SLOVENSKI INŠTITUT ZA REVIZIJO
LJUBLJANA

ZAKLJUČNO DELO
ZA STROKOVNI NAZIV PREIZKUŠENI NOTRANJI REVIZOR

NOTRANJE REVIDIRANJE KIBERNETSKE VARNOSTI V BANKI

Idrija, junij 2021 Milan Osterman

IZJAVA

Milan Osterman, vpisan v izobraževalni program za pridobitev strokovnega naziva preizkušeni notranji revizor izjavljam, da sem avtor tega zaključnega dela in skladno s 1. odstavkom 21. člena Zakona o avtorskih in sorodnih pravicah dovoljujem objavo zaključnega dela na spletnih straneh Slovenskega inštituta za revizijo.

V Idriji, 8.6.2021 Podpis: 

KAZALO VSEBINE

KAZALO TABEL

KAZALO SLIK

UVOD

Delovanje družbe je vedno bolj odvisno od informacijsko-telekomunikacijskih sistemov, saj je večina aktivnosti podprta s sodobnimi orodji, ki so povezana na svetovni splet. To je tudi v veliki meri značilno za finančno področje, še zlasti bančništvo. Po drugi strani se s povečanjem obsega uporabe povečajo tudi tveganja, med njimi zagotovo v zadnjem času izstopajo tista, ki se tičejo kibernetske varnosti.

1 OPREDELITEV PODROČJA IN OPIS PROBLEMA

1.1 Področje pregleda

Predmet obravnave v zaključni nalogi bo notranje revidiranje kibernetske varnosti v banki. Kibernetsko tveganje, ki spada v skupino operativnih tveganj, se nanaša na izpostavljenost škodi oziroma izgubi zaradi napadov na informacijski sistem ali druge kršitve, ki se navezujejo na uporabo tehnologije v organizaciji (RSA, 2016, str. 1), je zaradi uporabe vse bolj obsežnih in kompleksnih informacijskih rešitev že nekaj časa med najvišje uvrščenimi tveganji. Tovrstna tveganja se bodo zaradi nadaljnje digitalizacije še povečala (Svetovni gospodarski forum, 2020). Zato morajo organizacije zagotoviti ustrezno kontrolne mehanizme za njihovo prepoznavanje in preprečevanje oziroma obvladovanje, saj so v nasprotnem primeru posledice njihove uresničitve lahko kritične. Na podlagi teh dejstev je odločitev za prikaz izvedbe notranjerevizijskega pregleda kibernetske varnosti v banki še toliko lažje razumljiva. V zaključni nalogi se za namen predstavitve notranjerevizijskega pregleda uporablja tudi samo izraz revizija in za notranjega revizorja tudi samo revizor, saj je glede na to, da druge vrste pregledov niso vključene, majhna možnost, da bi prihajalo do nejasnosti. Ker je revizijsko poročilo kot izdelek pregleda namenjeno v prvi vrsti višjemu vodstvu, je tudi nekoliko prilagojeno v smislu izogibanja izrazito tehničnim izrazom, kar se odrazi tudi v zaključni nalogi.

1.2 Namen in cilj

Namen dela je prikazati načrtovanje in izvedbo postopkov notranjerevizijskega posla za področje kibernetske varnosti, ki vključujejo uporabo veščaka za izbrana tehnična področja. Iz podanih opisov podlag ter izvedenih aktivnosti je namen tudi prikazati sposobnost samostojne izvedbe takšnega posla na ustrezni strokovni ravni s strani avtorja.
Cilj naloge je predstaviti izvedbo notranjerevizijskih postopkov ugotavljanja skladnosti kontrolnega sistema z zakonodajo in dobrimi praksami za področje kibernetske varnosti. Prejemniki revizijskega poročila tako prejmejo zagotovilo, v kolikšni meri kontrolni sistem na pregledanem področju izpolnjuje zahteve zakonodaje ter vodilnih dobrih praks v zvezi s kibernetsko varnostjo. Slednje daje odgovor na vprašanje, ali se lahko kibernetska varnost banke glede na splošno znane ranljivosti v času pregleda smatra kot ustrezna. Skladnost navedena v cilju ne obsega samo skladnosti z zakonodajo, temveč zajema tudi preverjanje s priporočili izbranih dobrih praks. Glede na specifike banke, v kateri poteka notranjerevizijski pregled, so sicer zakonodajne zahteve dokaj splošne, saj banka ne posluje s prebivalstvom niti ne izvaja storitev plačilnega prometa za stranke; torej ne deluje na področjih, kjer so zahteve sicer najostrejše. Cilj pregleda ni podati zagotovilo celovite skladnosti s katero od dobrih praks, saj so bili iz posameznih okvirov oziroma standardov vzeti samo deli sodil, ki so relevantni za pregled kibernetske varnosti z upoštevanjem specifičnega poslovnega modela banke. To je tudi skladno z nameni okvirov, ki predstavljajo dobre prakse, saj za razlik od standardov omogoča določeno mero fleksibilnosti pri doseganju želenega. Od ciljev notranjega kontroliranja je pregled večinoma omejen na skupino ciljev skladnosti, saj to sovpada z zagotovilom, ki je navedeno predhodno. Zagotovilo je omejeno na oceno uspešnosti delovanja kontrol z vidika skladnosti z zakonodajo in dobrimi praksami. Cilji z drugih področjih, na primer glede na učinkovitost izvajanja kontrol, so vključeni v smislu podaje dodatnih ugotovitev in ne dajanja zagotovil.
Izvedba revizijskih postopkov je bila opravljena z upoštevanjem pravil stroke, v skladu z veljavno zakonodajo in Mednarodnimi standardi strokovnega ravnanja pri notranjem revidiranju predpisi ter

metodologijo COSO. Pri slednjem je bilo smiselno upoštevanih vseh pet sestavin notranjega kontroliranja.
Na podlagi izvedenih postopkov je bila dana ocena skladnosti z zakonodajo in dobrimi praksami ter ugotovitve glede zaznanih pomanjkljivosti, ki zajemajo stanje, sodilo, razlog in posledice neustrezne zasnove oziroma pomanjkljivega delovanja notranjih kontrol. Podana so tudi priporočila za odpravo ugotovljenih nepravilnosti in pomanjkljivosti ter predstavljen okvir za spremljavo realizacije priporočil.
Pri izvedbi revizijskih postopkov se je v skladu z izbrano metodologijo COSO in upoštevajoč zakonodajo z oziroma na specifiko banke ter relevantne dobre prakse preverjalo, kot že okvirno navedeno, ali so vzpostavljene ustrezne notranje kontrole ter ali te delujejo na način, da izpolnjujejo zahteve zakonodaje oziroma kot narekujejo dobre prakse. V primeru ugotovitev s področja učinkovitosti so bile te podane kot dodatne ugotovitve ne kot zagotovilo. Preverjalo se je predvsem kontrolno okolje, ocenjevanje tveganj, kontrolne aktivnosti, informiranje in komuniciranje ter nadziranje.
Zaključna naloga je izvirno delo, pripravljeno samostojno s strani avtorja in sodi v okvir presojanj znotraj notranjerevizijske dejavnosti.

1.3 Predpostavke in omejitve

Notranjerevizijske aktivnosti so bile izvedene ob upoštevanju določil Mednarodnih standardov strokovnega ravnanja pri notranjem revidiranju. Izvedene si bile naslednje faze notranjega revidiranja: načrtovanje, izvedba, poročanje, arhiviranje, zagotavljanje ustrezne kvalitete izvedbe in spremljanje uresničevanja revizorjevih priporočil.
Pri revidiranju so bili poleg veljavnih zakonov in predpisov ter dobrih praks upoštevani interni pravilniki in delovna navodila organizacije. Testiranje je bilo izvedeno s pomočjo orodij informacijske tehnologije predvsem za tehnični del opravljeno v največji možni meri na celotni populaciji, v ostalih primerih pa so bili izbrani dovolj veliki reprezentativni vzorci, ki omogočajo podajo mnenja o ugotovitvah glede ustreznosti in, če smiselno oziroma potrebno, učinkovitosti notranjega kontrolnega sistema. Pojasnila glede izbire vzorca so podana pri opisu postopkov. Revizijski program je pripravljen na podlagi ocene tveganj in ob upoštevanju zakonodajnih zahtev. V pregled so bila vključena tveganja, ki so preliminarno ocenjena kot zmerna in visoka z določeni, spodaj navedenimi izjemami. To je možno kljub dejstvu, da cilj obsega tudi preveritev skladnosti upravljanja področja kibernetske varnosti z zakonodajo, na podlagi česar bi se lahko sklepalo, da je potreben pregled vseh tveganj, ki jih je moč povezati z zakonodajnimi zahtevami. Vendar so zakonske zahteve za takšno vrsto banko, kot je vključena v pregled, relativno splošne, v primeru bolj specifičnih zahtev omejitev na zmerna in visoka tveganja ne bi bilo več smiselna, saj bi morala biti zajete obsežne zakonodajne zahteve. Tako so bile, kot že omenjeno, v pregled vključena vsa tveganja, ki so bila ocenjena kot zmerna in visoka, ter dodatno še bolj specifična določila Zakona o varstvu osebnih podatkov ter Uredbe GDPR glede revizijskih sledi. Za notranje kontrole je bila izvedena začetna ocena ustreznosti, ki je bila tudi eden od podlag za vključitev v revizijski program. Poleg omenjenih izjem v povezavi z zakonskimi zahtevami so bile v pregled vključene tudi vse kontrole v zvezi z varnostnimi nastavitvami sistemov, ki jih je pregledal najeti veščak (zunanji izvajalec).

Pri delu so bile uporabljene spoznavne podlage, ki omogočajo poglobljeno seznanitev s področjem pregleda, in sicer od zakonodaje, ki vključuje zakone, podzakonske akte in predpise Banke Slovenije, predpisi in gradiva s področja notranjega revidiranja, vpogled v trenutne trende vključno z aktualnimi viri tveganj, tehnikami upravljanja s tveganji ter dobrimi praksami s področje revidiranje (COBIT, ITAF, ISO/IEC 27001 ter 27002, NIST, OSSTMM, MITRE ATT&CK ter OWASP), ki so opisani v nadaljevanju.

Revizijski postopki se, kjer smiselno, osredotočajo na obdobje zadnjega leta pred pregledom (2020), saj so tako pokriti aktualni dogodki in spremembe na področju kibernetske varnosti v banki. Čeprav so bile revizije s področja informacijske varnosti tudi v vmesnem obdobju, je bil čas nekoliko razširjen, da se zagotovi večja pokritost in izniči možnost izpustitve pomembnih dokumentov, kot so na primer zapisniki odborov ali sej drugih organov banke. Ugotovitve zunanjega izvajalca varnostnega pregleda se nanašajo na postopke izvedene v obdobju 1.2.2021 – 10.2.2021.

Glede na to, da je bil v pregled za izvedbo tehničnih postopkov preverjanj vključen zunanji izvajalec, so s tem povezana dodatna tveganja, ki jih je potrebno nasloviti in ustrezno obvladovati. Ta tveganja so se obravnavala tekom načrtovanja revizijskega pregleda, v povezavi z njimi so bili izvedeni postopki, ki so zahtevani glede na vzpostavljena pravila obvladovanja tveganj v banki povezanih z oddajo storitev v izvajanje zunanjim izvajalcem. Poglavitna identificirana tveganja so se nanašala na potencialno:

- neustrezno kvaliteto izvedenih storitev,
- nepravočasno izvedene storitve,
- izgubo nadzora nad izvajanjem postopkov,
- presežene stroške,
- nepooblaščen dostop do zaupnih podatkov ali nepooblaščeno izvajanje operacij,
- razkritje zaupnih podatkov,
- omejitve neodvisnosti oziroma nepristranskosti.

Mehanizmi za obvladovanje teh tveganj so bili opredeljeni v fazi načrtovanja notranjerevizijskega pregleda.

Pomembna omejitev glede zagotovil, ki so osnovane na podlagi dobrih praks, je zavedanje, da se nove varnostne ranljivosti sistemov ugotavljajo ves čas. To pomeni, da bi mogoče pri ponovitvi pregleda čez čas bile ugotovljene dodatne pomanjkljivosti. Zato je priporočljivo, da se pregledi kibernetske varnosti izvajajo periodično ter, da so vzpostavljeni postopki za prejemanje informacij glede novih ugotovljenih ranljivosti ter izvedbo ustreznih ukrepov.

1.4 Uporabljene metode preučevanja

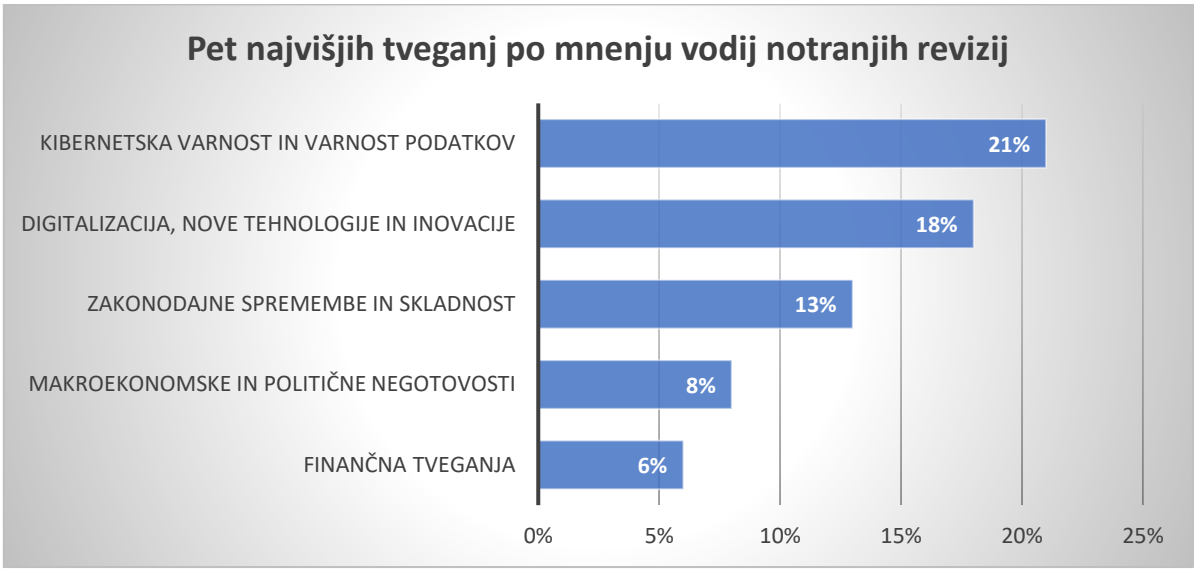
V zaključni nalogi je uporabljen deskriptivni pristop, s katerim je predstavljen postopek izvedbe notranjerevizijskega pregleda in ugotovljeni zaključki v zvezi z opravljenimi revizijskimi aktivnostmi. Teoretični del naloge je rezultat preučevanj zakonodaje, dobrih praks in ostale literature za področje kibernetske varnosti. Tako je zagotovljena podlaga za izvedbo presoje notranjega kontrolnega sistema s pomočjo metode kompilacije. Temelj za pripravo praktičnega dela naloge so informacije pridobljene s pomočjo preučevanja internih aktov banke, razgovorov z revidiranci, internega raziskovanja ter kontrole podatkov. Uporabljeno je bilo preiskovanje in vrednotenje (poizvedovanje (intervjuji), opazovanje – spremljanje izvajanja procesov), preverjanje in preizkušanje ter analitični postopki (primerjava in preučevanje)). Ugotovitve preverjanj so bile primerjane z dobrimi praksami ter v relevantnih primerih z določili predpisov oziroma zakonodaje ter presojane z vidika skladnosti in, kjer smiselno, učinkovitosti. Pri obdelavi podatkov je bila uporabljena metoda komperacije. Izsledki revizijskih aktivnosti so podani opisno in tabelarično.

