnosti na radu*“ koji se donosi na temelju određenih ciljeva sigurnosti na radu i periodično se pregledava.

U fazi provedbe (poglavlje 8. – slika 5) provodi se operativno planiranje i kontrola kojom organizacija definira što je nužno u svakom procesu za kontrolu zahtjeva kojima se osigurava sigurnost zaposlenika. Ključni element takvog planiranja i kontrole jest dokument *„Eliminacija opasnosti i ublažavanje rizika“* a kontrola se provodi na način da se primjenjuje hijerarhija kontrola na rizike (Constantine, 2018:9).

Prema ovom prikazu hijerarhije kontrola, najmanje je učinkovita kontrola opremanja radnika zaštitnom opremom, a najučinkovitija fizičko uklanjanje opasnosti.

U ovoj fazi provedbe, na temelju identifikacije opasnosti i procjene rizika, organizacija definira kako odgovoriti na *„hitne slučajeve*“. Primjer hitnog slučaja može biti izlijevanje opasnih kemijskih tvari, a kontrola kao odgovor jest podizanje uzbune i paljenje alarma, evakuacija i zatvaranje prostora gdje se izljev dogodio. Potrebno je i testirati spremnost na hitne slučajeve te osvijestiti zaposlene o mogućnosti takvih događaja, što se postiže propisanim testovima i treninzima. Primjer treninga kojim se testira spremnost na hitne slučajeve može biti vježba evakuacije, a provodi se paljenjem alarma, kontaktiranjem službi spašavanja, simuliranom evakuacijom, određivanjem odgovornosti zaposlenika itd. (Constantine, 2018:18)



Slika 6. Prikaz hijerarhije kontrola
Izvor: (prilagođeno prema Constantine, 2018:18)

2.3. ISO 22000 - standard u području sigurnosti hrane

U svrhu usklađivanja zahtjeva za upravljanje sigurnošću hrane na globalnoj razini, 19. lipnja 2018. objavljena je nova verzija standarda ISO 22000:2018: Food safety management systems (u daljnjem tekstu: FSMS).

Naglašena je veza između ISO 22000 i HACCP-a. U prehrambenoj industriji jedan od najvažnijih i najpoznatijih certifikata jest „Analiza rizika i kritične kontrolne točke" (engl. *Hazard Analysis Critical Control Point* – u daljnjem tekstu: HACCP). HACCP je sustavna metoda za utvrđivanje, procjenu i kontrolu opasnosti za sigurnost hrane, koja je nastala u Sjedinjenim Američkim Državama početkom 1960-ih. Danas je sustav HACCP međunarodno priznat i usklađen s postojećim standardima ISO 9001 i ISO 22000, a njegova je primjena obavezna u svim dijelovima svijeta i svim fazama proizvodnje hrane.

Provodi se kroz 7 osnovnih principa (Mortimore, Wallace, 2001:16):

- provođenje analize opasnosti – prikupljanje i procjena informacija o opasnostima i uvjetima koji dovode do njihove prisutnosti kako bi se moglo odlučiti koje su opasnosti značajne za sigurnost hrane te one moraju biti uključene u sustav i postupke temeljene na načelima HACCP sustava;
- utvrđivanje kritične kontrolne točke (engl. *Critical Control Points* – u daljnjem tekstu: CPP) – i provođenje kontrole, koja je ključna za sprječavanje ili uklanjanje opasnosti za sigurnost hrane ili smanjenje pojavnosti ili učinka opasnosti na prihvatljivu razinu (npr. kuhanje, hlađenje, pH);

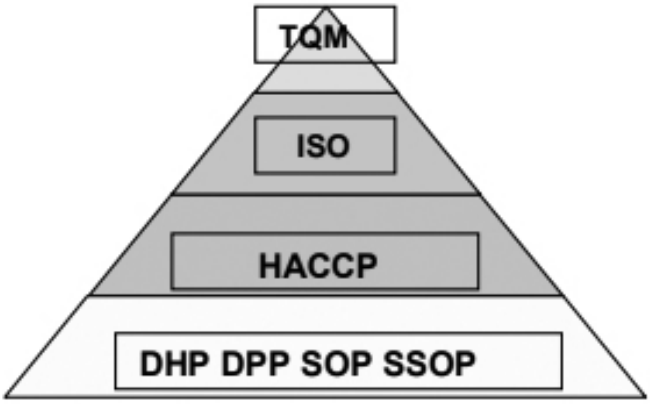
- utvrđivanje kritičnih granica koje su kriterij koji razdvaja prihvatljivo od neprihvatljivog;
- utvrđivanje sustava nadzora kontrole nad CCP-om;
- utvrđivanje korektivne mjere, tj. aktivnosti koja se mora poduzeti kada rezultati praćenja ukazuju na gubitak kontrole na kritičnoj kontrolnoj točki;
- utvrđivanje postupka za verifikaciju, tj. provjeru kod koje se pregledom i razmatranjem objektivnih dokaza utvrđuje funkcioniraju li uspostavljene validirane metode, procedure, ispitivanja;
- uspostavljanje dokumentacije svih postupaka.

