Siniša Radić
Univerzitet u Beogradu –
Ekonomski fakultet

Bojan Savić
Univerzitet u Beogradu –
Poljoprivredni fakultet

ZNAČAJ STANDARDA ISO 27001 U UPRAVLJANJU RIZIKOM OD PREVARE U BANKARSTVU

THE IMPORTANCE OF ISO 27001 IN FRAUD RISK MANAGEMENT IN BANKING

Apstrakt

U eri digitalne transformacije bankarskog sektora tehnološke inovacije postaju kritičan faktor razvoja. Da bi pružile blagovremene, pouzdane i cenovno prihvatljive usluge klijentima, banke su sve više usmerene ka digitalnim rešenjima. Podizanjem interakcije između klijenata i banaka na viši nivo kreira se i prostor za realizaciju novih pretnji i rizika. Jedna od najznačajnijih pretnji je prevara, koja može dovesti do značajnih gubitaka kako za banke, tako i za njihove klijente. Primenom digitalne tehnologije u bankarskom poslovanju tradicionalni oblici prevare su evoluirali i postali sofisticiraniji, tako da je neophodno dublje razumevanje načina na koji inovacije menjaju prirodu rizika od prevare. Nove okolnosti zahtevaju od banaka da se pobrinu da savremena rešenja ne utiču samo na unapređenje korisničkog iskustva, već i da se identifikuju novi izazovi u oblasti informacione bezbednosti, kao i da se pripremi adekvatan odgovor na njih. Efikasno upravljanje rizikom od prevare u savremenom bankarstvu podrazumeva razvijanje integralnog sistema za upravljanje informacionom bezbednošću koji je u funkciji sprečavanja, otkrivanja i odvraćanja od prevara. Budući da se radi o problematici koja je kompleksna, aktuelna i od opšteg značaja, ne samo u bankarstvu, Međunarodna organizacija za standardizaciju je izdala grupu standarda serije ISO 27000 koja se bavi pitanjima razvoja sistema za upravljanje informacionom bezbednošću.

U radu su predstavljeni ključni nalazi relevantnih istraživanja u kojima su se autori bavili izazovima, motivima i koristima na području implementacije standarda ISO 27001 u razvijanju sistema za upravljanje informacionom bezbednošću u bankama. Cilj rada je da se, uz uvažavanje svih koristi koje donosi harmonizacija na području informacione bezbednosti, učini i kritički osvrt, odnosno sagledaju negativne strane tog procesa. Od brojnih faktora zavisi u kojoj meri ***će*** *u konkretnom slučaju razvoj sistema za upravljanje informacionom bezbednošću doprineti efikasnijem upravljanju rizikom od prevare u bankama i generisanju koristi koje prevazilaze troškove. U istraživanjima koja su razmotrena u radu kao faktori od primarnog značaja izdvojili su se obučenost i svesnost zaposlenih i kultura etičnosti. Pojedini autori dodatno ističu važnost uspostavljanja ravnoteže između informacione bezbednosti i operativne efikasnosti.*

***Ključne reči**: rizik od prevare, ISO 27001, informaciona bezbednost, digitalna transformacija, bankarstvo*

***JEL klasifikacija**: M49, M15, G21*

Abstract

In the era of digital transformation of the banking sector, technological innovation is becoming a critical development factor. In order to provide timely, reliable and affordable services to clients, banks are increasingly relying on digital solutions. By raising the interaction with clients to a higher level, banks face new threats and risks. One of the most significant threats is fraud, which can lead to significant losses for both banks and their clients. With the application of digital technology in banking business, traditional forms of fraud have evolved and become more sophisticated, so a deeper understanding of how innovation is changing the nature of fraud risk is necessary. New circumstances require banks to ensure that modern solutions not only result in the improvement of user experience, but also to identify new challenges in the field of information security, as well as to prepare an adequate response to them. Effective fraud risk management in a modern banking implies the development of an integral information security management system, which has the function of preventing, detecting and fraud deterrence. Since it is an issue that is complex, current and of a general importance, not only in banking, the International Organization for Standardization (ISO) has issued a group of standards ISO 27000 that deals with development of information security management systems.

The paper presents the key findings of relevant research in which authors discuss challenges, motives and benefits in implementing ISO 27001 standard in banks. Besides all the benefits that come from harmonization in the field of information security, the goal of the paper is to make a critical review, that is, to look at the negative sides of that process. The extent to which the development of information security management systems will contribute to more effective fraud risk management in banks and the creation of benefits that exceed costs depends on the numerous factors. In the research that is discussed in the paper, the employees' training and awareness, as well as the ethic culture are pointed out as factors of primary importance. Certain authors additionally emphasize the importance of establishing a balance between information security and operational efficiency.