2 NOTRANJE REVIDIRANJE KIBERNETSKE VARNOSTI

2.1 Predstavitev področja kibernetske varnosti

Digitalizacija je v zadnjem obdobju ena od najpogosteje uporabljenih izrazov v besednjaku predstavnikov organizacij, ko gre govor o razvoju poslovnih modelov. Dodaten pospešek pri večji uporabi spletnih tehnologij pri poslovanju izvira iz Covid-19. Hkrati s tem se povečujejo tudi tveganja, ki se nanašajo na kibernetsko varnost, kar je med drugim jasno razvidno iz poročila Evropske zveze inštitutov za notranjo revizijo (ECIIA).

Slika 1: Pet najvišjih tveganj po mnenju vodij notranjih revizij



Vir: ECIIA, Risk in focus 2020, stran 2

V skladu z opredelitvijo v Zakonu o informacijski varnosti se na splošno kibernetska varnost razume kot sposobnost zaščititi, varovati in braniti kibernetski prostor pred kibernetskimi grožnjami, incidenti in kibernetskimi napadi. Izraz pokriva zelo široko področje, kjer je veliko odvisno od konteksta, v katerem se obravnava. V primeru te zaključne naloge se nanaša na finančno institucijo, bolj natančno banko, podrobnosti bodo predstavljene v sledečih poglavjih.

Kibernetska varnost je na splošno gledano povezana z napadi od zunaj, ki se lahko seveda izvajajo z namerno ali nenamerno pomočjo znotraj organizacije. V grobem takšno opredelitev zagovarjajo vse vidnejše organizacije, kot so NIST, ISACA ali ISO. Kibernetska varnost se ukvarja z zaščito vseh sredstev, ki so podvrženi napadom oziroma nepooblaščenim dostopom, kot so računalniki, strežniki, omrežje, druge naprave in sistemi ter aplikacije. Poleg tega se kibernetska varnost v prvi vrsti nanaša na zaščito podatkov v digitalni obliki. Po drugi strani se informacijska varnost nanaša na zaščito podatkov ne glede na njihovo obliko in se dejansko navezuje na varovanje podatkov in informacijskih sistemov pred nepooblaščenimi dostopi, uporabo, razkritji, prekinitvami, spremembami ali uničenjem (Solm, 2018).

2.2 Predstavitev organizacije

Notranjerevizijske storitve bodo predstavljene na ilustrativnem primeru Banke d.d. (odslej tudi banka), ki nudi izbrane storitve le pravnim osebam. Slednje večinoma obsegajo kreditiranje, ostale storitve obsegajo le manjši del poslovanja in ne predstavljajo dodatnih tveganj za področje informacijske varnosti, saj med njimi ni izvajanja plačilnega prometa za stranke, ponujanja računov v domači ali tuji valuti ter sprejemanja depozitov. Elektronsko bančništvo in s tem dostop strank do informacijskega sistema banka je omejeno na oddajo dokumentov in poročil strank ter dostop do izbranih informacij.

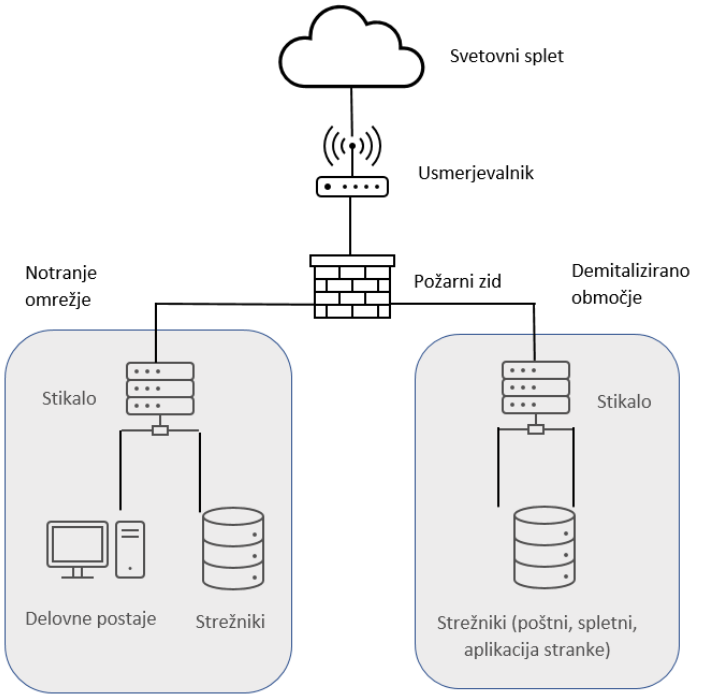
Informacijski sistem banke je heterogen, za posamezna področja se uporabljajo različne aplikacije, ki so med seboj povezane z vmesniki. Glavne poslovne aplikacije so:

- sistem za podporo procesu financiranja (aplikacija Krediti);
- sistem za upravljanje portfeljev finančnih instrumentov (aplikacija FI);
- glavna knjiga in saldakonti (aplikacija GK);
- sistem, prek katerega stranke oddajajo dokumente te poročajo (aplikacija Stranke).

Vsi sistemi so nameščeni na fizičnih in virtualnih strežnikih na lokaciji banke, rezervna lokacija ne bo predmet pregleda. Aplikacija, do katerega dostopajo stranke je nameščena v t.i. demilitariziranem območju (DMZ). Banka veliko pozornosti namenja informacijski varnosti in uporablja požarni zid z

naprednimi funkcijami zaznave in preprečevanja nepooblaščenih dostopov vključno s sistemom ATP (Advanced Threat Protection) ter orodje za upravljanje varnostnih informacij in dogodkov (Security Information and Event Management - SIEM). Prav tako se uporablja več različnih operacijskih sistemov ter sistemov za upravljanje z zbirkami podatkov. Poenostavljena shema omrežja je prikazana na spodnji sliki.

Slika 2: Poenostavljena shema omrežja banke

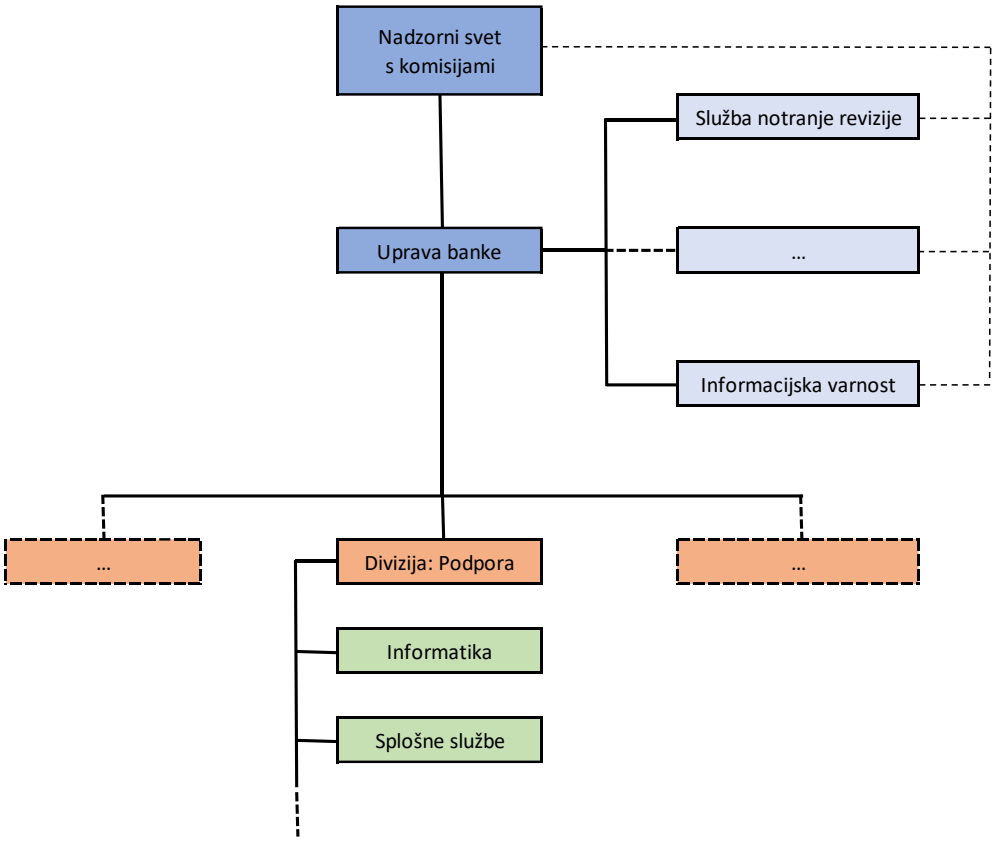


Vir: Banka

V organizaciji je vzpostavljena neodvisna služba notranje revizije (odslej tudi SNR), katere namen je izvedba revizijskih aktivnosti na strokoven in neodvisen način in ki daje neodvisna zagotovila glede ustreznosti oziroma učinkovitosti delovanje sistema notranjih kontrol. Služba ima zaposlenega notranjega revizorja z znanji s področja informacijske tehnologije, za kar poseduje tudi ustrezna potrdila. Le za kompleksne tehnološke postopke preverjanja posameznih področij se koristi pomoč zunanjega veščaka, kar bo tudi izvedeno v konkretnem primeru, ki se obravnava v okviru te zaključne naloge. SNR izvaja redne notranjerevizijske preglede z upoštevanjem hierarhije pravil, ki jih je sprejel Slovenski inštitut za revizijo.

V grobem je banka poleg organizacijskih enot, ki so podrejene neposredno upravi in poleg tega poročajo tudi neposredno tudi nadzornemu svetu oziroma njegovim komisijam, razdeljena tudi na divizije. Izsek iz organizacijske sheme, ki je relevanten za področje pregleda je prikazana na spodnji sliki.

Slika 3: Izsek iz sheme organiziranosti banke



Vir: Banka

V skladu s Sklepom o ureditvi notranjega upravljanja, upravljalnem organu in procesu ocenjevanja ustreznega notranjega kapitala za banke in hranilnice mora banka zagotoviti uresničevanje notranjih kontrol predvsem na podlagi dokumentiranih pravil in postopkov razvoja ter zagotavljanja skladnosti poslovanja banke s predpisi, standardi in notranjimi akti ter zahtevami Banke Slovenije in drugih pristojnih nadzornih organov ter zagotoviti varnost informacijskih sistemov in informacij banke. Za preverjeno področje Banka razpolaga z naslednjimi ključnimi internimi akti:

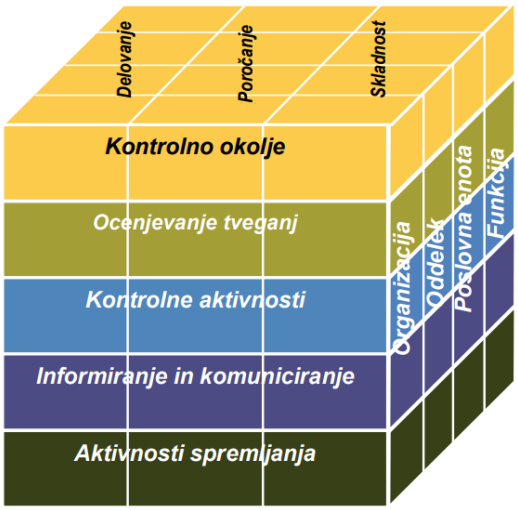
- Varnostno politiko,
- IT strategijo banke,
- Pravilnikom o obravnavi in poročanju varnostnih dogodkov,
- Pravilnikom o načrtu neprekinjenega poslovanja,
- Pravilnikom o upravljanju pravic in dostopov do informacijskih sistemov banke,
- Pravilnikom o upravljanju sistemov in omrežja banke,
- Pravilnikom o razvoju aplikacij,
- Pravilnikom o upravljanju revizijskih sledi,
- Pravilnikom o uporabi IKT opreme in dostopih,
- Pravilnikom o skrbništvu sistemov, poročil in podatkov,
- Navodilom za izdelavo varnostnih kopij in arhiviranje,
- Navodilom za upravljanje strežnikov.

2.3 Podlage na področju notranjega revidiranja

Kot metodološki pristop za ocenjevanje sistemov upravljanja organizacije, tveganj in notranjih kontrol je banka oziroma služba notranje revizije prevzela COSO Celovit okvir notranjega revidiranja (odslej tudi COSO okvir), ki ga je Odbor za notranjo revizijo pri Slovenskem inštitutu za revizijo uvrstil na tretjo raven Hierarhije pravil. COSO okvir je po objavi v 1992 postal eden vodilnih okvirov za vzpostavitev, uveljavitev in izvajanje notranjega kontroliranja in za ocenjevanje uspešnosti notranjega

kontroliranja (Protiviti, 2021). V posodobljeni verziji 2013 ohranja temeljno opredelitev pojma notranjega kontroliranja, vseh pet sestavin notranjega kontroliranja ter zahtevo, da je potrebno upoštevati prav vse od njih za ocenjevanje uspešnosti sistema notranjega kontroliranja. Okvir tudi še nadalje poudarja pomembnost presoje (poslovodstva pri vzpostavitvi, uveljavitvi in izvajanju notranjega kontroliranja in pri ocenjevanju uspešnosti sistema notranjega kontroliranja), hkrati pa prinaša izboljšave in pojasnila za lažjo uporabo gradiva; ena od njih je ureditev temeljnih zamisli, ki so bile uvedene v prvotnem okviru. Te zamisli so zdaj oblikovane v načela, ki so povezana s petimi sestavinami in dajejo jasno podlago za vzpostavitev in uveljavitev sistemov notranjega kontroliranja in razumevanje zahtev za uspešno notranje kontroliranje. Okvir je bil dopolnjen tudi z razširitvijo ciljev poleg računovodskega poročanja še na druge pomembne oblike poročanja, kot sta neračunovodsko in notranje poročanje, ter je tudi odraz upoštevanja mnogih sprememb v poslovnem in delovnem okolju v zadnjih nekaj desetletjih.
Okvir zelo nazorno prikazuje razmerje med cilji (kar si organizacija prizadeva doseči), sestavinami (kar je potrebno za doseganje ciljev) in organizacijskim ustrojem organizacije (organizacijske enote in drugo) v obliki kocke, ki je prikazana na spodnji sliki.