Hrvatska agencija za hranu navodi da implementacija HACCP-a ima brojne prednosti kao što su: identifikacija i sprječavanje opasnosti u lancu hrane utemeljenih na znanstvenim istraživanjima, učinkovitiji nadzor i inspekcija na temelju vođene dokumentacije; sustav sljedivosti, odgovornost svih sudionika u proizvodnji i preradi hrane, te dovodi do razvoja međunarodne trgovine. (HAH, 2007)

Pahor, Jurčević, Marković (2005), našli su da HACCP sustav uspješno funkcionira samo uz realizaciju preduvjetnih programa (engl. *pre-requisite programme* - u daljnjem tekstu: PRP). To je zajednički naziv koji se rabi za opisivanje svih aktivnosti koje se primjenjuju uz HACCP plan, a koje utječu na zdravstvenu ispravnost hrane. Prema Pravilniku o pravilima uspostave sustava i postupaka temeljenih na načelima HACCP sustava (NN 68/15.), PRP-ovi su strukturalni, higijenski i drugi zahtjevi koje subjekt u poslovanju s hranom mora ispuniti te aktivnosti koje mora provoditi, a koji su potrebni za održavanje higijene u cijelom lancu hrane. Za razliku od kritičnih kontrolnih točki, PRP-ovi nisu specifični za određeni korak procesa i ne kontroliraju određenu opasnost. Preduvjetni programi sastoje se od:

- dobre higijenske prakse (engl. *good hygiene practices*, u daljnjem tekstu: GHPs);
- dobre proizvođačke prakse (engl. *good manufacturing practices*, u daljnjem tekstu: GMPs);
- standardnih operativnih postupaka (u daljnjem tekstu: SOP);
- standardnih sanitacijskih operativnih procesa (engl. *standard sanitation and operating procedures*, u daljnjem tekstu: SSOP).

HACCP se zasniva na preduvjetnim programima, a sam je poslužio kao temelj za nastanak standarda ISO 22000 (slika 7). Svi sudionici lanca hrane moraju provoditi PRP-ove, prije nego što u poslovanju počnu primjenjivati postupke utemeljene na HACCP-u. Proces dizajniranja i implementacije sustava za upravljanje sigurnošću hrane u organizaciju ovisan je o mnogim faktorima, posebno opasnostima za sigurnost hrane, te o veličini i strukturi organizacije. Jedan od ključnih ciljeva standarda ISO 22000 jest njegova usklađenost s principima HACCP-a, a HACCP plan je ključni dokument standarda. Međutim, postoje razlike između HACCP-a i ISO standarda, koji ide dalje od same sigurnosti hrane i uključuje proces i strukturu poslovanja.



Slika 7. Odnos preduvjetnih programa, HACCP-a i ISO standarda
Izvor: (Pahor, Jurčević, Marković, 2005:3)

ISO (ISO, 2018) 22000 međunarodni je standard koji je priznat širom svijeta jer usklađuje nacionalne i međunarodne standarde uzimajući u obzir principe HACCP-a. Ovaj standard uključuje seriju osnovnih zahtjeva za sigurnost hrane koje se primjenjuje na sve vrste organizacija i tvrtki koje se bave proizvodnjom hrane, od obiteljskih farmi do multinacionalnih tvrtki. Sve navedene organizacije koje su dio lanca hrane moraju uspostaviti *Sustav upravljanja sigurnošću hrane* (u daljnjem tekstu: FSMS), te spomenutog koristiti kako bi se spriječili mogući štetni učinci na ljudsko zdravlje. Nova verzija standarda ISO 22000 objavljenja je 2018. godine i usklađena s drugim standardima iz „ISO" serije, s ciljem uspostavljanja jedinstvenog sustava upravljanja unutar organizacije i integracije s ostalim „ISO" standardima. Do lipnja 2021. godine, sve tvrtke moraju obaviti tranziciju na novu normu, a ISO 22000:2005 tada će biti povučen.