***Keywords**: fraud risk, ISO 27001, information security, digital transformation, banking*

***JEL classification**: M49, M15, G21*

1. Faktori promena i savremene tendencije u bankarskom poslovanju

U decenijama koje su iza nas banke su prolazile kroz proces stalnog prilagođavanja velikim promenama. Kreditno-depozitna aktivnost je ostala jezgro bankarske delatnosti, ali su se deregulacija, tehnološke inovacije i globalizacija poslovanja izdvojile kao glavni agensi promena u poslovanju i strategijama banaka (Goddard et al., 2007). Sedamdesetih godina prošlog veka započela je deregulacija bankarskog sektora u SAD i Evropi, čime su uklonjene barijere za cenovnu, geografsku i proizvodnu konkurenciju između banaka. Prva i druga direktiva Evropske Unije imale su značajan uticaj na liberalizaciju kretanja kapitala na prostoru zemalja članica EU. Direktive su bile usmerene na kreiranje jedinstvenog finansijskog tržišta u Evropskoj Uniji. Uvođenje evra kao jedinstvene valute u zemljama članicama Evro zone predstavljalo je dodatni podsticaj jačanju konkurencije na prostoru većeg dela EU. Konačno, primena Akcionog plana za finansijske usluge (Financial Services Action Plan) u EU od 1999. do 2004. godine dodatno je doprinela čvršćoj integraciji bankarskog sistema EU. Konkurenciju bankama predstavljale su i druge finansijske institucije koje su osmislile alternativne proizvode i usluge (polise životnog osiguranja, ugovore rentne štednje i sl.), ali i trgovinske i proizvodne kompanije, budući da su prepoznale ogroman potencijal dodatne zarade u pružanju finansijskih usluga kupcima. Deregulacija je stoga podstakla banke da prošire svoju aktivnost, kako u pogledu opsega proizvoda i usluga, tako i u pogledu teritorijalne prisutnosti. To je uticalo na unapređenje poslovne efikasnosti i diversifikaciju rizika. Međutim, druga strana deregulacije je sve izraženija konkurencija, kako od strane konkurentskih banaka, tako i od strane drugih finansijskih i nefinansijskih entiteta.

Transformaciji bankarskog poslovanja značajno je doprineo i tehnološki napredak, delujući na bankarske proizvode, usluge i poslovne procese. Pod tehnološkim razvojem se podrazumeva kako razvoj u sferi informacione tehnologije, tako i u oblasti finansijske tehnologije. Nove informacione tehnologije su omogućile bankama da smanje jedinične troškove, povećaju kvalitet i opseg usluga, unaprede dostupnost svojih proizvoda i usluga, što je ostvareno širenjem mreže bankomata, POS terminala, razvojem aplikacija za plaćanje i komuniciranje sa klijentima, učestalim elektronskim anketiranjem klijenata i slično. Prilikom godišnjeg izveštavanja, banke sve više pažnje u nefinansijskim izveštajima posvećuju informacijama o ulaganjima u nove informacione tehnologije i digitalizaciji poslovanja i usluga.

Revolucionarnim se ipak može smatrati sistem elektronskog plaćanja. Analiza efekata uvođenja sistema elektronskog plaćanja u finansijskom sistemu SAD (Berger, 2003) pokazuje da su uštede koje se na ovaj način ostvaruju enormne (troškovi papirnog materijala, štampe, zarada zaposlenih koji su vršili obradu dokumenata, troškovi arhiviranja dokumentacije). Međutim, ono što se dodatno može okarakterisati epohalnim je činjenica da je u potpunosti eliminisan značaj geografskih distanci i da su proizvodi i usluge banaka postali globalno dostupni. Istovremeno, razvoj finansijskih tehnologija je omogućio da banke efektivnije upravljaju rizicima i donose kvalitetnije odluke o strukturi portfolija.

Sve veću konkurenciju poslovnim bankama u sadašnjem vremenu predstavljaju i finansijsko-tehnološke kompanije (*Fin-tech companies*). Finansijsko-tehnološke kompanije pružaju alternativu tradicionalnim metodama vršenja finansijskih usluga i njihovo poslovanje je bazirano na stalnim inovacijama i novim tehnologijama. Područja na kojima ove kompanije trenutno najviše dolaze do izražaja su mobilno bankarstvo, investicione usluge i oblast kriptovaluta. Renominarini Forbes je na svojoj internet stranici (https://www.forbes.com/advisor/investing/top-fintech-companies/) objavio listu od deset najvećih finansijsko-tehnoloških kompanija u svetu po vrednosti u 2024. godini i na njoj su se u prvih pet našle sledeće kompanije (država gde se nalazi sedište kompanije i vrednost kompanije u milijardama američkih dolara navedeni su u zagradi respektivno): *Ant Group* (Kina, 78,5), *Stripe Inc.* (Irska, 50), *Revolut* (Velika Britanija, 33), *Chime Financial Inc.* (SAD, 25) i *Rapyd* (Velika Britanija, 15). Prema drugom izvoru (https://courses.cfte.education/ranking-of-largest-fintech-companies/), kao vodeće finansijsko-tehnološke kompanije po tržišnoj kapitalizaciji u 2024. godini navode se *Visa* (SAD, 557,8 mlrd USD), *Mastercard* (SAD, 427,9 mlrd USD), *Intuit* (SAD, 187,6 mlrd USD), *Fiserv* (SAD, 88,5 mlrd USD) i *Shopify* (Kanada, 75,7 mlrd USD). Imajući u vidu sve veći značaj novih vrsta finansijskih usluga, vremenom se javila i potreba za uvođenjem nove regulative. Osnovu takve regulative na prostoru EU predstavlja Direktiva za usluge plaćanja (*Payment Services Directive*) doneta od strane Evropske komisije (PSD, Directive 2007/64/EC, kasnije zamenjena sa PSD2, Directive (EU) 2015/2366), koja ima za cilj da reguliše usluge plaćanja i poslovanje vršilaca ovih usluga na području Evropskog ekonomskog prostora. Bez obzira na enormnu stopu rasta finansijsko-tehnoloških kompanija, ne treba prevideti i potencijalne izazove i pretnje njihovom daljem razvoju, a kao najvažniji se može istaći sigurnost podataka korisnika usluga.