Slika 4: Zgradba COSO Celovitega okvirja notranjih kontrol



Vir: COSO prevod 2013

Poleg tega okvir predstavlja načela, ki veljajo tako za cilje delovanja kot poročanja in skladnosti ter izhajajo neposredno iz sestavin. To pripomore k temu, da lahko organizacija z njihovo uporabo doseže uspešno notranje kontroliranje. Načel je skupaj 17 in predstavljajo temeljne zasnove, povezane z vsako sestavino. Povzetek načel je predstavljen na spodnji sliki.

Slika 5: Povzetek COSO načel

Kontrolno okolje	Ocenjevanje tveganj	Kontrolne aktivnosti	Informiranje in komuniciranje	Aktivnosti spremljanja
1. Zavezanost k neoporočenosti in etičnim vrednotam	6. Jasna opredelitev ustreznih ciljev	10. Izbira in razvoj kontrolnih aktivnosti	13. Uporaba ustreznih kakovostnih informacij	16. Izvedba stalnih in ločenih ocenjevanj
2. Neodvisnost od poslovodstva in izvajanje nadzora	7. Identifikacija in analiza tveganj	11. Izbira in razvoj splošnih kontrolnih aktivnosti v zvezi s tehnologijo	14. Interna komunikacija	17. Ocenjevanje in obveščanje o pomanjkljivostih
3. Ustrezen ustroj organizacije, pooblastila in odgovornosti	8. Ocena tveganj prevar	12. Uvedba skozi usmeritve	15. Komunikacija navzven	
4. Zavezanost k razvoju kvalitet zaposlenih	9. Identifikacija in analiza pomembnih sprememb			
5. Odgovornost pri izvajanju nalog notranjega kontroliranja				

Vir: COSO 2013, 2013, stran 5-6; COSO in the Cyber Age, 2015, stran 3

Nadalje okvir določa zahteve za uspešen sistem notranjega kontroliranja, ki daje sprejemljivo zagotovilo glede doseganja ciljev, vendar ob upoštevanju zahtev da je prisotna in deluje vsaka od petih sestavin skupaj z ustreznimi načeli ter da vseh pet sestavin deluje skupaj in povezano. Pri uporabi okvira se je potrebno zavedati tudi, da obstajajo omejitve, ki vplivajo na uspešnost sistema notranjega kontroliranja, na primer med drugim morebitno pristranskost uporabnikov, človeških napak, zunanjih dogodkov, ter da je uporaba odvisna tudi od tega, komu so rezultati namenjeni. COSO je objavil tudi Celovit okvir za upravljanje tveganj v organizacijah (Okvir ERM), ki se dopolnjuje s Celovitim okvirom notranjega revidiranja, vendar je v primeru zaključne naloge uporabljen slednji.

Služba notranje revizije je ustanovljena v skladu z Zakon o bančništvu (ZBan-2), njeno delovanje v banki in tudi odnose navzven urejajo trije interni akti:

- **Pravilnik o delovanju službe notranje revizije**, ki opredeljuje funkcijo notranje revizije, namen, poslanstvo, obseg delovanja in naloge, odgovornosti in pristojnosti, neodvisnost ter standarde revizijskega dela. Dokument po naravi predstavlja notranjerevizijsko temeljno listino v skladu z Mednarodni standardi strokovnega ravnanja pri notranjem revidiranju in kot tak tudi določa položaj službe notranje revizije v organizaciji, vključno z naravo razmerja funkcijske odgovornosti vodje notranje revizije organu nadzora, daje pooblastila za dostop do zapisov, zaposlenih, prostorov in opreme, ki so pomembni za izvajanje posla, ter opredeljuje področje in dejavnosti notranje revizije. Dokument je, kot tudi Revizijska politika in Revizijski priročnik v nadaljevanju, potrjen s strani uprave ter nadzornega sveta.
- **Revizijska politika**, ki opredeljuje glavna načela službe notranje revizije in daje splošne smernice o načrtovanju in izvedbi revizijskih aktivnosti, poročanje revizijskih ugotovitev, spremljanje implementacije revizijskih priporočil, oceno sistema notranjih, spremljanje revizijskih aktivnosti, model kvalitete ter izboljšanje revizijskih aktivnosti.
- **Revizijski priročnik** bolj podrobno opisuje metodologijo, ki jo uporablja služba notranje revizije. V dokumentu so podani podrobni opisi pristopov, ki jim je potrebno slediti pri notranjerevizijskih aktivnostih in minimalni standardi kvalitete, ki jih morajo vsi revizorji upoštevati pri svojem delu.

2.4 Zakonodaja in dobre prakse

Pregled opredeljuje regulativa za področje bančništva s poudarkom na informacijski varnosti. Slednje vključuje zakone, podzakonske akte in predpise Banke Slovenije. Kot pomoč oziroma usmeritev pri pripravi revizijskih postopkov pa služijo dobre prakse, kot so okviri in standardi za področje informacijske varnosti.

2.4.1 Zakonodaja, podzakonski akti in predpisi Banke Slovenije

Zakon o bančništvu, kot krovni zakon, ki ga morajo upoštevati slovenske banke, vključuje predvsem splošne zahteve, ki se posredno navezujejo na informacijsko varnost, in sicer predvsem v poglavjih 6.3.6 (Upravljanje operativnega tveganja) ter 6.4 (Mehanizmi notranjih kontrol). Že bolj natančen je Sklep o ureditvi notranjega upravljanja, upravljalnem organu in procesu ocenjevanja ustreznega notranjega kapitala za banke in hranilnice. Ta v peti in šesti točki prvega odstavka 33. člena določa, da mora banka zagotoviti uresničevanje notranjih kontrol, in sicer predvsem na podlagi dokumentiranih pravil in postopkov, kar se tiče tudi varovanja premoženja banke in razvoja ter zagotavljanja varnosti informacijskih sistemov in informacij banke. Slednje se navezuje naprej na odstavek, ki govori o tem, sicer na dokaj splošnem nivoju, da notranje kontrole pri informacijskih sistemih vključujejo med drugim pri zagotavljanju varnosti informacijskih sistemov logične in fizične kontrole pri dostopanju do informacijskih sistemov.

Nadalje Zakon o informacijski varnosti, kot tudi povzema Nacionalni Interoperabilnostno Okvir (NIO, 2021), ureja področje informacijske varnosti in ukrepe za doseganje visoke ravni varnosti omrežij in informacijskih sistemov v Republiki Sloveniji, ki so bistvenega pomena za nemoteno delovanje države v vseh varnostnih razmerah ter zagotavljajo bistvene storitve za ohranitev ključnih družbenih in gospodarskih dejavnosti v Republiki Sloveniji. V njem so določene minimalne varnostne zahteve in zahteve za priglasitev incidentov za zavezance tega zakona, kar so tudi banke, saj bančništvo v osnovi spada med kritično infrastrukturo. Poleg tega predpis ureja pristojnosti, naloge, organizacijo in delovanje pristojnega nacionalnega organa za informacijsko varnost, kar je Uprava Republike Slovenije za informacijsko varnost, ki deluje kot organ v sestavi Ministrstva za javno upravo. V skladu s sporazumom z Ministrstvom za javno upravo opravlja naloge vladnega centra za odzivanje na omrežne incidente SI-CERT (Slovenian Computer Emergency Response Team), ki deluje v okviru javnega zavoda Arnes (Akademska in raziskovalna mreža Slovenije). Ta center je pristojen za priglasitev incidentov izvajalcev bistvenih storitev iz sektorjev energija, digitalna infrastruktura, oskrba s pitno vodo in njena distribucija, zdravstvo, promet, infrastruktura finančnega trga, preskrba s hrano in varstvo okolja, ponudnikov digitalnih storitev ter bančništvo. Banke morajo sicer, kot zahteva Sklep o uporabi Smernic o poročanju o večjih incidentih v skladu z Direktivo (EU) 2015/2366 (PSD2), poročati o večjih incidentih kibernetske varnosti tudi Banki Slovenije. Zakon o informacijski varnosti opredeljuje tudi postopke za določitev izvajalcev bistvenih storitev, ki jim predpis nalaga še dodatne obveznosti, vendar banka, ki jo opisujemo v tem zaključnem delu, to ni. Prav tako banka ni na splošno zavezana neposredno slediti zgoraj omenjeno direktivo PSD2, saj ne nudi plačilnih storitev, z izjemo določil, ki so zahtevane z drugimi veljavnimi predpisi v Republiki Sloveniji, vendar je direktiva zaradi dokaj podrobno podanih zahtev lahko dober vir za uvajanje dobre prakse.

Po drugi strani pa se od banke pričakuje sledenje Smernicam EBA o upravljanju tveganj, povezanih z IKT in varnostjo (EBA/GL/2019/04), saj je bila njihova uporaba zahtevana s Sklepom Banke Slovenije o uporabi Smernic o upravljanju tveganj, povezanih z IKT in varnostjo. Smernice posredno vključujejo tudi določene zahteve Direktive 2013/36/EU (CRD) v zvezi z notranjim upravljanjem ter Direktive (EU) 2015/2366 (PSD2). Smernice se med drugim nanašajo na sledeča področja:

- ureditev upravljanja in strategija,
- uporaba tretjih oseb v vlogi ponudnikov

- organiziranost in cilji
- vzpostavitev in vzdrževanje funkcij, procesov in sredstev
- ocenjevanja in obvladovanja tveganj
- poročanje,
- nadzor,
- politiko informacijske varnosti
- fizično in logično varovanje,
- varnost IKT operacij
- stalno spremljanje varnosti
- pregledi, ocena in testiranje informacijske varnosti,
- usposabljanje in ozaveščanje o informacijski varnosti
- upravljanje operacij IKT
- upravljanje incidentov in problemov IKT
- upravljanje projektov IKT
- upravljanje sprememb IKT, ki vključujejo nakupe in razvoje sistemov,
- upravljanje neprekinjenega poslovanja.

Iz prikazanega seznama področij je razvidno, da smernice celoviti obravnavajo področje informacijske tehnologije in varnosti ter so zelo aktualne tudi za ta revizijski pregled, saj med drugim opisujejo zahteve glede pregledov informacijske varnosti vključno z načini testov, na primer vdornimi testi, pogoje za preizkuševalce ter tudi okvirne frekvence pregledov.

Pri izvedbi notranjerevizijskega pregleda sta bila smiselno uporabljena tudi Zakon o varstvu osebnih podatkov (ZVOP-1) ter GDPR uredba (Uredba (EU) 2016/679 Evropskega Parlamenta In Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES (Splošna uredba o varstvu podatkov)).
Medtem, ko regulatorni predpisi, nudijo neko osnovo za opredelitev pregledov, je za podrobnejšo določitev obsega izvedbe oziroma podrobnih korakov potrebna uporaba splošno prepoznanih in sprejetih standardov, okvirov in dobrih praks, ki so opisano v naslednjem poglavju.

2.4.1 Dobre prakse

Od dobrih praks za področje upravljanja informacijske varnosti oziroma izvajanja revizij na področju informacijske tehnologije so uporabljeni sledeči okviri in standardi:

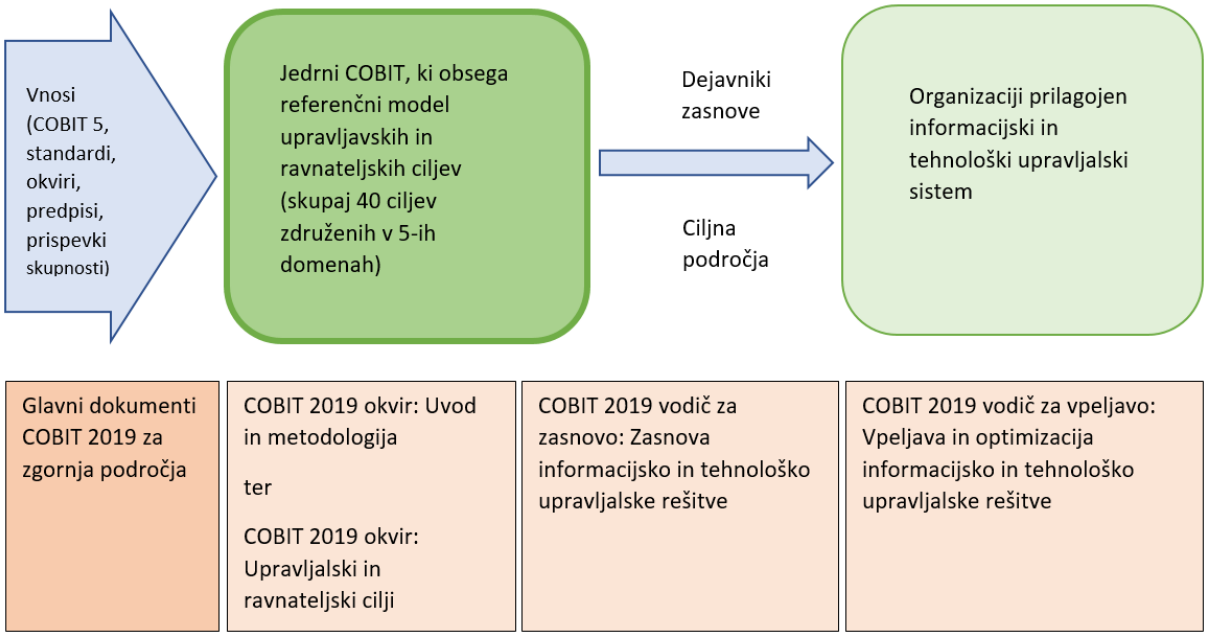
- Cobit 2019 in Cobit 5,
- ITAF (IT Assurance Framework/Okvir za dajanja zagotovil na področju informacijske tehnologije)
- ISO/IEC 27001:2013 Sistemi upravljanja informacijske varnosti – Zahteve in 27002:2013 Kodeks izvajanja kontrol informacijske varnosti,
- NIST v. 1.1,
- OSSTMM 3.0 (Open Source Security Testing Methodology Manual),
- OWASP top 10,
- MITRE ATT&CK.