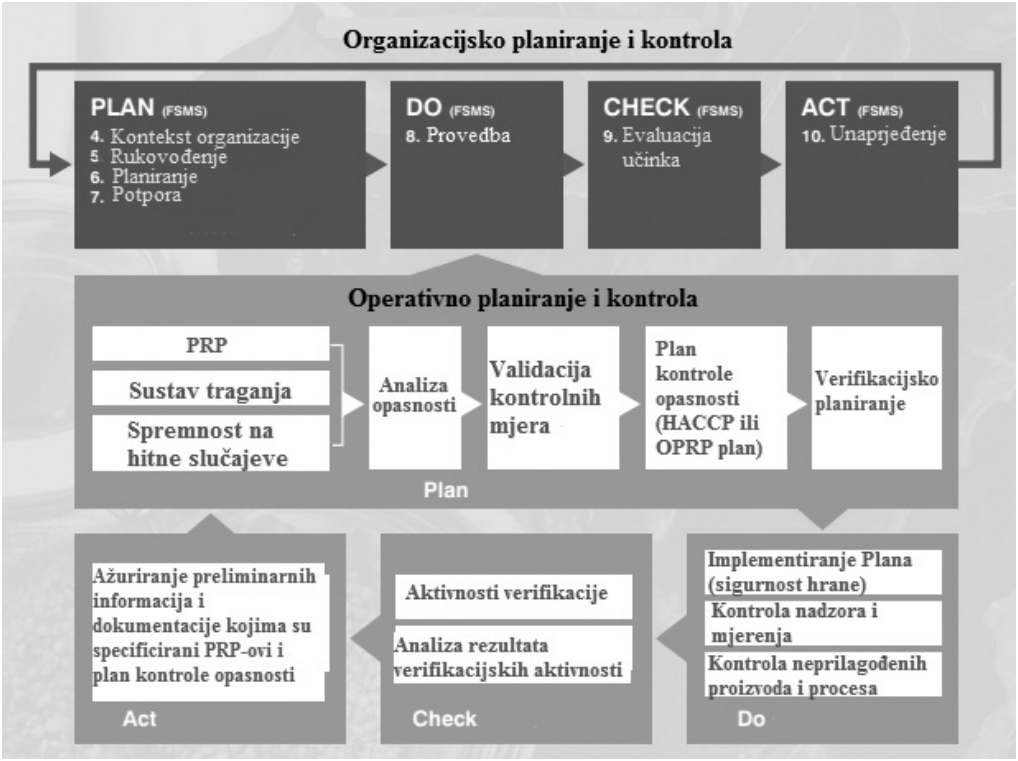
Najvažnije promjene i novosti koje je donijela nova verzija standarda jesu:

- HLS - olakšava korištenje standarda i ima istu strukturu kao ostali ISO standardi;
- razmišljanje utemeljeno na riziku – odnosi se na različite pristupe riziku, što je ključno za postizanje učinkovitog FSMS-a, pri tome razlikujući rizik na organizacijskoj i operativnoj razini. Organizacija planira i provodi aktivnosti za rješavanje rizika na organizacijskoj razini, dok su rizici na operativnoj razini osnova za povećanje učinkovitost FSMS-a i postizanje boljih rezultata;
- „PDCA" ciklus - svaka faza uključuje 4 glavna elementa sustava kontinuiranog poboljšanja; koji se provodi u dva odvojena ciklusa, jedan pokriva sustav upravljanja, a drugi HACCP principe;
- proces rukovanja - daje detaljan opis razlika među ključnim terminima, kao što su kritične kontrolne točke, preduvjetni programi i operativni preduvjetni programi (engl. *Operational prerequisite programme* – u daljnjem tekstu: OPRP) (ISO, 2018).

OPRP je kontrolna mjera ili kombinacija kontrolnih mjera koje se primjenjuju za sprječavanje ili smanjenje *"značajne opasnosti za sigurnost"* (engl. *significant food safety hazard*) hrane na prihvatljivu razinu i gdje kriterij djelovanja i mjerenja ili promatranja omogućuje učinkovitu kontrolu procesa i/ili proizvoda, dok je PRP osnovni uvjet i aktivnosti koje su potrebne unutar organizacije i kroz lanac hrane za održavanje sigurnosti hrane. Kritična kontrolna točka korak je u procesu u kojem se primjenjuju kontrolne mjere za sprječavanje ili smanjivanje značajne opasnosti za sigurnost hrane na prihvatljivu razinu i definirane kritične granice i mjerenja.

„PDCA" ciklus u ovom standardu može se ukratko opisati:

- Plan: utvrđivanje ciljeva sustava i njegovih procesa, osiguravanje potrebnih sredstava, te određivanje rizika i mogućnosti;
- Do: obavljanje planiranoga;
- Check: praćenje i mjerenje procesa, proizvoda i usluga, analiziranje dobivenih rezultata i informacija, izvještaj o rezultatima;
- Act: ako je potrebno, poduzeti mjere za poboljšanje.