Globalizacija kao treći bitan faktor koji utiče na trendove u savremenoj bankarskoj praksi može se sagledati i kao posledica prethodno opisanih uticaja – deregulacije i tehnološkog napretka. U cilju stvaranja preduslova za globalizaciju finansijskog sistema i bankarskog poslovanja, kao bitna pretpostavka nameće se usklađenost regulatornog okvira pod kojim se u različitom privredama odvija bankarska delatnost. Zbog toga je harmonizacija relevantne regulative koja je na snazi u različitim zemljama, odnosno njihovim finansijskim sistemima, veoma bitan korak u procesu globalizacije bankarskog poslovanja. U Evropskoj Uniji harmonizacija regulative u sektoru finansijskih usluga izvršena je u okviru programa jedinstvenog tržišta EU (*Single Market Program*), dok je harmonizacija zahteva koji se tiču adekvatnosti kapitala banaka propisana sporazumima koji su u praksi poznati pod skraćenim nazivima Bazel I (1988. god.), Bazel II (2006. god.) i Bazel III (2010. godine).

Na osnovu prethodnog možemo zaključiti da poslovanje savremenih banaka odlikuje visok intenzitet konkurencije i primena novih informacionih i finansijskih tehnologija, kao i da poslovanje ima globalni karakter. U takvim okolnostima nivo razmene informacija između banaka i okruženja je mnogo veći nego ranije, ali je veći i značaj informacija za donošenje adekvatnih poslovnih odluka. To potencira značaj preduzimanja neophodnih mera i aktivnosti usmerenih na unapređenje informacione bezbednosti banaka odnosno na zaštitu poverljivih informacija korisnika bankarskih usluga.

2. Glavne pretnje informacionoj bezbednosti i upravljanje rizikom od prevare

Imajući u vidu opšte društveno-političko stanje u 2022. godini, kao glavne pretnje informacionoj bezbednosti na internet stranici Evropskog parlamenta navedene su sledeće (https://www.europarl.europa. eu/topics/en/article/20220120STO21428/cybersecurity-main-and-emerging-threats):

- hakerski upadi korišćenjem softvera za preuzimanje kontrole (*ransomware*) - preuzimanje kontrole nad podacima od strane hakera uz zahtev za otkupom da bi se povratila kontrola,
- instaliranje *malware* softvera (virusi, crvi, "trojanci" i *spyware*) koji nanosi štetu u sistemu,
- pretnje socijalnog inženjeringa - korišćenje ljudske greške da bi se dobio pristup informacijama ili uslugama,

- pretnje usmerene na podatke - targetiranje izvora podataka u cilju dobijanja neovlašćenog pristupa podacima (kroz povredu ograničenja pristupa) ili zloupotrebom curenja podataka,
- pretnje usmerene na dostupnost koje se realizuju kroz nedostupnost tražene usluge,
- pretnje usmerene na dostupnost koje se realizuju putem nedostupnosti interneta,
- prenošenje netačnih informacija, bilo da se radi o informacijama koje su falsifikovane sa namerom ili o deljenju pogrešnih informacija, i
- napadi na lance snabdevanja, usmereni na odnose između poslovnih organizacija i dobavljača.

Uvidom u navedene pretnje informacionoj bezbednosti stiče se utisak da kod većine postoji direktan ili indirektan ekonomski motiv učinioca, odnosno da se u njima mogu prepoznati elementi prevare. U tom kontekstu se i sve aktivnosti preduzete na suzbijanju pretnji informacionoj bezbednosti mogu shvatiti i kao aktivnosti realizovane u procesu upravljanja rizikom od prevare. Jedna od definicija prevare u bankarskim poslovima sa stanovništvom navodi da je to bilo koji pokušaj učinioca "da ostvari finansijski dobitak na račun legitimnih klijenata ili finansijskih institucija kroz bilo koji kanal transakcija, kao što su kreditne kartice, debitne kartice, ATM uređaji, onlajn bankarstvo ili čekovi" (Sudjianto et al., 2010, str. 5). Pojedini autori prave razliku između prevare u kojoj je učinilac prevare korisnik usluga banke (*first-party fraud*) i prevare u kojoj je korisnik usluga žrtva prevare izvršene od strane učinioca koji je ukrao identitet korisnika, koristi njegovu izgubljenu ili ukradenu karticu, falsifikuje karticu ili dolazi do neautorizovanog pristupa računu korisnika usluga banke na drugi način (*third-party fraud*) (Greene, 2009).