Prvi trije bodo uporabljeni s strani službe notranje revizije pri načrtovanju in tudi izvedbi revizijskih postopkov, Cobit 2019/Cobit 5 ter ISO/IEC 27001/27002 pa z vidika določitve obsega pregleda in revizijskih pristopov, ITAF pa kot dopolnitev Standardom strokovnega ravnanja pri notranjem revidiranju. OSSTMM, OWASP ter MITRE ATT&CK so služili kot podlage za opredelitev postopkov, ki jih bo izvedel zunanji izvajalec. Slednji bo moral upoštevati te dokumente pri svojem delu, po drugi strani bodo uporabljeni tudi s strani službe notranje revizije za potrebe nadzora. NIST, Cobit, ISO/IEC 27001/27002 ter MITRE ATT&CK so uporabljeni kot sodila za uspešnost kontrol, slednji le s strani zunanjega izvajalca tehničnega dela pregleda.
Glavne značilnosti posameznih dobrih praks so opisane v nadaljevanju.

COBIT (Control Objectives for Information and Related Technologies)

COBIT (Kontrolni cilji za informacijske in sorodne tehnologije/Control Objectives for Information and Related Technologies), pripravljen s strani organizacije ISACA (Združenje za revizijo in nadzor informacijskih sistemov), se v stroki veliko omenja kot celovit sistem za razumevanje IT nadzorstva, saj povezuje IT s poslovnimi potrebami na osnovi skrbništva nad določenimi procesi. V bistvu je to okvir za upravljanje z IT, ki zagotavlja metrična in zrelostna orodja ravnateljstvu, s katerimi se opravlja nadzor. Razvit pa je bil z namenom, da pomaga vzpostaviti kriterije varnosti ter uspešnega nadzora pri upravljanju na področju informacijske tehnologije. Nad njim bdi IT Governance Institute v okviru ISACA, ki ima največ zaslug za to, da je skupek standardov sprejet kot vzor za kontrolo nad informacijami ter informacijsko tehnologijo in z njo povezanimi tveganji nasploh.

Slika 6: Pregled COBIT-a 2019



Vir: Povzeto po COBIT 2019 s strani avtorja

Bistvo COBIT-a je okvir, ki v trenutno aktualni verziji (COBIT 2019) združuje štirideset (Cobit 5 pa 37) upravljalskih in ravnateljskih ciljev za prav toliko IT procesov. Cilji so združeni v pet skupin (tako Cobit 2019 kot Cobit 5), ena je upravljalska:

- ovrednotenje, usmerjanje in nadzor;
- štiri pa ravnateljske:
- usklajevanje, načrtovanje in organiziranje,
- gradnja, nabava in vpeljava,
- dostava, storitve in podpora ter
- spremljanje, ovrednotenje in ocenjevanje.

Vsak cilj je povezan z enim procesom, ki pripomore k doseganju cilja. Skupine ciljev so združene glede na lastnosti. Cilj je v bistvu koncept, ki zagotavlja z določeno stopnjo verjetnosti, da se izognemo določenim tveganjem, torej običajno zmanjšamo ali celo odpravimo možnost, da se dogodi nek nezaželen dogodek s pomočjo določene kontrole oziroma več kontrol. Na ta način, upoštevajoč relevantna tveganja, izdelamo seznam, ki nam pogosto služi kot glavna osnova pri sestavljanju revizijskega programa. Tveganja, ki jih prepoznamo in vključimo v proces pregleda, razdelimo po prioriteti in izberemo najvišje ocenjena s ciljem posvetiti ustrezno pozornost pomembnejšim. COBIT sicer omogoča precej široko uporabo, na primer tudi vzpostavitev modela kazalnikov oziroma ocenjevanje zrelosti nekega področja, vendar bo uporaba v tem primeru omejena na namen notranjerevizijskega pregleda. Cobit okvir je sicer v banki običajno uporabljen kot osnovna podlaga za

izvedbo revizijskih pregledov s področja informacijske tehnologije, ki se glede na specifike posameznega pregleda dopolnjuje z drugimi standardi in dobrimi praksami. V obravnavanem revizijskem pregledu kibernetske varnosti je bil kot splošni okvir uporabljen COBIT 2019, pri oblikovanju posameznih korakov pa COBIT 5, saj COBIT 2019 še ni bil povezan z NIST okvirom. Pred tem je bila izpeljana podrobna primerjava med obema verzijami standardov, ki je pokazala, da prilagoditve niso potrebne, saj pregled ni bil odvisen od elementov, kjer so bile izvedene glavne spremembe (na primer SDLC tehnologij, kot sta DevOp in Agile).

NIST okvir (National Institute of Standards and Technology)

NIST okvir je bil razvit s strani Nacionalnega instituta za standarde in tehnologijo v ZDA na zahtevo sklepa predsednika države za izboljšanje kibernetske varnosti kritične infrastrukture v 2013. Pripravljen je bil na osnovi obstoječih standardov, smernic ter dobrih praks, prva verzija je bila zaključena v letu 2014. Okvir sestoji iz treh glavnih komponent:

- jedra,
- ravni implementacije in
- profilov.

Jedro predstavlja niz izbranih kibernetskih aktivnosti in želenih ciljev ter vodi organizacijo pri upravljanju in zmanjševanju kibernetskega tveganja. Ravni pomagajo organizaciji določiti, kako izvajati upravljanje z omenjenimi tveganji. So eden od vodil pri izbiri sprejemljivega tveganja, prioritet in opredelitvi potrebnih virov. Profili so določeni glede na lastne cilje, nivoje sprejemljivih tveganj in dodeljenih virov glede na cilje v povezavi z jedrom. Profili pomagajo določiti potrebne nadgradnje kibernetske varnosti v organizaciji.

Ker okvir zaradi svoje praktičnosti predstavlja koristno orodje pri obvladovanju kibernetskih tveganj, je bil v službi notranje revizije izbran za enega od ključnih okvirov pri izvedbi pregledov s področij, ki se tičejo kibernetske varnosti in je bil tudi delno prirejen za uporabo, kar predstavlja dokument v prilogi 6.

ISO/IEC 27001:2013 Informacijska tehnologija - Varnostne tehnike - Sistemi upravljanja informacijske varnosti – Zahteve in ISO/IEC 27002:2013 Informacijska tehnologija – Varnostne tehnike – Kodeks izvajanja kontrol informacijske varnosti (Information technology — Security techniques — Code of practice for information security controls)

Standarda ISO/IEC 27001:2013 in ISO/IEC 27002:2013 s področja informacijske varnosti sta pripravila Mednarodna organizacija za standardizacijo (International Organization for Standardization - ISO) in Mednarodna elektrotehnična komisija (International Electrotechnical Commission - IEC). V osnovi izvirata iz britanskega standarda BS 7799, ki je bil pozneje nadgrajen v ISO/IEC 17799 ter se uvrščata v t.i. družino standardov ISO 27000, katerih vsebina se nanaša na upravljanje informacijske varnosti. Medtem ko standard ISO/IEC 27001:20003 predstavlja predvsem sistem upravljanja informacijske varnosti, je standard ISO/IEC 27002:2013 kodeks izvajanja kontrol informacijske varnosti. Z drugimi besedami to pomeni, da je slednji namenjen predvsem izbiri kontrol za implementacijo sistema, ki temelji na ISO/IEC 27001:2013, oba pa sta poslovodno in od posameznih tehnoloških rešitev neodvisni orodji. Njun poglavitni namen je podati celovit pregled varovanja informacij pri poslovanju organizacije, na podlagi katerega je moč pripraviti temelje za izgradnjo sistema vodenja varovanja informacij. Informacijsko tehnologijo in informacije obravnavata v vseh možnih oblikah, ne le v elektronski, zato je veliko kontrol od skupno 114 organizacijske narave in niso povezane s tehnologijo. Omenjene kontrole, ki so namenjene doseganju 35-ih ciljev, so združene v 14 poglavjih. Za namen zaključne naloge so bili uporabljene izbrane kontrole, ki so se v teku priprav izkazale kot relevantne za pregled. Uporabljena dokumenta sta sicer standarda, vendar sta v tem primeru bila uporabljena kot primer dobre prakse, saj aktivnosti niso bile namenjene certificiranju organizacije.

ITAF (Okvir za dajanja zagotovil na področju informacijske tehnologije/ IT Assurance Framework)

ITAF je okvir pripravljen s strani ISACA, ki pri izvajanju storitev dajanja zagotovil nudi notranjemu revizorju na področju informacijskih sistemov pomoč pri zasnovi, izvedbi in poročanju. S tega vidika je komplementaren Standardom strokovnega ravnanja pri notranjem revidiranju, saj v osnovi pokriva podobno tematiko, vendar je bolj osredotočen na področje informacijske tehnologije in s tem vključuje

izrazoslovje in koncepte specifične za IT področje ter naslavlja nekatere posebnosti IT revizorja, in sicer predvsem z vidika vlog, odgovornosti, znanja in veščin, skrbnosti, postopkov ter poročanja. V tem primeru naloge je bil uporabljen predvsem z vidika izrazoslovja ter dodatnega preverjanja, da so vključeni vsi potrebni vidika pregleda.

OSSTMM 3.0 (Priročnik za metodologijo glede varnostnega testiranja - Open Source Security Testing Methodology Manual)

OSSTMM je priročnik, ki opisuje metodologijo za izvedbo varnostnih pregledov na področju informacijske tehnologije, prvenstveno kibernetske varnosti. Razvit je bil s strani instituta ISECOM (Institute for Security and Open Methodologies). Metodologija nudi pomoč pri testiranju varnosti na petih področjih in kot končni rezultat nudi celoviti oceno procesov na področju varnosti. Omenjenih pet področij sestavljajo:

- varnost z vidika človeškega faktorja,
- fizična varnost,
- brezžične komunikacije,
- telekomunikacije,
- podatkovna omrežja.

Uporaba metodologije je bila zahtevana s strani službe notranje revizije za zunanjega izvajalca varnostnega pregleda, da se zagotovi minimalni nivo izvedbe postopkov, in sicer predvsem glede vdornega testa.

OWASP (Projekt za zaščito odprtih spletnih aplikacij/The Open Web Application Security Project)

Fundacija OWASP je mednarodna neprofitna organizacija, katere namen je prispevati k izboljšanju varnosti programske opreme. Eden od njihovih projektov je tudi dokument »OWASP top 10«, ki predstavlja deset najbolj kritičnih tveganj za spletne aplikacije glede na mnenje večine članov, ki so v aktualni verziji v času pregleda (verzija 2017) sledeči:

- vrivanje (Injection),
- podtikanje skript (Cross-Site Scripting),
- napaka pri avtentikaciji in upravljanju sej (Broken Authentication and Session Management),
- nezavarovan neposreden dostop do objektov (Insecure Direct Object References),
- potvarjanje spletnih zahtevkov (Cross-Site Request Forgery (CSRF)),
- napake v varnostnih nastavitvah (Security Misconfiguration),
- nezadostna zaščita kriptografskih podatkov pri hrambi (Insecure Cryptographic Storage),
- neprimerna zaščita neposrednega dostopa do URL-ja (Failure to Restrict URL Access),
- nezadostna zaščita podatkov pri prenosu (Insufficient Transport Layer Protection),
- nepreverjene preusmeritve brskalnika (Unvalidated Redirects or Forwards).

V dokumentu je vsako od tveganj podrobneje predstavljeno, kar notranjemu revizorju pomaga identificirati ter oceniti pomanjkljivosti. V primeru zaključne naloge je bil dokument uporabljen komplementarno z MITRE ATT&CK, kar je bilo določeno v dogovoru z zunanjim izvajalcem.

MITRE ATT&CK

MITRE ATT&CK je med najbolj pogostimi orodji za uporabo metodologije »Cyber Kill Chain«. Ta povzema taktiko vojaškega napada, ki jo je na področju informacijske varnosti prvič v bolj standardizirani obliki uporabil Lockheed Martin. Okvir je v bistvu obsežna baza znanja o taktikah in tehnikah kibernetskih napadalcev, ki pomaga oceniti tveganja na tem področju. Razlog, zakaj je ta okvir v zadnjem času tako množično uporabljen, je predvsem v dejstvu, da je z njim mogoče lažje predvideti potencialna obnašanja napadalca in v skladu z ugotovitvami pravočasno okrepiti kontrolno okolje. Okvir omogoča, da uporabnik natančno identificira grožnjo, jo poveže z ustrezno kontrolo in tudi presodi, ali je slednja ustrezna. Skratka, je zelo praktičen. Pri tem je koristno tudi to, da uporablja poenoteno izrazoslovje in zelo podrobno opisane taktike ter tehnike, ki jih dopolnjujejo najrazličnejši strokovnjaki, saj je odprt za vse. Sklopi, ki se nekoliko razlikujejo glede na verzijo (za organizacije vključno z oblačno okolje, mobilna) lahko strnemo oziroma smiselni povzamemo v šest sklopov:

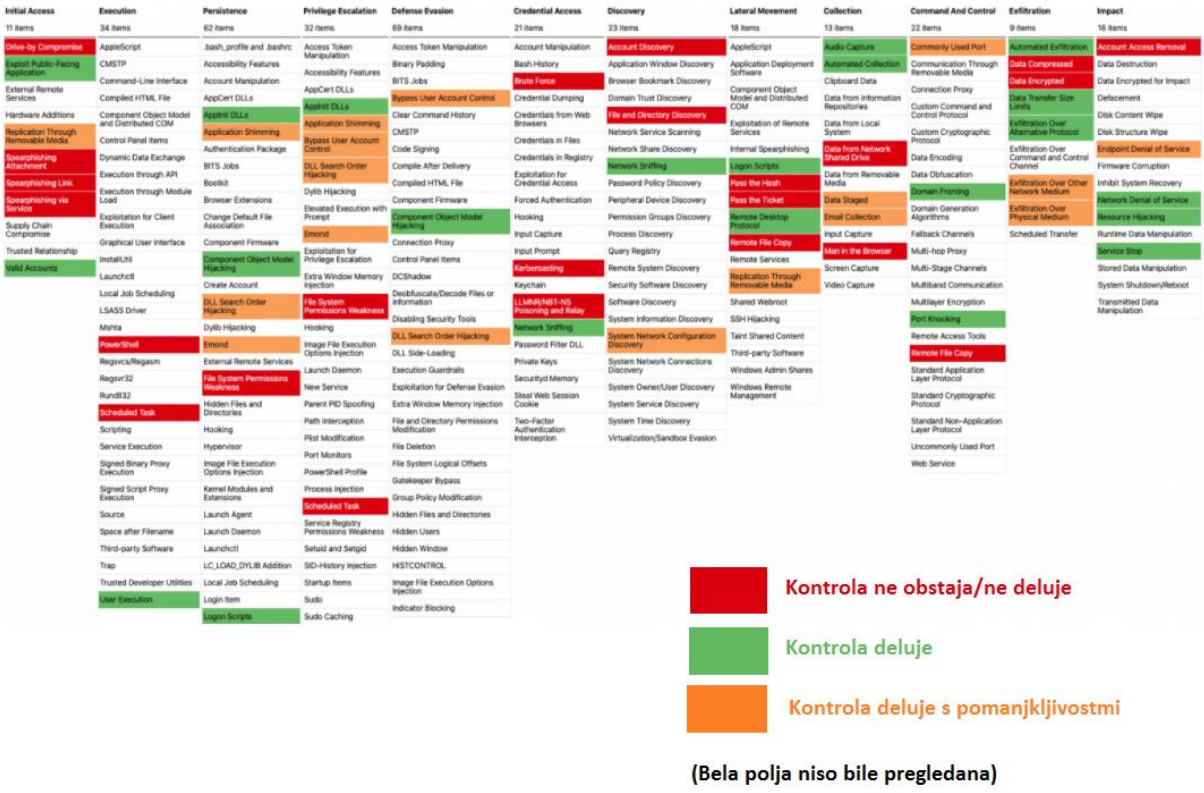
- poizvedovanje: skeniranje, iskanje varnostnih ranljivosti;
- priprava napada: način, vektor napada;

- dostava oziroma prenos: distribucija, širjenje, medij;
- zagon oziroma izraba (eksploatacija): izraba ranljivosti;
- post-eksploatacija: prevzem nadzora, prikrito gibanje, prikrito vztrajanje;
- doseganje cilja: odtekanje podatkov, sabotaža, prevzem upravljanja.