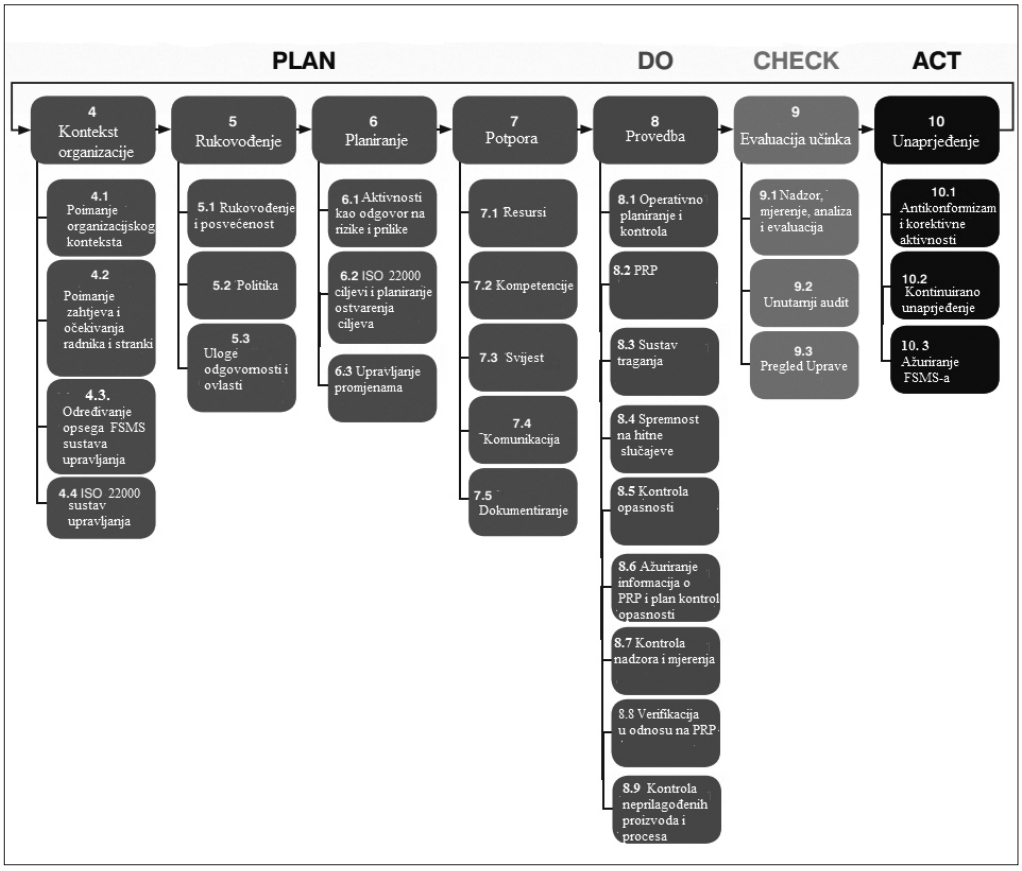


Slika 8. Prikaz PDCA ciklusa ISO 22000
Izvor: (prilagođeno prema Vaquero, 2018:7)

Prema Vaqueru (2018), koncept PDCA u ovome standardu odvija se u 2 ciklusa, pa je komunikacija između njih od izuzetne važnosti (slika 8):

- prvi ciklus odnosi se na organizacijsko planiranje i kontrolu i cjelokupni okvir FSMS-a, a uključuje kontekst organizacije, rukovođenje, planiranje i potporu te evaluaciju učinka i unaprjeđenje;
- drugi ciklus odnosi se na operativno planiranje i kontrolu i obuhvaća sve operativne procese unutar sustava za sigurnost hrane koji su opisani u fazi provedbe ovoga standarda.

Kombinirajući PDCA za upravljanje rizikom poslovanja i HACCP-a za identifikaciju, prevenciju i kontrolu opasnosti za sigurnost hrane, ISO 22000 pomaže organizacijama da smanje izloženost riziku i povećaju sigurnost. Osim toga standard određuje kako kontinuirano provoditi poboljšanje sustava upravljanja sigurnošću hrane.



Slika 9. Model PDCA primijenjen na FSMS
Izvor: (prilagođeno prema Vaquero, 2018:13)

U fazi organizacijskog planiranja kao i u prethodnim standardima jedna od ključnih komponenti sustava upravljanja jest utvrditi rizike i prilike te aktivnosti kao odgovor na njih (poglavlje 6.1. – slika 9). Na temelju utvrđenog konteksta i potreba i očekivanja stranki, akcijskim planom nužno je odgovoriti na pitanja što se želi postići, što nas može spriječiti u ostvarenju, kako odgovoriti na te prijetnje, kako se rizici mogu pretvoriti u prilike i kako ih iskoristiti, kada je potrebno poduzeti aktivnosti i tko će ih poduzeti i evaluirati te aktivnosti. ISO standard 22000 razlikuje dva tipa uspravljanja rizikom, obuhvaća standardne rizike koji imaju utjecaj na cijeli sustav upravljanja sigurnošću hrane, ali i na rizike koji mogu biti kontrolirani uspostavom i održavanjem PRP-a, OPRP-a i CCP-a.

U fazi provedbe (poglavlje 8. – slika 9), prvotno je potrebno utvrditi sposobnost organizacije za ispunjavanje zahtjeva standarda, te osigurati da su potrebne kontrole odabrane i primijenjene. Standard zahtijeva da se prije provođenja analize opasnosti, na temelju liste PRP-a, odaberu prikladni PRP-i (na temelju veličine, konteksta i aktivnosti organizacije) koji će pomoći organizaciji u kontroliranju sigurnosti hrane.