Rizik od prevare je jedan od glavnih rizika koji može značajno ugroziti kako finansijske performanse, tako i imidž i reputaciju poslovnih entiteta. U klasifikaciji rizika, rizik od prevare je potkategorija operativnog rizika (Bessis, 2015). U poslednje vreme operativnom riziku se posvećuje velika pažnja, pogotovo u bankama i drugim finansijskim institucijama. Značajnu ulogu u potenciranju operativnog rizika u bankarskom sektoru ima regulativa Bazelskog komiteta za nadzor nad bankama (Bazelski standardi). Operativni rizik je rizik povezan sa greškama i događajima u obradi transakcija ili u drugim poslovnim aktivnostima. Sagledavanje rizika od prevare je u stvari razmatranje verovatnoće da do takvih grešaka ili događaja

dođe usled namernog čina osmišljenog da učinilac ostvari ekonomsku ili drugu korist. To podrazumeva sprovođenje detaljnih radnji od strane multidisciplinarnog tima koji čine pojedinci različitih profila. Međutim, ovo je isuviše usko posmatranje problematike upravljanja rizikom od prevare, budući da borba protiv prevara počinje pre izvršenja čina prevare i obuhvata širok spektar aktivnosti. U širem smislu, efektivna strategija borbe protiv prevara ima četiri glavne međuzavisne komponente, a to su (Chartered Institute of Management Accountants, 2008):

- sprečavanje (prevencija) prevara,
- otkrivanje (detekcija) prevara,
- odgovor na prevare i
- odvraćanje od prevara.

Sprečavanje prevara je u većini slučajeva ekonomičnije nego otkrivanje, istraživanje i oporavak od učinjenih prevara. Ipak, kod sprečavanja prevara treba imati meru i postupke treba uvoditi na bazi detaljne analize odnosa troškova i koristi. U savremenim uslovima sprečavanje prevara se može shvatiti i kao proces uspostavljanja i razvoja sistema za upravljanje informacionom bezbednošću (*Information Security Management System – ISMS*). Imajući u vidu kompleksnost informacionih tehnologija koje su danas u upotrebi, sprečavanje prevara se ne može svesti na listu radnji koje treba ili ne treba činiti. Stoga se upravljanje informacionom bezbednošću bazira na međunarodnim standardima koji daju uputstva kako postići željenu bezbednost informacija. Sistem za upravljanje informacionom bezbednošću se bazira na primeni principa standarnih internih kontrola na informacione resurse. Procesi tog sistema čine integralni deo sveobuhvatnog procesa upravljanja rizikom u poslovnim entitetima (*Enterprise risk management*). Svrha sistema za upravljanje informacionom bezbednošću je da se ostvare sledeći ciljevi (Hopwood et al., 2012):

- poverljivost - dostupnost samo ovlašćenim licima,
- integritet - tačnost (unos i obrada podataka bez grešaka) i potpunost (sprečavanje neovlašćenog dodavanja, uklanjanja ili izmene unetih podataka), kao i
- raspoloživost - u pravo vreme onima kojima je to neophodno, čime se potencira pravovremenost.

Pojam informacione bezbednosti se u savremenim uslovima percipira mnogo šire od ograničavanja pristupa informacijama neovlašćenim licima. Bezbednost informacija se sagledava na bazi ukupnog autputa informacione

bezbednosti (*information security deliverable*) koji je kruna sistema za upravljanje informacionom bezbednošću. Uspostavljanjem sistema se nastoje ostvariti poželjni autputi informacione bezbednosti, što u najširem smislu uključuje: procese povezane sa bezbednošću informacija, hardverske i softverske komponente, povezane usluge, efektivnu organizacionu strukturu, adekvatno okruženje, kao i kvalifikovan i posvećen kadar u profesiji (Hopwood et al., 2012). Prema tome, da bi se ostvario odgovarajući nivo informacione bezbednosti neophodan je visok stepen interakcije između tehnologije, organizacije i ljudi u cilju zaštite informacija od potencijalnih rizika. Neophodan je set politika i procedura za upravljanje rizikom u domenu osetljivih podataka. Stoga je bitno da se prilikom oblikovanja sistema za upravljanje informacionom bezbednošću uspostavi organizaciona struktura sa definisanim nadležnostima, da se propišu neophodne procedure i da se definišu resursi potrebni za realizaciju svih aktivnosti. Međunarodni standardi relevantni za uspostavljanje sistema za upravljanje informacionom bezbednošću razvijeni su upravo u cilju pružanja podrške poslovnim organizacijama u realizaciji ovog složenog poduhvata, a standard koji je trenutno aktuelan u ovoj oblasti je standard ISO 27001 iz serije standarda ISO 27000 Međunarodne organizacije za standardizaciju (ISO), poznat i kao standard IEC 27001 izdat od strane Međunarodne elektrotehničke komisije (IEC). Standard ISO/IEC 27001 propisuje najbolje pristupe osmišljene u praksi za uspostavljanje, primenu, održavanje i kontinuirano usavršavanje sistema za upravljanje informacionom bezbednošću (Shojaie, 2018). Standard ISO 27001 možemo shvatiti i kao sistematski pristup upravljanju informacionim resursima u cilju ostvarenja sopstvenih zahteva poslovne organizacije u pogledu informacione bezbednosti sa svrhom da se podrži njeno uspešno poslovanje (Flechais et al., 2003) uz uvažavanje očekivanja klijenata i regulatornih zahteva u ovoj oblasti. To su sve razlozi zbog kojih standard ISO 27001 može biti od velike pomoći u poboljšanju organizacionih performansi u domenu finansija, prava, upravljanja i poslovnih operacija (Gillies, 2011). Pomenimo na kraju da su se pojedini autori detaljnije bavili izazovima u sertifikaciji poslovnih organizacija u oblasti upravljanja informacionom bezbednošću i koracima koje je potrebno sprovesti u implementaciji standarda ISO 27001 primenom metodologije "Planiraj - Primeni - Proveri - Deluj" (*PDCA: Plan - Do - Check - Act*) koja je propisana u standardu, kao i efikasnošću te metodologije (npr. Jevelin & Faza, 2023).