Okvir ponuja sicer še nadaljnje možnosti uporabe, na primer identifikacijo napadalcev, vendar bo v primeru zaključne naloge uporabljen za oceno skladnosti kontrol vzpostavljenih v banki s predlaganimi v okviru, in sicer verzija z dne 27.10.2020.

Primer izpolnjene matrike za primer končnih ocen kontrolnih mehanizmov po izvedenem pregledu, ki je bila za namen predstave vzeta s spletne strani organizacije MITRE in prirejena, je na spodnji sliki. V tem primeru so kontrole označene v matriki glede na oceno delovanja, vendar so lahko ocene oblikuje tudi drugače, glede na cilj pregleda. Namen vključitve je prikazati nazornost predstavitvene matrike, zato slaba berljivost imen posameznih kontrol ni bistvena.

Slika 7: Primer izpolnjene matrike MITRE ATT&CK za končno oceno kontrolnih mehanizmov vzet s spletne strani organizacije MITRE



Vir: Prirejeno po spletni strani organizacije MITRE (19.4.2021)

2.5 Ocenjevanje tveganj ter kontrolnega okolja za njihovo obvladovanje v banki

Banka redno ocenjuje tveganja, ki jih prevzema v okviru svojega poslovanja, ter kontrolno okolje, s katerim omenjena tveganja obvladuje. Proces ocenjevanja je sestavljen iz sledečih postopkov:

- določitev poslovnih procesov ter njihove pomembnosti,
- izbira pomembnih področij tveganja ter ocena njihovega vpliva,
- določitev pomembnosti kontrolnega okolja za posamezne procese,
- ocena inherentnega tveganja,
- ocena kontrolnega okolja,
- ocena preostalega tveganja.

Končni rezultat ocenjevanja je matrika ocen preostalega tveganja oziroma tveganosti ob upoštevanju kontrolnega okolja in je pripravljena na osnovi posameznih matrik (matrike tveganj, matrika ocen inherentnega tveganja, matrike ocen kontrolnega okolja).
Prvi korak na poti do ocenjevanja preostalega tveganja je razdelitev banke na poslovne procese. V nadaljevanju se vsakemu od njih določi pomembnost, in sicer na podlagi izbranih finančnih kazalnikov ter kvalitetnih kriterijev. Naslednji korak je določitev pomembnejših tveganj za posamezen proces. Za vsakega od njih se po procesih določi utež glede pomembnosti, ki je sestavljana iz več elementov, značilnih za posamezni proces. Vsak element se oceni posamično, vrednost uteži je združena ocena elementov po vnaprej določenem izračunu.
Po določitvi pomembnih tveganj se za vsako od njih po procesih določi inherentno tveganje, t.j. tveganje, ki izhaja iz bančne dejavnosti in trenutnega položaja banke brez upoštevanja ocene kontrolnega okolja. Ocena tveganja se določi z ocenjevanjem elementov posameznih področij. Elemente se ocenjuje kvantitativno in kvalitativno, in sicer najprej na ravni poslovnih procesov, nato se združijo še v ocene tveganosti na ravni poslovnih procesov in na ravni področij tveganj, ki privede do matrike ocen inherentnega tveganja.
Ocena kontrolnega okolja je prav tako izvedena na podlagi elementov, ki se nanašajo na okvir upravljanja s tveganji, poročanje (notranje in zunanje) in organiziranost, dokumentiranost pravil, kontrolni oziroma revizijski pregledi, skladnost z zakonodajo, ravnijo IT podpore, kadrovsko ureditvijo ter goljufije in prevare. Elementi se ocenijo na ravno procesa s pomočjo posebne lestvice za ocenjevanje in so nato v naslednjem koraku združene v oceno notranjih kontrol na nivoju posameznega poslovnega procesa in pa tudi v oceno notranjih kontrol na ravni banke. Tako dobimo matriko ocen kontrolnega okolja, ki je tabelarični prikaz ocene kakovosti kontrolnega okolja na nivoju poslovnih procesov banke ter na nivoju banke kot celote. Nato se izvede še ocena preostalega tveganja, to je ocene tveganja ob upoštevanju kvalitete kontrolnega okolja.
Kar se tiče kibernetske varnosti, je to področje vključeno kot eden od elementov pri ocenjevanju operativnega tveganja ter tudi v okviru kontrol informacijske varnosti kot eden od elementov za ocenjevanja kontrolnega okolja banke. Posredno je področje upoštevana tudi v okviru tveganja ugleda kot samostojnega tveganja ter tveganja skladnosti v okviru operativnega tveganja. To zagotavlja upoštevanje vidika kibernetske varnosti pri upravljanju tveganj banke, ki pridobiva na pomembnosti, saj je poslovanje banke vedno bolj odvisno od IT podpore, obenem se veča kompleksnost sistemov in tudi tehnik napadalcev.

3 IZVEDBA NOTRANJEGA REVIDIRANJE KIBERNETSKE VARNOSTI

3.1 Načrtovanje notranjega revidiranje kibernetske varnosti

Dobro načrtovanje je eden od bistvenih predpogojev za uspešno izvedbo revizijskih aktivnosti v več pogledih, saj so na podlagi njegovih rezultatov razporejeni viri ter določena področja in obsegi, ki bodo določali, kaj in na kakšen način bo ocenjeno.

Načrtovanje aktivnosti notranje revizije v obravnavani banki poteka na treh nivojih:
- strateško načrtovanje,
- letno načrtovanje,
- operativni načrt oziroma revizijski program posameznega posla.

Strateško načrtovanje pokriva obdobje treh let, kar sovpada s splošnim strateškim načrtovanjem v banki, ter kot rezultat bolj splošno določa področja ter vsebino okvirnega notranjega revidiranja v omenjenem obdobju ter kaže potrebe po virih, ki bodo omogočali notranji reviziji izvajanje svojega poslanstva. Strateški plan se preveri ob vsakem letnem oziroma ad-hoc načrtovanju ter se prav tako kot letni načrt predloži v potrditev upravi ter nadzornemu svetu. Oba, tako strateški kot letni načrt temeljita skladno s Mednarodnim standardom strokovnega ravnanja pri notranjem revidiranju številka 2010 na oceni tveganj posameznih področij, ki so potencialno predmet revidiranja. Področja so izpeljana iz procesov banke, vendar dopolnjena in nadalje bolj podrobno razdeljena in sestavljajo t.i. revizijsko okolje.

Najmanj enkrat letno oziroma po potrebi pogosteje se izvede omenjeno ocenjevanje tveganj področij, pri čemer se upoštevajo sledeči vidiki:

- ocene tveganosti posameznih področij banke, ki ga letno izvede posebna delovna skupina z namenom priprave celovitega pregleda nad banko v smislu identifikacije tveganj ter njihovega obvladovanja;
- stopnja revizijskega pokritja zunanjih dajalcev zagotovil;
- čas od zadnjega revizijskega pregleda ter stopnja pokritja področja z revizijskim pregledom;
- spremembe v notranjem okolju, na primer reorganizacije, spremembe IT podpore;
- spremembe v zunanjem okolju vključujoč spremembe predpisov;
- nivo realizacije priporočil.

Vsi ti elementi se v skladu s sprejeto metodologijo kvantificirajo in na podlagi uteži se za vsako področje izračuna ocena. Nadalje se upoštevajo še sledeči kriteriji:

- obvezne notranje revizije kot zahtevane s predpisi,
- predlogi uprave ter nadzornega sveta.
- morebiti nedokončane revizije iz preteklega obdobja,
- predvideni pregledi s strani drugih dajalcev zagotovil, da se prepreči podvajanje dela.

Ob upoštevanju še zgoraj naštetih kriterijev se področja razdelijo v tri skupine, pri čemer se najvišje ocenjena področja, torej prva skupina, uvrstijo v letni načrt dela. Vodja notranje revizije letni in strateški načrt dela predloži v potrditev upravi ter nadzornemu svetu.

Načrtovanje aktivnosti poteka v interno razviti aplikaciji, kamor se vnesejo tudi okvirna obdobja za izvedbe posameznih revizij, potrebni viri za izvedbo pregleda, okvirni cilj ter obseg revizije, kar je del letnega načrta dela notranje revizije in se tudi predstavi upravi oziroma nadzornemu svetu.

Pri načrtovanju posameznega pregleda se revizor podrobneje seznani s področjem revidiranja, procesi na tem področju, cilji ter odgovornimi, predvsem pa s tveganji ter vzpostavljenimi notranjimi kontrolami, saj ta faza temelji na analizi upravljanja tveganj ter kontrolnih mehanizmov za njihovo zaznavanje oziroma obvladovanje.

Revizijski pregled revidiranja kibernetske varnosti je bil načrtovan za začetek leta 2021. Zasnova pregleda je vključevala tveganja povezana s kibernetsko varnostjo v okviru IT varnosti v povezavi s procesom tehnološko informacijske podpore, povezana tveganja tudi iz drugih področij, kot so na primer posamezni deli fizične varnosti, strateško in operativno planiranje ter upravljanje s tveganji, da se zagotovi celovitost pregleda in s tem boljša pokritost tveganj. Izbor je bil opravljen na podlagi ocene tveganosti ter predhodno opisane metodologije. V skladu z metodologijo službe notranje revizije naj bi bilo načeloma vsako področje pokrito vsaj enkrat v obdobju treh let. Glede na višjo oceno tveganosti za IT varnost, je to področje vsaj delno vključeno v redne revizijske preglede na letni osnovi.
Po potrditvi letnega načrta, v katerega je bila vključena tudi izvedba omenjenega pregleda, se določi notranji revizor(ka) oziroma revizijska skupina, ki bo izvajal(a) aktivnosti. Vodja te skupine mora pred izvedbo pregleda pripraviti načrt samega revizijskega pregleda, ki obsega:

- določitev ciljev in obsega pregleda,
- pridobitev razumevanja področja pregleda,
- identifikacija in ocena tveganj za področje pregleda vključno s tveganji prevar,
- identifikacija in začetna ocena ključnih notranjih kontrol,
- določitev revizijskih postopkov,
- priprava revizijskega načrta ter razdelitev aktivnosti med člani revizijske skupine.

Načrt pregleda mora potrditi vodja notranje revizije.

Pri načrtovanju revizijskega posla je bilo z izvedbo zgornjih korakov sledeno zahtevam Mednarodnega standarda strokovnega ravnanja pri notranjem revidiranju številka 2201, ki zahteva upoštevanje:

- strategij in ciljev dejavnosti, ki se pregleduje, in sredstev, s katerimi ta dejavnost obvladuje svoje izvajanje;
- pomembnih tveganj za cilje, vire in delovanje te dejavnosti ter sredstev in načinov, s katerimi se morebitni vpliv tveganja ohranja na sprejemljivi ravni;

- ustreznosti in uspešnosti upravljanja dejavnosti, obvladovanja tveganj in kontrolnih postopkov v primerjavi z ustreznim okvirom ali modelom;
- priložnosti za pomembnejše izboljšave pri upravljanju dejavnosti, obvladovanja tveganj in kontrolnih postopkih.

V omenjenem pregledu je bilo zaradi specifičnosti področja oziroma tehničnih znanj, ki so potrebna za pregled sistemov že od vsega začetka načrtovano, da se angažira zunanjega izvajalca, veščaka za pregled tehničnih področij. To je bilo tudi vključena v letni načrt ter predvideni potrebni viri v finančnem načrtu. Podrobnejši opisi izvedenih postopkov s strani zunanjega izvajalca so podani v poglavju Izvedba revizijskega pregleda, tu so v nadaljevanju opredeljeni mehanizmi za obvladovanje specifičnih tveganj zaradi angažiranja zunanjega izvajalca za izvedbo posameznih delov revizijskega pregleda tehnične narave. Poglavitna identificirana tveganja so se nanašala na morebitno neustrezno kvaliteto izvedenih storitev, nepravočasno izvedene storitve, izgubo nadzora nad izvajanjem postopkov, presežene stroški, nepooblaščen dostop do zaupnih podatkov ali nepooblaščeno izvajanje operacij, razkritje zaupnih podatkov, omejitve neodvisnosti ali nepristranskosti. Mehanizmi za obvladovanje naštetih tveganj so obsegali:

- natančno pogodbeno opredeljeni obsegi, zneski, roki in pogoji izvedenih storitev vključno z dokumentiranostjo postopkov ter dostavljenimi dokumenti, ki morajo biti potrjeni s strani SNR,
- opredeljeni načini izvedbe postopkov z obvezujočim upoštevanjem v pogodbi določenih dobrih praks, in sicer predvsem mednarodno priznanih okvirov ter standardov,
- izbor izvajalca na podlagi natančno določenih kriterijev glede znanj ter izkušenj,
- opredeljene pogodbene kazni za zamude in nekvalitno izvedbo,
- pogodbeno opredeljeni postopki nadzora in poročanja,
- izjave glede neodvisnosti,
- natančno opredeljene pravice dostopov in vključenost dodeljenih uporabniških imen v spremljavo,
- pogodbena določila glede varovanja zaupnih podatkov,
- določeni pogoji, ki morajo biti izpolnjeni pred izvedbo plačila izvedenih storitev,
- prisotnost predstavnika notranje revizije pri izvajanju postopkov.