Standard (Food Standards Australia, 2017) zahtijeva uspostavu i dokumentiranje „sustava traganja" i uporabu i održavanje prikladne opreme koja služi za nadzor i mjerenje unutar sustava traganja. Potrebna je i uspostava sustava spremnosti na hitne slučajeve poput prirodnih katastrofa, potresa, sabotaža i provjera učinkovitosti sustava. Kontrolu opasnosti provodi tim za sigurnost hrane, te prije provođenja *Analize opasnosti* mora prikupiti relevantnu dokumentaciju o znanstvenim spoznajama, regulacijama, potrebama kupaca itd. *Analiza opasnosti* mora na temelju ozbiljnosti prijetnje i vjerojatnosti te pojave odrediti specifične mjere poradi prevencije ili ublažavanja opasnosti na prihvatljivu razinu. Nadalje, u pogledu kategorizacije kontrolnih mjera, potrebna je procjena za svaku mjeru pojedinačno o tome hoće li potpadati u OPRP ili CCP.

Nakon kategorizacije mjera donosi se *Plan kontrole opasnosti* koji sadržava podatke o poduzetim mjerama i vrstama opasnosti za sigurnost hrane koje su kontrolirane, akcijskim kriterijima, načinu nadzora aktivnosti, vrstama korektivnih aktivnosti i o tome tko ih poduzima. Nadalje, propisano je da kritične razine iz CCP-a i akcijski kriteriji iz OPRP-a moraju biti uspostavljeni na način da su podložni nadzoru i mjerenju, što organizaciji omogućava adekvatno postupanje ukoliko dođe do prelaska razina CCP-a i kriterija OPRP-a (neprilagođeni proizvodi). U dijelu standarda koji se odnosi na verifikaciju u odnosu na PRP-e i *Plan kontrole opasnosti* određeno je kako PRP, OPRP i CCP moraju biti implementirani i učinkoviti, te da razine opasnosti moraju biti na prihvatljivim razinama. U kontroli neprilagođenih proizvoda i procesa propisano je da zaposlenici koji su zaduženi za poduzimanje korektivnih aktivnosti moraju biti kompetentni, a aktivnosti se poduzimaju nakon nadmašivanja razina određenih OPRP-om i CCP-om, te proizvod koji je rezultat tih nadmašenih razina mora biti izoliran (prilagođeno prema Vaquero, 2018:25).

Potrebno je napomenuti kako je i HZN prihvatio ovaj standard kao ''HRN EN ISO 22000-Sigurnost hrane'' te je dio nacionalne regulative i sustava kontrole hrane.

2.4. ISO 31000 - Upravljanje rizikom

Prema normi ISO 31000 rizik se definira kao djelovanje nesigurnosti na ciljeve organizacije. Upravo iz razloga ostvarenja ciljeva organizacije primjenjuje se upravljanje rizicima.

Svrha upravljanja rizicima jest povećanje vjerojatnosti da će organizacije ostvariti svoje ciljeve kroz upravljanje prijetnjama i nepovoljnim situacijama, te da će biti spremne iskoristiti mogućnosti koje se mogu pojaviti (Adelsberger, 2015:5).

Poradi boljeg upravljanja rizicima unutar organizacije, te učinkovitijeg implementiranja sustava upravljanja koji će proaktivno djelovati na rizike, organizacija ''ISO'' dizajnirala je normu ISO 31000, koja je posljednji put nadograđena 2018. godine (HZN, 2018.). Nužno je napomenuti da ova norma nije propisana obligatornom za organizacije, te se organizacija po njoj neće certificirati (za razliku od ostale tri norme obuhvaćene ovim radom), ali potencijalno može biti od velike pomoći organizaciji budući da omogućuje veći stupanj vjerojatnosti postizanja ciljeva, poboljšano identificiranje prilika i opasnosti; uspostavlja učinkovit okvir za planiranje i donošenje odluka, pridonosi povjerenju dioničara – što u konačnici može rezultirati sigurnijim radnim okruženjem. Hrvatski zavod za norme također je usvojio normu ISO 31000 pod nazivom ''HRN ISO 31000-Upravljanje rizikom''.

Ova norma može pomoći organizacijama u uspostavljanju strategije, postizanju ciljeva i donošenju pravilnih odluka i tako pridonijeti zaštiti i stvaranju imovine i resursa koje organizacija posjeduje, što se očituje kroz ključne elemente ove norme, a to su načela, okvir i proces. Načela predstavljaju temelj za upravljanje rizikom te ih je potrebno uzeti u obzir pri uspostavljanju okvira i procesa upravljanja rizikom kako bi upravljanje bilo djelotvorno. Okvir upravljanja rizikom temelji se na PDCA ciklusu te u njeg potpadaju dodjela ovlasti i odgovornosti, integracija, dizajniranje, uspostavljanje, vrednovanje i poboljšanje upravljanja rizicima. Proces upravljanja rizicima karakterizira sustavna primjena politika, procedura i praksi s aktivnostima komuniciranja, utvrđivanje konteksta, nadzor, preispitivanje, dokumentiranje i izvještavanje o rizicima. Važan je element u ovoj fazi utvrđivanje konteksta, njime moraju biti obuhvaćeni ciljevi organizacije, utjecaj vanjske okoline na ostvarenje tih ciljeva, dioničari i vanjski suradnici, te se na temelju tih kriterija može ocijeniti priroda i složenost rizika organizacije (HZN, 2019., prilagođeno prema „*HRN ISO 3100-Upravljanje rizicima*“).