U nastavku rada razmatranje će biti usmereno na motive za usvajanje i primenu standarda ISO 27001 i izazove koji prate proces implementacije ovog standarda u bankama.

3. Motivi za primenu i izazovi primene standarda ISO 27001 u bankama

Kao što je prilikom uvodnih razmatranja rečeno, savremeno poslovanje u bankarskom sektoru značajno je utemeljeno na tehnologiji i podrazumeva obradu enormne količine osetljivih finansijskih podataka, čime dolaze do izražaja izazovi na području informacione bezbednosti. Ne samo da se radi o pitanju od kritične važnosti, nego se radi i o problematici koja stalno evoluira pod uticajem promena u regulatornim zahtevima i u informacionoj i finansijskoj tehnologiji. Imajući to u vidu, standard ISO 27001 kao opšteprimenljivi međunarodni standard za izgradnju sistema za upravljanje informacionom bezbednošću ima veoma veliki značaj za sve poslovne entitete čije je poslovanje utemeljeno na primeni informacionih tehnologija u obradi velike količine podataka, pa samim tim i za banke.

Pre nego što se fokus usmeri na probleme koji se javljaju u primeni standarda ISO 27001, neophodno je razumeti motive za usvajanje i implementaciju ovog standarda u poslovnim organizacijama uopšte, kao i u bankama. Jedan od glavnih motiva je potreba unapređenja informacione bezbednosti i otpornosti poslovnih organizacija na rizike i pretnje po podatke i sisteme identifikovanjem tih rizika i pretnji i upravljanjem istim. Kao povezana korist i motiv u odnosu na prethodno može se navesti izgradnja poverenja i reputacije kod stejkholdera kroz posvećenost procesu upravljanja informacionom bezbednošću i transparentnost u tom procesu što bi moglo voditi povećanom tržišnom učešću i rastu profita (Kitsios et al., 2023). Zatim, tu je svakako i potreba da se postigne usaglašenost sa zakonskom i drugom relevantnom regulativom u oblasti sigurnosti i privatnosti podataka, koju u bankarskom sektoru čine Opšta uredba o zaštiti podataka o ličnosti (GDPR), Direktiva za usluge plaćanja 2 (PSD2, *Directive (EU) 2015/2366*), Sarbejns-Oksli zakon (SOX) i drugi relevantni akti u zavisnosti od konkretnih okolnosti. Kao naredni motiv može se istaći želja da se ostvari konkurentska prednost i prepoznatljivost na tržištu kroz pružanje pouzdane i bezbedne usluge, unapređenje odnosa sa korisnicima usluga i poboljšanje njihove satisfakcije i korisničkog iskustva, kao i jačanje njihove lojalnosti (Hoffmann & Birnbrich, 2012), što posebno dobija na značaju u uslovima sve šire primene veštačke inteligencije (Elaprolu et al., 2023). Istraživanja pokazuju da čak i najava sertifikacije poslovnih entiteta u domenu informacione bezbednosti ima statistički značajan pozitivan uticaj na njihovu tržišnu vrednost (Deane et al., 2019) i performanse (Podrecca et al., 2022). Jedan od motiva za implementaciju standarda ISO 27001 može biti i jasno definisanje uloga

i odgovornosti zaposlenih i odeljenja angažovanih u realizaciji aktivnosti koje su usmerene na unapređenje informacione bezbednosti odnosno izgradnja organizacione strukture koja bi bila u funkciji podrške realizaciji tih aktivnosti (Ewuga et al., 2024). Na kraju, unapređenjem praksi usmerenih na informacionu bezbednost u bankama i razvojem svesnosti o značaju tog pitanja, kao i kulture etičnosti koja bi podržala napore preduzete u toj oblasti, demonstrira se društvena odgovornost u poslovanju banaka i doprinosi se opštem društvenom blagostanju (Ewuga et al., 2024). Svi navedeni motivi za primenu standarda ISO 27001 su uglavnom svojstveni za banke uopšte, dok u konkretnom slučaju do izražaja mogu doći i neki motivi specifični za određenu banku.