3.1.1 Obseg in cilji notranje revizijskega posla

Po Turku obseg revizije (2002, s. 378) predstavljajo revizijski postopki, ki so v danih okoliščinah potrebni za dosego cilja posamezne revizije, cilji (2002, s. 647) pa natančne navedbe, kaj se z revizijo želi doseči in na katera vprašanja naj revizija odgovori. Revizijski koraki (Turk, 2002, s. 647) predstavljajo posamezne stopnje revidiranja v okviru sprejete revizije. Sawyer cilje razdeli na splošne in specifične (2003, s. 226), pri čemer se splošni zasledujejo skozi ves revizijski pregled in so določeni z obsegom, specifični revizijski cilji pa so povezani s posameznimi izvedbenimi (operativni) cilji. Po drugi strani Sawyer navaja (2003, s. 223), da revizijski cilji, ki jih ne deli dalje, opredeljujejo obseg. Revizijske postopke enači z s tehnikami, ki jih revizor uporabi, da lahko presodi, ali so bili izvedbeni cilji doseženi. Obseg pa opisuje (Sawyer, 2003, s. 223), kaj bo pregled pokrival in kaj ne.

Cilj notranje revizijskega posla v konkretnem primeru je preveriti skladnost kontrolnega sistema z zakonodajo in dobrimi praksami za področje kibernetske varnosti. Namen pregleda je tako odkriti pomanjkljivosti oziroma odstopanja na preučevanem področju ter podati ukrepe za njihovo odpravo in tako zmanjšati operativno tveganja na raven, ki je sprejemljiv za banko. Pri določitvi cilja je bil upoštevan Standard strokovnega ravnanja pri notranjem revidiranju št. 2210. V okviru revizijskega poročila je podana stopnja zagotovila, v kolikšni meri kontrolni sistem na pregledanem področju izpolnjuje zahteve zakonodaje ter vodilnih dobrih praks v zvezi s kibernetsko varnostjo, kar z drugimi besedami pomeni, da je podano ocena, ali je kibernetska varnost banke glede na splošno znane ranljivosti v času pregleda smatra kot ustrezna.

Obseg posla je opredeljen na podlagi zastavljenega revizijskega cilja, kot določa Mednarodni standard strokovnega ravnanja pri notranjem revidiranju št. 2220, ki pa v skladu s standardom št. 2210 odraža rezultate začetne ocene tveganj.

Obseg pregleda, ki temelji na oceni tveganosti, je zajemal sledeče elemente:
- strategijo,
- podlage,
- organiziranost,
- zunanje varnostno preverjanje storitev,
    - splošni pregled naprav in storitev iz javno dostopnega omrežja (vključno s podatki o omrežju, strežnikih, tipologiji, storitvah),
    - podrobnejši pregled DNS storitev, poštnih storitev, VPN povezav,
- varnostni pregled požarne pregrade,
    - dostopi, sistemske nastavitve, varnostne politike,
    - nadzorovan vdorni test,
- pregled sistemov za informacijsko zaščito,
- notranji varnostni pregled kritičnih aplikacij in sistemov,
    - Varnostni pregled strežnikov in omrežnih naprav,
    - Pregled sistemske programske opreme,
    - Pregled kritičnih 4 aplikacij (izbrane aplikacije) z vidika nepooblaščenega dostopa ter nepooblaščenega izvajanja operacij (za podporo procesu financiranja, za upravljanje portfeljev finančnih instrumentov, glavna knjiga in saldakonti, aplikacija za poročanje strank ter dveh povezanih interno razvitih aplikacij za vodenje šifrantov ter vodenje osnovnih sredstev),
- socialni inženiring,
- poročanje,
- nadzor.

Podrobnejši obseg revizije je razviden tudi iz revizijskega programa, ki je v prilogi 5.

Tehnični del pregleda (pregled naprav in storitev opravljen z avtomatiziranimi orodji in ročnimi postopki, nastavitve sistemov, priprava scenarijev ribarjenja in pošiljanje povezanih sporočil) je izvedel zunanji izvajalec pod nadzorom službe notranje revizije. Z njim je bil dogovorjen tudi verifikacijski pregled glede implementacije priporočil, natančen čas izvedbe bo dogovorjen naknadno po pregledu glede na ugotovitve in priporočila.
Pregledano obdobje (evidence varnostnih dogodkov, zapisniki, poročila) je za leto 2020.

Pri določitvi obsega revizije so se upoštevali tudi pregledi oziroma izsledki iz pregledov, ki so bili izvedeni v preteklosti (v predhodnih dveh letih) in so v deloma tudi komplementarni, saj se vsaj delno nanašajo na področje informacijske varnosti:
- Načrt neprekinjenega poslovanja,
- IT varnost – dostopne pravice
- Upravljanje dogodkov operativnega tveganja,
- Upravljanje sprememb na področju informacijske tehnologije,
- Informacijska varnost.

Zato je bilo po eni strani več pozornosti namenjeno elementom, ko so bili na podlagi predhodnih pregledov ocenjeni kot bolj tvegani, po drugi strani pa so bili za določene, z namenom izogibanja podvajanju dela, ob ustrezni oceni tveganosti izbrani manj podrobni postopki preverjanja (na primer eskalacijski postopki v zvezi z dogodki operativnega tveganja).

Upoštevani so bili tudi pregledi službe informacijske varnosti. V zvezi s tem so bile pregledana njihova poročila za zadnji dve leti. Omenjena organizacijska enota letno izvede vsaj en obsežnejši varnostni pregled, poleg tega pregleda vsako novo aplikacijo ob prenosu v produkcijo.

Z upoštevanjem cilja obsega revizijskih aktivnosti ter zapletenosti področja je bila pripravljena ocena potrebnih virov, s čimer so bile upoštevane zahteve Mednarodnega standarda strokovnega ravnanja pri notranjem revidiranju št. 2230. Pripravljena ocena po posameznih podpodročjih je razvidna iz spodnje tabele.

Tabela 1: Ocena potrebnih virov za izvedbo notranje revizijskega pregleda

PODPODROČJE	**OCENJENA POTREBA PO VIRIH (ČLOVEK DNI)**
NAČRTOVANJE IN PRIPRAVA Opredelitev ciljev in obsega Angažiranje zunanjega izvajalca Najava revizijskega pregleda Uvodni sestanek Seznanitev s področjem Priprava memoranduma Seznanitev in ocena kontrol Revizijski program	6,5
IZVEDBA PREGLEDA Izvedba postopkov Koordinacija zunanjega izvajalca Ugotovitve in priporočila	7
POROČANJE Priprava osnutka poročila Uskladitev poročila Končno poročilo Zaključni sestanek Komuniciranje	4
DOKUMENTIRANJE Vnos v aplikacijo Dokumentiranje in arhiviranje dokumentacije	1
POREVIZIJSKE AKTIVNOSTI Ocena kakovosti	1,5
SKUPAJ	**20**

V zgornji tabeli ni upoštevan čas za spremljavo izvedbe revizijskih priporočil, ki je tudi v okviru letnega načrtovanja ločen od posameznih revizijskih pregledov. Razdelitev dela med posamezne člane revizijske skupine so izvedene ločeno. V tem primeru pregleda bo postopke izvedel en notranji revizor, ki bo tudi koordiniral aktivnosti zunanjega izvajalca.

Formalno se revizijski pregled začne s potrditvijo posla s strani vodje Službe notranje revizije. Predpogoj za izvedbo omenjene potrditve je dokončanje sledečih elementov:

- določitev podlage za izvedbo revizijskega postopka, ki je v tem primeru letni načrt dela službe notranje revizije;
- določitev cilja in obsega revizijskega pregleda;
- narejena ocena potrebnih virov – v tem primeru poleg zaposlenih v službi notranje revizije in predvidenega števila potrebnih dni za izvedbo še sodelovanje zunanjega izvajalca.

3.1.2 Priprave na izvedbo pregleda

Korak priprave na izvedbo pregleda sicer pod takim nazivom ni formalno opredeljen v metodologijo notranje revizije, vendar so tukaj smiselno predstavljeni trije zelo pomembni standardni koraki ter še četrti, specifičen za ta posel, ki je spodaj naveden kot zadnji:

- najava revizijskega pregleda,
- uvodni sestanek,
- predhodna raziskava področja z memorandumom o načrtovanju revizijskih aktivnosti,
- vključitev zunanjega izvajalca.

Pred začetkom revizijskih postopkov se revidirancem pošlje najava, s katero se jih obvesti o nameravanih aktivnostih. Najava se pošlje prek elektronske pošte, in sicer praviloma en teden pred začetkom t.i. terenskega dela, kar pomeni izvedbo postopkov pri revidirancih. V tem konkretnem pregledu je bila najava posredovana vodji informacijske varnosti, vodji oddelka informatike, vodji splošnih služb, direktorju divizije Podpora ter v vednost upravi. Najava je odložena v elektronski arhiv pod oznako A.02.01, dokument je tudi priložen kot priloga 3.
V najavo so vključeni sledeči elementi:

- podlaga za izvedbo revizijskega pregleda,
- datum začetka revizijskih aktivnosti ter predvidenem zaključku,
- notranji revizorji, ki bodo izvajali revizijske postopke ter vodji revizijske skupine, če je revizorjev več,
- cilj in obseg revizijskega pregleda,
- seznam začetnih potrebnih podatkov oziroma dokumentov.

V konkretnem primeru je najava vsebovala zahtevo za posredovanje morebitnih izvedbenih navodilih, ki niso hranjeni v centralni zbirki internih aktov banke.

Kmalu po začetku izdane najave je organiziran tudi uvodni sestanek, na katerem so obravnavane predvsem sledeče zadeve:

- predstavljen in, če potrebno, dodatno pojasnjen cilj in obseg revizijskega pregleda;
- predstavljene so tudi predvidene revizijske metode ter potek revizijskih aktivnosti;
- pridobljene so dodatne informacije o predmetu revizije oziroma izmenjavi le-teh z revidiranci. s slednjimi so razjasnjene morebitne nejasnosti v zvezi s spoznanji o revidiranem področju, ki so bili pridobljeni do časa izvedbe uvodnega sestanka ter s tem poglobljeno razumevanja področja revidiranja s strani revizorja;
- pridobljeno je mnenje revidirancev o posebnostih področja ter predstavljenih postopkih skupaj z izpostavitvijo morebitnih delov procesa, ki zahtevajo večjo pozornost pri izvedbi pregleda;
- dogovorjen je okviren potek postopkov pregleda pri revidirancih.

Uvodni sestanek je lahko skupen z vsemi revidiranci naenkrat, ločeno ali kombinacija obeh načinov, odločitev je odvisna od vodja revizijske skupine in njegove ocene o najučinkovitejšem pristopu. V konkretnem primeru je bil organiziran za vse skupaj, na njem še ni bilo zunanjega izvajalca, ki se je pridružil sestankom pozneje.

Najpozneje po posredovanju najave začne notranji revizor oziroma revizijska skupina s predhodno raziskavo področja, ki obsega:

- seznanitev z zakonodajo, ki ureja področje revidiranja;
- vpoglede v ustrezne baze;
- seznanitev z internimi akti, ki urejajo področje revidiranja;
- seznanitev z interno organiziranostjo revidiranega področja;
- seznanitev s popisom procesov ter kontrol;
- pregled ugotovitev iz predhodnih revizij ter zunanjih dajalcev zagotovil;
- pregled ključnih sklepov organov oziroma odborov upravljanja s področja pregleda;
- pregled relevantnih poročil za notranje in zunanje uporabnike.

Omenjeni izvedeni postopki z navedeno dokumentacijo predstavlja osnovo za pripravo dokumenta Memorandum o načrtovanju pregleda z namenom pridobitve ustrezne stopnje razumevanja področja za

te faze ter tudi izhodišče za oceno izpostavljenosti možnim tveganjem ter opredelitvijo ključnih kontrol za obvladovanje tveganj ter okvirni nabor revizijskih postopkov za doseganje ciljev pregleda. Memorandum, ki sestoji iz spodaj navedenih delov, se shrani v mapo A.04:

- opis področja,
- oddelki vključeni v revizijski pregled,
- zunanji in notranji predpisi/akti,
- predhodni zunanji in notranji pregledi
- sklepi organov in odborov,
- notranja in zunanja poročila,
- cilj revizijskega pregleda,
- ključni dejavniki tveganja,
- okvirni obseg pregleda in predvideni postopki revidiranja,
- obdobje zajeto v pregled,
- vodja revizijskega pregleda in člani

Primer Memoranduma je v prilogi 2.

Na podlagi izvedenih začetnih postopkih in pridobljenih informacijah je bila pripravljena začetna analiza sestavin notranjega kontroliranja v skladu s COSO metodologijo. Njena struktura ter rezultati začetne analize so sledeči:

- Kontrolno okolje
    - Etične vrednote: so na visokem nivoju. Vodstvo vodi z zgledom, predpisi so vzpostavljeni in se komunicirajo tako v obliki dokumentov kot prek izobraževanj.
    - Upravljanje s tveganji: ustrezno vzpostavljeno in redno izvajano. V pregledih visoko ocenjeno.
    - Strategija: Postavljena, cilji so usklajeni.
    - Organiziranost: Segregacija dolžnosti zagotovljena, vzpostavljeni so odločevalski in poročevalski tokovi.
    - Podlage: Pomembni procesi, pristojnosti in postopki so dokumentirani.
    - Informacijski sistem: Kompleksen osrednji sistem, podporne aplikacije ter varnostni sistemi. Zaradi kompleksnosti precej zunanjega izvajanja.
- Ocenjevanje tveganj
    - Proces: Postopki za identifikacijo in ocenjevanje pomembnih tveganj so vzpostavljeni. Izvajajo se vsaj letno oziroma ob vsaki spremembi.
    - Podlage: Postopki identifikacije in ocenjevanja so dokumentirani. Elementi IT varnosti ter tudi kibernetske varnosti so vključeni.
- Kontrolne aktivnosti
    - Podlage: Procesi so popisani in redno ažurirani. V okviru popisov so identificirane kontrole. Kontrole so postavljene tako, da podpirajo doseganje ciljev.
    - Izvedba: Zavedanje med zaposlenimi je ustrezno. Zaradi kompleksnosti aplikativnih kontrol oziroma preobremenjenosti pri ročnih se lahko pojavljajo napake.
- Informiranje in komuniciranje
    - Notranje: Vzpostavljeni so komunikacijski tokovi. Predvidena so redna poročila za področje informacijske varnosti, ki je predstavljano IT odboru ter posredovano tudi upravi/NS.
    - Zunanje: Opredeljeni so poročevalski tokovi kot zahtevano z zakonodajo v primeru kritičnih incidentov (do začetka izvedbe revizijskega pregleda ni bilo takšnih dogodkov).
- Aktivnosti spremljanja
    - Redne aktivnosti izvaja OE informacijske varnosti. Poslovodstvo in IT odbor ter tudi NS so obveščeni o ugotovitvah. V skladu z oceno tveganosti preglede izvaja tudi služba notranje revizije, ki prav tako poroča upravljalnim organom.