Potrebno je napomenuti kako norma ISO 31000 također primjenjuje koncept razmišljanja utemeljenog na rizicima ''RBT''. Norma ISO 31000 daje generičke smjernice za svaki korak u procesu upravljanja rizikom, te se na temelju tih smjernica kreira okvir upravljanja rizikom unutar organizacije. Uz ovu normu primjenjuje se i norma ''ISO 31010 - Upravljanje rizikom-Metode procjene rizika'' koja daje konkretne upute kako odabrati i u kojim slučajevima primijeniti određenu metodu za procjenu rizika.

Značajka je norme ISO 31000 okvir upravljanja rizikom ili koncept poznat pod nazivom ''organizacijsko upravljanje rizikom“, (engl. *Enterprise Risk Management*, u daljnjem tekstu: ERM). Prema Kentonu (2019) ERM je planirana poslovna strategija čiji je cilj identifikacija, procjena i priprema za bilo koju vrstu ugroze, opasnosti koja može spriječiti

organizaciju u ostvarenju ciljeva. Također, Gordon, Loeb i Tseng (2009) tvrde da je u moderno doba došlo do promjene paradigme organizacija u pogledu upravljanja rizikom, stoga organizacije u moderno doba moraju težiti holističnom pristupu upravljanju rizikom ili ''ERM''-u.

3. POSEBNOSTI I ZAJEDNIČKI ELEMENTI U PRIMJERIMA STANDARDA SIGURNOSTI – RASPRAVA

Sva tri analizirana standarda koriste Demingov „PDCA" model za upravljanje kvalitetom. To je sustavan pristup koji služi za upravljanje sustavom sigurnošću u području informacijske sigurnosti - ISO standard 27000, sustavom sigurnosti u području zaštite na radu ISO standard 450001, i u području sigurnosti hrane - ISO standard 22000. Sastoji se od 4 osnovne faze: faze planiranja, faze implementacije sigurnosne politike, faze provjere ili nadzora procesa sigurnosti na radu i faze poduzimanja aktivnosti na poboljšanju sustava sigurnosti u pojedinom području.

Usmjeravajući promatranje i analizu navedenih standarda na posebnosti i sličnosti u dijelu sustava upravljanja rizikom, možemo zamijetiti određene posebnosti pojedinih normi koje su, prije svega, prilagođene „prirodi" područja koje uređuje pojedina norma. Tako je norma 27001 prioritetno usmjerena u procjeni rizika na ranjivost u interakciji s prijetnjom. Polazna zadaća u takvom sustavu jest prepoznati ranjivosti ili slabosti svakog dijela imovine koja podržava kritične informacije i podatke. U fazi poduzimanja, norma 27001 za svaki utvrđeni rizik koji je neprihvatljiv za organizaciju donosi *„Plan obrade rizika"* kojim se određuje način postupanja s rizikom.

Norma ISO 45 001 u osnovi svojeg sustava sigurnosti ima *„razmišljanje utemeljeno na riziku*" (RBT) koje je usmjereno na prijetnje sigurnosti na radu vezane ne isključivo na unutarnje već i na vanjske elemente djelovanja organizacije, kao što su nabava robe i usluga i njihov utjecaj na sigurnost na radu. Identifikacija opasnosti ključna je aktivnost. Posebnost ove norme očituje se u činjenici da su identifikacija opasnosti i procjena rizika usmjerene na dva težišta. Prvi je usmjerenost na pojedine elemente organizacijske strukture koja provodi određenu aktivnost odnosno na identifikaciju opasnosti na zaposlene, sredstva za rad i radno okruženje; dok je drugo težište usmjereno na specifičnost samog procesa prema vrsti aktivnosti kao što su npr. proizvodnja nekog proizvoda u organizaciji, uredsko poslovanje u organizaciji, nabava i skladištenje nekog proizvoda i slično. Specifičnost je norme 45001 primjena hijerarhije kontrola na rizike u cilju eliminacije opasnosti i ublažavanja rizika sigurnosti na radu. Raspon u hijerarhiji kontrola kreće se od opremanja radnika zaštitnom opremom kao najmanje učinkovitom kontrolom do eliminacije odnosno fizičkog uklanjanja opasnosti kao najučinkovitijom kontrolom.

Kao jedna od značajnih posebnosti upravljanja rizicima u području norme ISO 22000 obveza je povezanosti između HACCP metode za utvrđivanje, procjenu i kontrolu opasnosti za sigurnost hrane koja se provodi kroz sedam koraka ili principa. Jedan je od principa ovog sustava kroz dijagram tijeka utvrđivanje kritičnih kontrolnih točaka u proizvodnji

i postupanju s hranom (CPP). Te točke postupanja s hranom podložne su kontroli radi otklanjanja, smanjivanja pojavnosti i učinka opasnosti za sigurnost hrane na prihvatljivu razinu. HACCP sustav funkcionira uspješno uz uvjet da se provode preduvjetni programi (PRP) koji se odnose na strukturalne, higijenske i druge zahtjeve koje mora ispuniti subjekt u poslovanju s hranom.