U pogledu izazova sa kojima se banke mogu sresti u implementaciji standarda ISO 27001 razmotrimo na početku pitanja saglasnosti sa različitim etičkim zahtevima i usaglašenosti sa relevantnim zakonima i propisima. Što se tiče prvog pitanja, prilično je teško ostvariti ravnotežu između informacione bezbednosti i poštovanja prava zaštite podataka korisnika usluga i drugih stejkholdera u duhu etičnosti. U tom cilju ISO 27001 zahteva sprovođenje određenih mera i kontrola osmišljenih da se obezbedi poverljivost, integritet i dostupnost informacionih resursa i zaštita tih resursa od različitih pretnji i rizika, a dodatno insistira na tome da informacije o uspostavljenim aktivnostima i merama usmerenim na informacionu bezbednost budu transparentno komunicirane zainteresovanim stejkholderima. Prema tome, standardom je demonstrirana posvećenost zaštiti osetljivih podataka i poštovanju privatnosti korisnika usluga. Međutim, sprovedenim merama ne bi trebalo da budu ugroženi interesi nosilaca (subjekata) podataka, odnosno da bude moguće da se bilo šta izvrši bez njihove saglasnosti, što znači da prava pristupa, brisanja ili ispravljanja podataka treba da budu u isključivoj nadležnosti nosilaca podataka. Pored toga, pojedinci treba da budu informisani o prikupljanju i upotrebi njihovih podataka od strane banke uz zahtev za njihov pristanak gde god se to smatra neophodnim. Ovo se odnosi kako na korisnike usluga, tako i na zaposlene. Stoga je bitno ostvariti balans između uspostavljenih mera usmerenih na bezbednost podataka i poštovanja privatnosti korisnika usluga, odnosno izbegavati previše rigidne mere bezbednosti kojima se narušava korisničko iskustvo bez adekvatnih pratećih koristi po informacionu bezbednost (Ewuga et al., 2024). Sve navedeno je od važnosti prilikom uspostavljanja sistema za upravljanje informacionom bezbednošću koji je usmeren na zaštitu osetljivih informacija korisnika usluga, ali i na pridržavanje etičkih standarda. U slučaju bilo

kakvih bezbedonosnih incidenata, odgovor treba da bude unapred definisan i osmišljen na način da se njime ne nanosi šteta pojedincima ili banci u celini, ali da se jasno demonstrira etički stav banke u adresiranju incidenta i obelodanjivanju neophodnih informacija. U duhu etičnosti je i kreiranje okruženja u kojima se zaposleni u bankama osećaju sigurnim da prijave svoja zapažanja po pitanju potencijalnog ugrožavanja bezbednosti informacija bez straha da će za to snositi posledice, kao i pružanje zaštite i podrške uzbunjivačima koji bi izneli informacije o mogućim rizicima narušavanja bezbednosti ili zloupotrebe informacija, kao i nepoštovanja etičkih standarda od strane zaposlenih. Svakako da bitnu ulogu u razvijanju svesnosti o značaju informacione bezbednosti u bankama imaju edukativne obuke na kojima bi značajno vreme trebalo posvetiti promovisanju etičnosti među zaposlenima koji imaju dodeljene odgovornosti u ovoj oblasti. Sa druge strane, to je neophodno i demonstrirati u praksi kroz pošten i nediskriminatoran pristup neophodnim resursima svim zaposlenima kojima su delegirane uloge i odgovornosti na očuvanju i unapređenju informacione bezbednosti u bankama.

Pored udovoljavanja etičkim zahtevima, banke treba da usaglase svoje aktivnosti i sa različitim zakonskim i drugim pravnim zahtevima u pogledu zaštite bezbednosti i privatnosti podataka (npr. sa regulativom GDPR, PSD2, SOX, zahtevima centralne banke i dr.), o čemu brigu vode zaposleni u odeljenju koje se bavi usaglašenošću poslovanja, ali ključna odgovornost u ovom domenu pripada najvišim organima upravljanja banke. Međutim, bitno je u poslovnim organizacijama uopšte, pa tako i u bankama, razvijati svesnost o značaju građenja kulture usklađenosti, u kojoj bi odgovornost za usklađenost sa relevantnim regulatornim zahtevima na području informacione bezbednosti delili svi zaposleni u skladu sa odgovornostima koje su im u tom domenu dodeljene. To je naročito bitno u uslovima stalnih promena regulatornih zahteva u oblasti usklađenosti za one aktivnosti koje su usmerene na informacionu bezbednost. Dodatno, banke mogu da posluju u pravnim sistemima različitih zemalja, tako da banke koje su članice iste bankarske grupe mogu da budu izložene različitim zahtevima po pitanju privatnosti i zaštite podataka. U takvim uslovima usklađenost pojedinačnih banaka sa relevantnim zahtevima nacionalnih regulatornih okvira u domenu informacione bezbednosti je veoma kompleksan zadatak. To je naročito kompleksno ukoliko pojedinačne banke u grupi imaju različite organizacione strukture ili koriste različite informacione sisteme (Ewuga et al., 2024). Stoga bi harmonizacija u ovoj oblasti u međunarodnim okvirima, koju omogućava usvajanje i primena standarda ISO 27001, doprinela da se navedena ograničenja u

značajnoj meri ublaže. Koristi od međunarodne harmonizacije odrazile bi se i kod prekograničnog toka podataka, jer bi se harmonizacijom relativizovala postojeća ograničenja.