V skladu z Mednarodnim standardom strokovnega ravnanja pri notranjem revidiranju št. 1210 morajo notranji revizorji imeti znanje, veščine in druge sposobnosti, ki so potrebne za izvajanje posameznih nalog. Pri tem ni nujno, da ima vsak revizor vsa znanja, veščine in druge sposobnosti, ki so potrebne pri

opravljanju njenih nalog. Ampak mora biti to doseženo na nivoju celotne službe notranje revizije, odvisno od kompetenc posameznega revizorja se potem ti razporejajo na posamezne posle. V primeru, da nihče od zaposlenih v službi notranje revizije nima potrebnih znanj za pregled določenega področja, je dolžnost vodje notranje revizije, da pridobi pomoč. V banki je v službi notranje revizije zaposlen preizkušeni revizor informacijskih sistemov, ki ima tudi znanja in izkušnje s tega področja, vendar je bilo za konkretni pregled predvideno, da se preverijo kontrolni mehanizmi, ki zahtevajo specifično tehnično znanje. Zato je bilo že v okviru letnega načrta, ki je potrjen s strani uprave in nadzornega sveta, predvideno, da se angažira zunanji strokovnjak oziroma veščak (v nadaljevanju zunanji izvajalec). Pri tem je bilo načrtovano, da bo zunanji izvajalec izvedel le posamezne tehnične dele pregleda, delo in rezultate bo koordiniral oziroma nadziral zaposleni v službi notranje revizije z dovolj strokovnega znanja za to nalogo.

V času priprav na notranje revizijski pregled so se tudi začeli postopki za pridobitev zunanjega izvajalca. Natančneje so bili določeni postopki, ki jih bo slednji izvedel in so v osnovi obsegali sledeče:

- zunanje varnostno preverjanje storitev (z upoštevanjem OSSTMM 3.0 (Open Source Security Testing Methodology Manual), OWASP top 10 in MITRE ATT&CK):
    - pregled naprav in storitev (omrežje, strežnike, tipologija, storitve, DNS storitev, poštne storitve, VPN povezave) z avtomatiziranimi orodji iz javno dostopnega omrežja ter ročni pregled in potrditev zaznanih pomanjkljivosti;
    - klasifikacija zaznanih pomanjkljivosti po metodologiji MITRE ATT&CK, ovrednotenje pomanjkljivosti glede na kritičnost ter priporočilo za odpravo.
- varnostni pregled požarne pregrade:
    - pregled varnostne politike, nastavitve požarnega zidu glede sistemskih pravil, segmentacije omrežja, dostopov uporabnikov in storitev, varnosti uporabljenih protokolov, zaznave in obveščanja morebitnih incidentov;
    - izvedba vdornega testa z upoštevanjem OSSTMM 3.0 (Open Source Security Testing Methodology Manual), OWASP top 10 in MITRE ATT&CK.
- pregled sistemov za informacijsko zaščito (z upoštevanjem OSSTMM 3.0 (Open Source Security Testing Methodology Manual), OWASP top 10 in MITRE ATT&CK):
    - pregled sistema SIEM:
        - organiziranosti ter odgovornosti;
        - Z vidika kontrol dostopa in možnosti nepooblaščenega spreminjanja nastavitev ter podatkov;
        - celovitosti vključenih virov;
        - poročilnih zmogljivosti sistema z vidika pripravljenih poročil;
        - zmogljivosti sistema glede na predvidene obremenitve ter hrambe podatkov;
        - pregled zaznav in alarmiranja s simulacijami zbiranja informacij iz zunanjega omrežja, poskusov nepooblaščenih dostopov iz zunanjega omrežja ter notranjega omrežja, uporabe nepooblaščenih naprav v notranjem omrežju, poskusov nepooblaščenih dostopov iz notranjega omrežja, prikritega (lateral movement) med segmenti, izvedba neavtoriziranih ter neobičajnih aktivnosti;
    - na strežnikih, omrežni opremi in končnih napravah (EDR).
- notranji varnostni pregled kritičnih aplikacij in sistemov (z upoštevanjem OSSTMM 3.0 (Open Source Security Testing Methodology Manual), OWASP top 10 in MITRE ATT&CK):
    - varnostni pregled strežnikov in omrežnih naprav, sistemske programske opreme z avtomatiziranimi orodji ter ročni pregled glede varnostnih nastavitev, uporabljenih protokolih komuniciranja, kontrolnih mehanizmov nepooblaščenega dostopanja in izvajanja operacij;
    - pregled kritičnih aplikacij z vidika nepooblaščenega dostopa ter nepooblaščenega izvajanja operacij:
        - sistem za podporo procesu financiranja (aplikacija Krediti);
        - sistem za upravljanje portfeljev finančnih instrumentov (aplikacija FI);

        - glavna knjiga in saldakonti (aplikacija GK);
        - sistem, prek katerega stranke oddajajo dokumente te poročajo (aplikacija Stranke).
- socialni inženiring:
    - izvedba dveh simulacij ribarjenj (phising napadov) z lažnimi sporočili – enkrat s zlonamerno povezavo in drugič s škodljivo priponko;
    - poskus nepooblaščene pridobitve informacij prek telefona (dva scenarija);
    - poskus nepooblaščenega vstopa v prostore banke.
- verifikacijski pregled o odpravi pomanjkljivosti:
    - izveden v roku 6 mesecev (točen datum določen naknadno) po izdaji končnega poročila z namenom preveritve odprave vseh ugotovljenih pomanjkljivosti.

Z namenom, da se pridobi zunanjega izvajalca, so bila pripravljena in poslana povpraševanja več ponudnikom, podjetjem s področja informacijske tehnologije, ki ponujajo varnostne storitve. V povpraševanjih so bila dodane še določene tehnične informacije (število sistemov in naprav, glavne značilnosti), ki so omogočale podjetjem pripraviti primerljive ponudbe. Določeno je bilo, da se bodo preverjanja opravila s predhodnim razkritjem dela informacij (t.i. grey-box pristop). Zahtevano je bilo, da ima v ekipi, ki bo opravila preverjanja, vsaj en od članov ekipe certifikat etičnega hekerja ter da so v zadnjih treh letih izvedbi vsaj tri tovrstne preglede v primerljivih organizacija. Povpraševanjem je bil priložen tudi že osnutek pogodbe, da so se potencialni ponudniki lahko seznanili s splošnimi pogoji sodelovanja, ki so med drugim vključevali:

- predmet pogodbe;
- kraj izvedbe in način izvedbe;
- način sodelovanja med službo notranje revizije ter zunanjim izvajalcem;
- določila glede nadzora in potrjevanja ustreznosti ter kvalitete dela ter morebitne popravljalne ukrepe;
- določila glede dokumentiranja postopkov ter poročanja vključno s predstavitvenimi sestanki;
- okvirnim terminom izvedbe ter končni datum za dokončanje vseh aktivnosti;
- upoštevanje zahtevanih standardov;
- določila glede hranjenja dokumentov ter zaupnosti in podatkov in nerazkrivanja nepooblaščenim osebam;
- določila glede neodvisnosti ter odsotnosti navzkrižja interesov;
- zahteve glede vsebine ponudbe.

Na osnovi prejetih ponudb je bilo z uporabo posebnega točkovnika izbrano podjetje, s katerim je bila podpisana pogodba za izvedbo storitev.

3.1.3 Začetna ocena tveganj na področju kibernetske varnosti ter mehanizmov za njihovo zaznavanje ter preprečevanje

Standard strokovnega ravnanja pri notranjem revidiranju številka 2201 zahteva, da se pri načrtovanju posla upošteva poleg strategij, ciljev in sredstev za obvladovanje izvajanja dejavnosti, ki se pregleduje, tudi pomembna tveganja ter sredstva in načine za njihovo ohranjanje na sprejemljivi ravni, ustreznost in uspešnost upravljanja dejavnosti, obvladovanja tveganj in kontrolnih postopkov ter priložnosti za izboljšave teh aktivnosti.
Skladno z zgoraj opisano zahtevo je potrebno pripraviti začetno oceno tveganj ter kontrolnih mehanizmov. Ocena tveganj temelji na kombinaciji ocene verjetnosti, da se uresničijo, ter moči vpliva na zastavljene cilje banke. Ocenjevanje poteka v obliki matrike tveganj, ki vključuje sledeče ocene:

- ocena verjetnosti uresničenja tveganja,
- ocena vpliva tveganja na doseganje zastavljenega cilja,
- začetna ocena posameznega tveganja,
- začetna ocena kontrolnega mehanizma.

Najprej se oceni verjetnost uresničenja tveganja oziroma nastanka dogodka. Glede na postavljene kriterije verjetnost lahko določimo kot veliko, srednjo ali majhno. Nadalje ocenimo morebitni vpliv tveganja na doseganje zastavljenih ciljev, pri čemer možen vpliv dogodka lahko določimo kot velik, srednji ali majhen. Začetna ocena posameznega tveganja se določi na podlagi kombinacije ocene verjetnosti uresničitve tveganja ter vpliva na doseganje cilja, začetna ocena ustreznosti kontrolnega mehanizma, ki se opredeli na podlagi predhodne raziskave področja, pa se določi kot ustrezna ali neustrezna. Kriteriji oziroma pojasnila za ocene so opredeljene v spodnjih tabelah.

Tabela 2: Ocena verjetnosti uresničenja tveganja

Ocena	Kriterij/pojasnilo
Velika	Velika verjetnost uresničitve tveganja, uresničitve se ponavljajo (enkrat letno ali pogosteje).
Srednja	Tveganje se je že uresničilo, taki dogodki se dogajajo občasno (okvirno enkrat na tri leta)
Majhna	Verjetnost za uresničitev tveganja je minimalna (okvirno enkrat na deset let).

Tabela 3: Ocena vpliva tveganja na doseganje zastavljenega cilja

Ocena	Kriterij/pojasnilo
Velik	Uresničitev tveganja ima občuten vpliv na doseganje zastavljenega cilja (padec v kakovosti storitev onemogoča normalno poslovanje, izguba ugleda lahko ogrozi poslovanje banke, znatne finančne izgube, hujša kršitev obveznosti z visoko verjetnostjo sankcij z znatnimi finančnimi posledicami, izguba informacij onemogoča normalno poslovanje banje, znatna poslovna škoda z dolgotrajnim vplivom).
Srednji	Uresničitev tveganja vpliva na doseganje zastavljenega cilja (občuten padec kakovosti storitev za stranke, izgubo ugleda je potrebno sanirati, opazna finančna izguba, kršitev zakonskih oziroma pogodbenih obveznosti z verjetnostjo posledic, izgubo informacij je potrebno sanirati, poslovna škoda še sprejemljiva in kratkotrajna).
Majhen	Vpliv na doseganje cilja je majhen ali zanemarljiv (majhen padec kakovosti storitev za stranke, ni neposredne izgube ugleda, majhna finančna izguba, majhne nepravilnosti pri izpolnjevanju zakonskih in pogodbenih določil brez posledic, brez izgube informacij oziroma zanemarljiva izguba, poslovna škoda brez večjega vpliva na poslovanje banke).

Podrobnejše opredelitve ocene verjetnosti in ocene vpliva tveganj so razvidne pri kriterijih za oceno kritičnosti ugotovitev na osnovi preostalega tveganja v poglavju 3.2.1 (tabeli 6 in 7).

Tabela 4: Začetna ocena posameznega tveganja

		Možen vpliv na doseganje ciljev		
		Velik	**Srednji**	**Majhen**
Verjetnost uresničitve tveganja	**Velika**	Visoko	Visoko/srednje*	Srednje
	Srednja	Visoko/srednje*	Srednje	Srednje/nizko*
	Majhna	Srednje	Srednje/nizko*	Nizko

*Oceno določi revizor na podlagi preučitve posameznih dejavnikov.

Tabela 5: Začetna ocena kontrolnega mehanizma

Ocena	Opis
Ustrezna	Kontrolni mehanizmi omogočajo doseganje zastavljenega cilja (ustrezno vzpostavljeni in učinkoviti)
Neustrezna	Kontrolni mehanizmi ne omogočajo doseganje zastavljenega cilja (neustrezno vzpostavljeni ali neučinkoviti)

Ocenjevanje tveganja ter kontrolnih mehanizmov je izvedeno v obliki matrike tveganj, ki je v prilogi 4 tega zaključnega dela. V njej so predstavljeni sledeči elementi:

- COSO sestavine,
- kontrolni cilji,
- tveganja,
- ocena verjetnosti uresničitve tveganja glede na lestvico v skladu z zgoraj opisano metodologijo,
- ocena vpliva tveganja na doseganje zastavljenega cilja glede na lestvico v skladu z zgoraj opisano metodologijo,
- ocena tveganja,
- kontrolni mehanizmi,
- začetna ocena kontrolnega mehanizma, ki temelji na predhodnih postopkih.

Pri vsakem tveganju je naveden tudi kontrolni mehanizem, katerega namen je zaznava ali preprečitev tveganja. Začetna ocena mehanizma je določena na osnovi predhodnih postopkov ter vključuje tako oceno ustreznosti vzpostavitve kot učinkovitosti izvajanja. Vsak kontrolni mehanizem je bil v okviru izvedbe revizijskega pregleda podrobneje pregledan z namenom podaje dejanske ocene delovanja. Revizijski pristopi za preverjanje, ali je tveganje dejansko ustrezno obvladovano, v sami matriki ni navedeno, ker je dokumentirano v obliki delovnih papirjev. V konkretnem primeru notranjerevizijskega posla je bila predhodno ocenjena kot neustrezna samo kontrola glede dokumentiranosti pravil, ker delovno navodilo za upravljanje sistema elektronske pošte ni bilo ažurirano. Kontrole v zvezi z varnostnimi nastavitvami sistemov so bile ocenjene predvsem na podlagi intervjujev, preteklih dogodkov operativnega tveganja, poročil in že izvedenih pregledov. Vse te tehnične kontrole so bile v okviru revizijskega pregleda podrobneje pregledane s strani zunanjega izvajalca, ne glede na začetno oceno. Ta je bila vseeno izvedena tudi zanje predvsem z vidika spoznavanja procesa in konsistentnejšega načrtovanja pregleda.