Norma 22000 u fazi poduzimanja aktivnosti na poboljšanju sustava sigurnosti kroz dokumente *„ Analiza opasnosti"* i *„Plan kontrole opasnosti"* donosi mjere radi prevencije ili ublažavanja opasnosti na prihvatljivu razinu s podacima o mjerama i vrstama opasnosti za sigurnost hrane, akcijskim kriterijima, načinu nadzora aktivnosti, vrstama korektivnih aktivnosti i o tome tko ih poduzima. Specifičnost je ISO 22000 standarda što razlikuje dva tipa upravljanja rizikom, obuhvaća standardne rizike koji imaju utjecaj na cijeli sustav upravljanja sigurnošću hrane, ali i na rizike koji mogu biti kontrolirani uspostavom i održavanjem PRP-a, OPRP-a i CCP-a.

Ono što je zajedničko i svakako uočljivo i važno kod norme 45001 i norme 22000 jest reakcija na hitne slučajeve, odnosno uspostava takvog sustava koji će spremno, primjenom odgovarajućih kontrolnih mjera reagirati na slučajeve opasnosti uzrokovane prirodnim katastrofama, potresima, sabotažama i drugim nepogodama koje mogu dovesti do katastrofalnih posljedica.

4. ZAKLJUČAK

ISO 31000 ''Upravljanje rizikom'' kao opća, generička norma, implementacijom uz navedene standarde sigurnosti može pružiti mnoge prednosti organizaciji. Naime, iako je upravljanje rizikom u tri standarda prezentirano ovim radom, nadogradnjom i integracijom u Aneks SL, uvršteno u sam sadržaj i upravljački okvir organizacije koja koristi pojedini standard – navedena norma ISO 31000 može i pored toga pružiti organizaciji generalne smjernice postupanja prilikom upravljanja rizikom te u konačnici osigurati sigurno okruženje u područjima primjene ovih standarda.

Povezanost ovih sustava naglašena je u pojedinim segmentima, pa tako zahtjev norme ISO 27001 navodi da je potrebno uzeti u obzir „unutarnji i vanjski kontekst organizacije" prema normi ISO 31000. Također, u poglavlju „Upravljanje rizikom informacijske sigurnosti" ISO 27001 standarda – navodi se da je upravljanje informacijskom sigurnošću ISO 27001 standarda usklađeno s ISO 31000 standardom. Svakako da je holistički pristup kroz stvaranje sveobuhvatnog okvira upravljanja rizikom (ERM) značajan doprinos norme ISO 31000 na području upravljanja rizikom u području sigurnosti.

Norma ISO 31000, kao i ostale norme prezentirane ovim radom, koncipirana je na način da se lako može integrirati u sustav upravljanja organizacije bez obzira na veličinu i vrstu djelatnosti. Ova norma nije usmjerena na upravljanje rizikom u specifičnom području sigurnosti poput informacijske ili sigurnosti na radu, nego predstavlja generalne upute (detaljno pojašnjenje termina i principa upravljanja rizikom, kao i pružanje općeg okvira za upravljanje rizikom) koje služe organizaciji pri organiziranju upravljanja rizikom.

LITERATURA

1. Adelsberger, Z. (2015). *Upravljanje rizicima prema ISO 31000: Temeljna norma za sve ISO sustave upravljanja.* HDK, Hrvatsko društvo za kvalitetu. Hrvatska: Bluefield, <http://www.hdkvaliteta.hr/file/articleDocument/documentFile/zdenko-adelsberger-upravljanje-rizicima-prema-iso-31000.pdf>. Pristupljeno 14.05.2019.
2. Bogati, J. (2011). Norme informacijske sigurnosti ISO/IEC 27K. *Praktični menadžment*: stručni časopis za teoriju i praksu menadžmenta, 2 (2), 112.-117. Ministarstvo obrane Republike Hrvatske, Odsjek za poslove obrane Virovitica.
3. Britvić, J. (2013). *Implementacija sustava upravljanja informacijskom sigurnošću temeljenog na normi ISO 27001:2010 s osvrtom na financijski sektor,* stručni rad. Virovitica: Visoka škola za menadžment u turizmu i informatici, <https://top-consult-grupa.hr/wp-content/uploads/2014/10/Josip-Britvi%C4%87-ISO-27001_2010-rad-2013.pdf>. Pristupljeno 19.12. 2019.
4. Calder, A. (2009). 2 Security based on ISO 27001/ISO 27002, Nizozemska: Van Harren Publishing.
5. Constantine, A. (2018). *ISO 45001:2018 Occupational Health and Safety Implementation Guide*, Velika Britanija: NQA.
6. Food Standards Australia (2017). *Food Traceability*, Australija: Food Standards Australija, <http://www.foodstandards.gov.au/industry/safetystandards/traceability/pages/default.aspx>. Pristupljeno 06.05.2019.
7. Gordon, L.A., Loeb, M.P., Tseng, C.Y. (2009). Enterprise risk management and firm performance: A contingency perspective, *Journal of Accounting and Public Policy*, 4 (28), 301.-327.
8. Hofer, D. (2016). Implementacija sustava upravljanja informacijskom sigurnošću ISO 27001:2013: *Koraci i prednosti. 14. Hrvatska konferencija o kvaliteti i 5. znanstveni skup za kvalitetu,* stručni rad. Baška, otok Krk, <https://issuu.com/svijet-kvalitete.com/docs/implementacija_sustava_upravljanja>. Pristupljeno 19.12.2019.
9. HZN (2019). Hrvatski zavod za norme, *HRN ISO 31000-Upravljanje rizikom,* Hrvatska, <https://www.hzn.hr/default.aspx?id=55>. Pristupljeno 21.5.2019.
10. HZN (2018). Hrvatski zavod za norme. Hrvatska, <https://www.hzn.hr/default.aspx?id=89>. Pristupljeno 05.05.2019.
11. HACCP (2007). Hrvatska agencija za hranu. Hrvatska: HAH, <https://www.hah.hr/arhiva/haccp.php>. Pristupljeno 08.05.2019.
12. ISO (2018) ISO/IEC 27000:2018(en): *Information technology — Security techniques — Information security management systems — Overview and vocabulary,* Velika Britanija: ISO, <https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-5:v1:en>. Pristupljeno 29.12.2019.
13. ISO (2018). ISO 22000:2018: *Food safety management systems - Requirements for any organization in the food chain*, Velika Britanija: ISO, <https://www.iso.org/obp/ui/#iso:std:iso:22000:ed-2:v1:en>. Pristupljeno 08.05.2019.