Kao ograničavajući faktor za širu implementaciju standarda ISO 27001 često se ističe i trajnost i zahtevnost samog procesa, kao i značajni troškovi koji su povezani sa procesom sertifikacije u oblasti upravljanja informacionom bezbednošću. Na primer, značajni bi mogli biti troškovi konsultantskih usluga u realizaciji procesa (Annarelli et al., 2020), kao i troškovi analize postojećih procesa, njihovog redizajna i kreiranja dokumentacije zahtevane u procesu sertifikacije (van Wessel et al., 2011). Pored toga, ističe se i da bi troškovi implementacije neophodnih bezbedonosnih kontrola, predloženih standardom ISO 27001, mogli biti prilično visoki (Montesino et al., 2012). Svi navedeni i drugi inkrementalni troškovi ovog procesa (kao i oportunitetni troškovi koje takođe treba uzeti u obzir - prim. aut.) mogu neizostavno poništiti očekivane koristi od procesa sertifikacije i dovesti u pitanje njegovu racionalnost (Stewart, 2018). To podržavaju i rezultati navedenih studija koji su kontradiktorni, naročito ako se posmatra uticaj procesa sertifikacije na tržišnu vrednost i pokazatelje tržišnih performansi poslovnih entiteta koji su prošli ovaj proces. Možda bi zaključak vredan pažnje bio da je implementacija standarda ISO 27001 preventivna inovacija bez bilo kakve koristi u pogledu stvorene vrednosti za poslovne organizacije (Mirtsch et al., 2021).

Navedimo na kraju još neke izazove za banke na području zaštite podataka korisnika usluga odnosno unapređenja informacione bezbednosti primenom standarda ISO 27001. Očekivano je da banke za regulatorna tela pripremaju sveobuhvatne izveštaje o usaglašenosti sa zahtevima standarda, kao i regulatornim zahtevima u vezi sa zaštitom i privatnošću podataka o korisnicima usluga. To će, uz neophodno obezbeđivanje dokaza o usaglašenosti za potrebe regulatornog nadzora, iziskivati angažovanje dodatnih resursa za tu svrhu i dovesti do uvećanih rashoda. Pored toga, stalne promene regulative, bilo one koja se odnosi na poslovanje u bankarskom sektoru ili one koja se tiče bezbednosti informacija, dovode do potrebe da se blagovremeno obezbede potrebni finansijski i ljudski resursi kako bi banke mogle da se prilagode novim zahtevima, a nedostatak resursa bi mogao predstavljati ograničenje za delovanje na ovom području. Sve navedeno, kao i nastojanje da se predvide buduće promene u zahtevima u vezi sa informacionom bezbednošću koje se odnose na banke, vodi kreiranju značajne neizvesnosti i potrebe za planskim i proaktivnim pristupom na ovom području.

Zaključak

U radu su prezentovani očekivani motivi i koristi, kao i izazovi sa kojima se banke mogu suočiti u procesu usvajanja i primene standarda ISO 27001 kao instrumenta harmonizacije u sferi upavljanja informacionom bezbednošću. Ovaj standard definiše okvir za uspostavljanje, primenu, održavanje i stalno unapređivanje sistema za upravljanje informacionom bezbednošću, koji treba da obuhvati sve aktivnosti koje banke sprovode na ovom području. To može biti veoma izazovno, pogotovo za banke koje su članice grupa i koje posluju u različitim pravnim sistemima, imaju različitu organizacionu strukturu ili koriste različite tehnologije i informacione sisteme, budući da u takvim uslovima sistem za upravljanje informacionom bezbednošću treba da bude prilagođen različitim ciljevima i strategijama pojedinih banaka, kao i različitim kulturama koje su unutar tih banaka razvijene. Nakon uspostavljanja sistema, od velike važnosti je i periodično informisanje stejkholdera o efektivnosti i performansama sistema pomoću definisanih mera i kontrola, što podrazumeva testiranja i periodične revizije procedura i aktivnosti, uspostavljanje vrednosnih kriterijuma i davanje povratnih informacija zaposlenima koji imaju dodeljene odgovornosti u sistemu za upravljanje informacionom bezbednošću. Naravno, to nije ni malo jednostavan zadatak, imajući u vidu da je u aktuelnom poslovnom okruženju spektar pretnji i rizika koje ugrožavaju informacionu bezbednost banaka sve raznovrsniji, a banke imaju ograničene finansijske i ljudske resurse koje mogu da usmere na ovo područje. Dodatni problem predstavlja nemogućnost uspostavljanja adekvatnih merila pomoću kojih bi se pretnje i rizici po informacionu bezbednost banaka na pravi način kvantifikovale i o kojima bi banke informisale zainteresovane stejkholdere, kao i jasnih i merljivih ciljeva u ovom domenu. U radu su takođe razmotrena određena etička pitanja i pitanja usaglašenosti koja se uvođenjem standarda ISO 27001 sama po sebi nameću, od kojih su mnoga zajednička za sve banke koje vrše implementaciju standarda, mada ima i onih koja su specifična za određene banke i kojima treba posvetiti dodatnu pažnju.

Literatura

Annarelli, A., Nonino, F., & Palombi, G. (2020). Understanding the management of Cyber Resilient Systems. *Computers & Industrial Engineering*, 149, 106829. https://doi.org/10.1016/j.cie.2020.106829

Berger, A. N. (2003). The economic effects of Technological Progress: Evidence from the Banking Industry. *Journal of Money, Credit, and Banking*, 35(2), 141–176. https://doi.org/10.1353/mcb.2003.0009

Bessis J. (2015). *Risk Management in Banking*, John Wiley & Sons, New Jersey.

Chartered Institute of Management Accountants (2008). *Fraud Risk Management: A Guide to Good Practice*. www.cimaglobal.com

Deane, J., Goldberg, D., Rakes, T., & Rees, L. (2019). The effect of information security certification announcements on the market value of the firm. *Information Technology and Management*, *20*(3), 107–121. https://doi.org/10.1007/s10799-018-00297-3

Elaprolu, S., Chola, C., Chandradhar, V., & Rodriguez, R. V. (2023). Applications of artificial intelligence on customer experience and service quality of the banking sector. *Artificial Intelligence and Knowledge Processing*, Chapter 25, 290–301. CRC Press. https://doi.org/10.1201/9781003328414-25

Ewuga, S. K., Egieya, Z. E., Omotosho, A., & Adegbite, A. O. (2024). ISO 27001 in banking: An evaluation of its implementation and effectiveness in enhancing information security. *Finance & Accounting Research Journal*, 5(12), 405–425. https://doi.org/10.51594/farj.v5i12.684

Flechais, I., Sasse, M. A., & Hailes, S.M.V. (2003). Bringing security home: a process for developing secure and usable systems. In *Proceedings of the 2003 workshop on New security paradigms* (NSPW '03). Association for Computing Machinery, NY, USA, 49–57. https://doi.org/10.1145/986655.986664

Gillies, A. (2011). Improving the quality of information security management systems with ISO 27000. *The TQM Journal*, 23(4), 367–376. https://doi.org/10.1108/17542731111139455

Goddard, J., Molyneux, P., Wilson, J. O. S., & Tavakoli, M. (2007). European banking: An overview. *Journal of Banking & Finance*, 31(7), 1911–1935. https://doi.org/10.1016/j.jbankfin.2007.01.002

Greene, M.N. (2009). Divided we fall: fighting payments fraud together. *Economic Perspectives*, Vol. 33 No. 1, pp. 37-42. (https://www.chicagofed.org/publications/economic-perspectives/2009/1qtr2009-part6-greene)

Hoffmann, A. O. I., & Birnbrich, C. (2012). The impact of fraud prevention on bank-customer relationships. *International Journal of Bank Marketing*, 30(5), 390–407. https://doi.org/10.1108/02652321211247435

Hopwood, W. S., Leiner, J. J., & Young, G. R. (2012). *Forensic accounting and Fraud Examination*. McGraw-Hill.

Jevelin, J., & Faza, A. (2023). Evaluation the Information Security Management System: A Path Towards ISO 27001 Certification. *Journal of Information Systems and Informatics*, 5(4), 1240-1256. https://doi.org/10.51519/journalisi.v5i4.572

Kitsios, F., Chatzidimitriou, E., & Kamariotou, M. (2023). The ISO/IEC 27001 information security management standard: How to extract value from data in the IT sector. *Sustainability*, 15(7), 5828. https://doi.org/10.3390/su15075828

Mirtsch, M., Blind, K., Koch, C., & Dudek, G. (2021). Information security management in ICT and non-ICT sector companies: A preventive innovation perspective. *Computers Security*, 109, 102383. https://doi.org/10.1016/j.cose.2021.102383

Montesino, R., Fenz, S., & Baluja, W. (2012). Siem-based framework for Security Controls Automation. Information Management & Computer Security, 20(4), 248–263. https://doi.org/10.1108/09685221211267639

Podrecca, M., Culot, G., Nassimbeni, G., & Sartor, M. (2022). Information security and value creation: The performance implications of ISO/IEC 27001. *Computers in Industry*, 142, 103744. https://doi.org/10.1016/j.compind.2022.103744

Shojaie, B. (2018). *Implementation of information security management systems based on the ISO/IEC 27001 standard in different cultures* (Doctoral dissertation, Staats-und Universitätsbibliothek Hamburg Carl von Ossietzky)

Stewart, A. (2018). A utilitarian re-examination of enterprise-scale information security management. *Information & Computer Security*, 26(1), 39–57. https://doi.org/10.1108/ics-03-2017-0012

Sudjianto, A., Nair, S., Yuan, M., Zhang, A., Kern, D., & Cela-Díaz, F. (2010). Statistical Methods for Fighting Financial Crimes. *Technometrics*, 52(1), 5–19. https://doi.org/10.1198/tech.2010.07032

van Wessel, R., Yang, X., & de Vries, H. J. (2011). Implementing international standards for Information Security Management in China and Europe: a comparative multi-case study. *Technology Analysis & Strategic Management*, 23(8), 865–879. https://doi.org/10.1080/09537325.2011.604155

https://courses.cfte.education/ranking-of-largest-fintech-companies/

https://www.europarl.europa.eu/topics/en/article/20220120STO21428/cybersecurity-main-and-emerging-threats

https://finance.ec.europa.eu/regulation-and-supervision/financial-services-legislation/implementing-and-delegated-acts/payment-services-directive_en

https://www.forbes.com/advisor/investing/top-fintech-companies/