14. ISO (2018) ISO 45001:2018 *Occupational Health and Safety Management Systems*, Velika Britanija: ISO, <https://www.iso.org/standard/63787.html>. Pristupljeno 05.05.2019.

15. Kenton, W. (2019). *Enterprise Risk Management,* SAD: Investopedia, <https://www.investopedia.com/terms/e/enterprise-risk-management.asp>. Pristupljeno, 14.05.2019.

16. Mortimore, S.E.Wallace, C. A. (2001). *Food Industry Briefing Series: HACCP*, Ujedinjeno Kraljevstvo: Blackwell Science.

17. Pahor, Đ., Jurčević, V., Marković, I. (2005). *Preduvjetni programi za uspješnu implementaciju i održavanje HACCP sustava u ugostiteljskim objektima*, Hrvatska: 6. Hrvatska konferencija o kvaliteti, <https://issuu.com/kvaliteta.net/docs/pahor_d_rad2>. Pristupljeno 08.05.2019.

18. Russell, J. (2018). *ISO 27001:2013 Information Security Implementation Guide*, Velika Britanija: NQA, <https://www.nqa.com/medialibraries/NQA/NQA-Media-Library/PDFs/NQA-ISO-27001-Implementation-Guide.pdf>. Pristupljeno 05.05.2019.

19. Šegudović, H. (2006). *Prednosti i nedostatci metoda za kvalitativnu analizu rizika*, Hrvatska: IFIGO, <http://www.infigo.hr/files/INFIGO-MD-2006-06-01-RiskAsses.pdf>. Pristupljeno 06.05.2019.

20. Tangen, S., Warris, A.M. (2012). Management makeover - New format for future ISO management standards, Velika Britanija: ISO, <https://www.iso.org/news/2012/07/Ref1621.html>. Pristupljeno 08.05.2019.

21. Vaquero, M. (2018). *ISO 22000:2018 Food Safety Implementation Guide*, Velika Britanija: NQA, <https://www.nqa.com/medialibraries/NQA/NQA-Media-Library/PDFs/NQA-ISO-22000-Implementation-Guide.pdf>. Pristupljeno 09.05.2019.

22. Pravilnik o pravilima uspostave sustava i postupaka temeljenih na načelima HACCP sustava, NN 68/ 2015.

RISK MANAGEMENT ACCORDING TO ISO SECURITY STANDARDS – DOMAINS OF INFORMATION SECURITY, OCCUPATIONAL SAFETY AND FOOD SAFETY

Abstract

Standards have been part of the society for thousands of years. They have developed and progressed the same way society did. In modern times it is almost impossible to imagine society without standards because they have become part of every aspect of society and society can't function without them. Standards developed in security aspect are especially important because they can help us decrease the possibility and influence of unwanted events, etc. hacker attacks, work injuries and food poisoning. This paper covers three security standards: standard ISO 27001 in the information security domain, standard ISO 45001 in the occupational safety domain and standard ISO 22 000 in the food safety domain. Main guidelines and activities are covered using the description and elaboration method, while main specialities and similarities of risk management in this specific areas of security systems are also underlined. Also, it describes the relation between this „special" fields of risk management and possibilities of the basic, generic approach to risk management organisation accordingly to ISO 31000 standard – Risk management.

Keywords: ISO standard 27001, ISO standard 45001, ISO standard 22000, risk management, ISO standard 31000.