Mednarodni standard strokovnega ravnanja pri notranjem revidiranju št. 2120 govori o zahtevi, da notranja revizija ovrednoti uspešnost postopkov obvladovanja tveganj in prispeva k njihovemu izboljšanju. V to sodi tudi ocena možnosti prevar ter ravnanje organizacije s tveganjem prevar. Ocenjevanje tveganj je tudi v tem pregledu zajemalo področje prevar, in sicer se je to presojalo predvsem glede vzpostavljenosti etičnega kodeksa, izobraževanj in komuniciranj. Na splošno so se revizijski postopki zasnovali z mislijo, da je potrebno upoštevati tudi možnost prevar.

3.1.4 Revizijski program

Mednarodni standard strokovnega ravnanja pri notranjem revidiranju št. 2240 zahteva pripravo in dokumentiranje programa dela, s katerim se dosežejo cilji posla. Standard nadalje zahteva, da delovni program vključuje postopke za prepoznavanje, proučitev, ovrednotenje in dokumentiranje informacij med potekom posla ter da je delovni program odobren pred izvedbo, vsaka sprememba mora biti prav tako odobrena.
Revizijski program je podrobnejši delovni načrt, kot ga opredeljuje Koletnik (2007, s. 194). Po Turku (2002, s. 648) je to celota podrobno naštetih revizijskih postopkov, potrebnih za uresničitev načrta revizije, za katere revizor meni, da jih je treba izvesti za uresničitev revizijskih ciljev. Revizijski načrt (Turk, 2002, s. 296) pa je posledek načrtovanja revizije, ki ima obliko listine z opredeljenimi potrebnimi revizijskimi nalogami, njihovim zaporedjem in roki za njihovo izvršitev, da bi dosegli cilje posamezne sprejete revizije. V njem se kaže revizijska strategija, na njem pa je zasnovan revizijski program.
Priprava revizijskega programa je odgovornost vodje revizijske skupine. Izhodišče programa so revizijski cilji, zastavljeni obseg ter v predhodnih fazah pripravljene začetne ocene tveganj ter kontrolnih mehanizmov. Na podlagi teh elementov je opredeljen potek revizijskih aktivnosti v sklopu izvedbene faze revizijskega pregleda. Del revizijskega programa so tudi vrste in obsegi postopkov uporabljeni v okviru preiskovanja in vrednotenja, in sodijo v sledeče skupine:

- poizvedovanj – intervjuji,
- opazovanj – spremljanje izvajanja procesov,
- preverjanje in preizkušanje,

- analitični postopki (primerjava in proučevanje ter
- olistinjenje in razvidovanje.

V revizijski program se vključijo vsa tveganja, ki imajo začetno oceno visoko ali srednje ter z njimi povezani kontrolni mehanizmi. Slednji bi bili vključeni v vsakem primeru, če bi se pokazalo, da niso ustrezno vzpostavljeni oziroma, da je izvedba neučinkovita. V pregled so tudi vključene zakonske zahteve ne glede na oceno ter kontrole v zvezi z varnostnimi nastavitvami sistemov, ki jih je pregledoval zunanji izvajalec.

Revizijski program mora potrditi vodja službe notranje revizije. Tu je potrebno poudariti, da se tekom pregleda lahko pokaže potreba po dopolnitvi revizijskega programa, pri čemer je potrebna ponovna potrditev vodje. S pripravo revizijskega programa se dejansko zaključi faza načrtovanje revizijskih aktivnosti. Potrjen revizijski program, ki nato služi za spremljavo izvedbe revizijskih postopkov, se odloži v mapo pod oznako A.07. Revizijski program za konkretni pregled je predstavljen v prilogi 5.

3.2 Izvedba revizijskega pregleda

Faza izvedba revizijskega posla sledi Mednarodnim standardom strokovnega ravnanja pri notranjem revidiranju št. 2300 (Izvajanje posla), 2310 (Prepoznavanje informacij), 2320 (Proučitev in ovrednotenje), 2330 (Dokumentiranje informacij) in 2340 (Nadziranje posla), ki govorijo o tem, da mora notranji revizor:

- prepoznati (zadostne, zanesljive, ustrezne in uporabne informacije),
- proučiti in ovrednotiti (za utemeljitev ugotovitev in izidov posla),
- dokumentirati (prepoznane informacije, ki podpirajo izide posla in ugotovitve)

dovolj informacij za dosego ciljev posla. Pri tem je posle potrebno nadzirati, da se zagotovi doseganje ciljev, kakovosti ter strokovno izpopolnjevanje zaposlenih.

Že v fazi načrtovanja so bile pridobljene osnovne informacije in podlage, kot so na primer dokumenti o organiziranosti, interni akti (pravilniki, delovna navodila), redna poročila, zapisniki organov banke na temo revizijskega pregleda. Dodatne informacije za pripravo revizijskega načrta so bile pridobljene predvsem z intervjuji ter spremljanjem izvajanja procesa oziroma podprocesov. Revizijski program je osnovno vodilo za izvedbo revizijskih aktivnosti in kot tak tudi določa vsebino delovnih papirjev, saj naj bi bil vsak od njih zaokrožena celota za dokumentiranje izvedbe določenega revizijskega postopka. V delovnem papirju so podrobno dokumentirani:

- kdo in kdaj je izvedel določeno revizijsko aktivnost,
- revizijski cilj,
- sodila,
- opis izvedbe revizijske aktivnosti,
- ugotovitve,
- zaključek oziroma sklep,
- dokazil oziroma povezave na dokazila.

Bistveni deli delovnega papirja se prenesejo v revizijski program (referenca na delovni papir, ugotovitev in priporočilo) ter nadalje v revizijsko poročilo (ugotovitve in priporočila).

Proučevanje in ovrednotenje informacij v skladu z Mednarodnim standardom strokovnega ravnanja pri notranjem revidiranju št. 2320 predstavlja podlago za utemeljevanje ugotovitev in rezultatov notranje revizijskih aktivnostih. Te aktivnosti so izvedene z uporabo revizijskih metod:

- poizvedovanja: predvsem intervjuji in delno tudi vprašalniki,
- opazovanja: na primer delovanja sistemov,
- vzorčenja,
- preizkušanja in preverjanja.

Z izvedbo revizijskih aktivnostih se je želelo ugotoviti:

1. ali je sistem notranjih kontrol ustrezno vzpostavljen – z metodologijo COSO,
2. ali so notranje kontrole v predmetnem procesu skladne z zakonodajo in priporočili dobrih praks.

Pri preizkušanju notranjih kontrol pod točko 2 zgoraj, smo ugotavljali, ali so notranje kontrole vzpostavljene za vsa tveganja, ki jih je potrebno obvladovati, torej za tveganja, ki je po odločitvi vodstva kot takšna niso sprejemljiva, ali pa so zahtevana z zakonodajo. Za presojo notranjih kontrol so bila uporabljena izbrana sodila, in sicer poleg zakonodaje še dobre prakse ter upoštevani interni akti. Na podlagi rezultatov primerjanj so bile osnovane ugotovitve.

Preverjanje notranjih kontrol je obsegalo pregled sledečega:
- ustreznost IT strategije,
- obstoj in primernost podlag,
- ustreznost organizacijske strukture,
- primernost upravljanja tveganj,
- vzpostavljenost in ustrezno izvajanje kontrol na področjih določenih v obsegu revizijskega pregleda.

Podrobnosti so razvidne iz revizijskega programa, ki je v prilogi 5.

Vsaka notranja kontrola je bila preverjena glede zasnove in smiselno izvedbe. Pri vsaki ugotovljeni pomanjkljivosti je bilo ocenjeno, ali je pomanjkljivost tako velika, da se na kontrolo ni moč zanašati, kar se je nato odražalo v priporočilih, in sicer tako glede ocene kritičnosti (prioriteta priporočila), kot glede predvidenih ukrepov za odpravo pomanjkljivosti. Pri avtomatskih kontrolah uporaba vzorčenja ni bila smiselna, pri preverjanju kontrol dostopa ter kontrol upravljanja sprememb pa so bili postopki izvedeni na vzorcu, in sicer:
- kontrole dostopa: vzorec je predstavljal 10 odstotkov celotne populacije, vsi privilegirani dostopi ter vse spremembe delovnih mest v zadnjem četrtletju 2020;
- kontrole upravljanja sprememb: vzorec je predstavljal 10 odstotkov vseh sprememb v letu 2020.

Revizijski postopki so bili izvedeni v skladu z revizijskih načrtom, ki tekom izvedbe pregleda ni bil dopolnjen ali spremenjen, saj ni bilo potrebe. Z zunanjim izvajalcem, ki je izvedel tehnični del pregleda, je bilo pogodbeno dogovorjen obseg pregleda, nabor orodij (NESSUS z izbranimi viri (feed-i), NMAP, Metasploit Framework) ter metodologija in dobre prakse, ki jih je moral upoštevati (OSSTMM, OWASP ter MITRE ATT&CK). Okvir MITRE ATT&CK v kombinaciji z OWASP je bil podlaga za preveritev skladnosti vzpostavljenih kontrol v banki s predlaganimi v okviru uporabljene dobre prakse za področje varnostnega preverjanja sistemov s strani zunanjega izvajalca, vključno z vdornim testom, torej je v tem primeru zelo pomemben z vsebinskega vidika, zato bo uporaba tudi nekoliko podrobneje predstavljena v nadaljevanju.

Osnove okvira MITRE ATT&CK so opisane v poglavju 2.4.1 Dobre prakse. Za potrebe ustrezne predstavitve uporabe je tu potrebno dodati še razdelitev na taktike, tehnike in postopke, kot jih opredeljuje okvir, in sicer:
- taktike: predstavljajo cilje, ki jih napadalci želijo doseči;
- tehnike: predstavljajo različne načine, s katerimi želijo napadalci doseči cilje;
- postopki: predstavljajo korake, ki jih napadalec uporabi za izvedbo tehnike ali niza tehnik.

Predstavljen bo primer preveritve kontrol v zvezi z odtekanjem podatkov (eksfiltracijo podatkov), ki je v danih razmerah in za okolje bančništva zelo aktualna. Taktika po MITRE ATT&CK strukturi je v tem primeru kraja podatkov. S to taktiko je povezanih v okolju za organizacije (mobilno okolje ni bilo predmet pregleda, saj mobilno poslovanje v času pregleda ni bilo na voljo) devet tehnik, ki so:
- T1020: avtomatski prenos (eksfiltracija) (npr. podvojitev prometa),
- T1030: omejen prenos podatkov (prenos v manjših paketih za zmanjšanje možnosti zaznave)
- T1048: prenos prek alternativnih protokolov (na primer DNS),
- T1041: eksfiltracija prek kanalov za nadzor,
- T1011: prenos prek drugih omrežjih (na primer brezžičnega omrežja),
- T1052: prenos prek fizičnih medijev,
- T1567: prenos prek spletnih storitev,
- T1029: prenos po urniku (da se lažje prekrije odtekanje podatkov),
- T1537: prenos v oblačne storitve.

Za bolj podrobno predstavitev je izbrana tehnika prenosa prek alternativnih protokolov (T1048) z uporabo postopkov v povezavi z DNS protokolom v skladu z opisom v MITRE ATT&CK okviru. V ta namen je bila v omrežje banke zunanjemu izvajalcu omogočena povezava računalnika, na katerem so bile prek PowerShell vrstice (ukazne vrstice) izvedene DNS poizvedbe vključujoč domeno, ki je bila pod nadzorom izvajalca. Zahtevki so potovali prek DNS infrastrukture do strežnika izvajalca pod prej omenjeno domeno, ki je bil predviden za zajem prometa. Povezovanje je bilo načrtovano prek izbranih transportnih vrat. To početje je zaznal SIEM, ki je opozoril na varnostni dogodek. Vendar je to zaznavalna kontrola, ki bi bila odvisna od hitrosti odziva odgovornih zaposlenih. Dogajanje je zaznal tudi varnostni sistem ATP (Advance Threat Protection), ki je povezovanje zaustavil in zahteval potrditev varnostne izjeme. Ta aktivnost je pomenila, da je varnostna kontrola za izvedeni korak ustrezno vzpostavljena in se tudi učinkovito izvaja, kar je v skladu s primerov dobre prakse MITRE ATT&CK. Rezultat pregleda je bil označen v matriki, ki omogoča hiter pregled stanja informacijske varnosti na podlagi opravljenih postopkov (primer je prikazan v poglavju 2.4.1 pod opisom okvira MITRE ATT&CK).

Tekom celotne izvedbe revizijskih postopkov preverjanja notranjih kontrol so bile ugotovljene pomanjkljivosti, ki so opisane v naslednjem poglavju.

Kot že omenjeno, se bili postopki ter ugotovitve dokumentirano v delovnih papirjih. Primer delovnega papirja je v prilogi 7.

3.2.1 Ugotovitve in priporočila notranje revizije

Postopki identifikacije, ovrednotenja ter klasifikacija ugotovitve glede na resnost so v metodologiji banke zasnovani s ciljem, da:

- revizor pridobi zadostno razumevanje pomanjkljivosti,
- se izboljša kontrolno okolje banke s poudarkom na zasnovi in delovanju notranjih kontrol,
- povezava ugotovljenih pomanjkljivosti kontrol v procesu z potencialnim vplivom tveganja,
- glede na dane možnosti čim natančneje opredeliti finančne in druge posledice.

V osnovi se vsaka ugotovitev navezuje na pomanjkljivost notranjih kontrol, ko zasnova ali izvedba notranje kontrole nista ustrezna, da bi lahko ustrezno naslavljala povezan učinek tveganja.

Pri vsaki ugotovitvi je potrebno opredeliti naslednje atribute:

- sodilo (želeno stanje),
- stanje (dejansko obstoječe stanje),
- vzrok za pomanjkljivost in
- učinek (vpliv tveganja).

Za vsako pomanjkljivost je potrebno odkriti temeljne vzroke za takšno stanje, kar se običajno doseže s tehniko ponavljanja vprašanja zakaj. Na primeru ugotovitve glede uspešnosti napada ribarjenja (phising napada), priporočilo RP-2021-03-04, ki je tudi navedeno v notranjerevizijskem poročilu v prilogi 8, je postopek sledeč:

- Zakaj 1: Zakaj je bil napad uspešen?
    - Ker zaposleni niso prepoznali lažnega sporočila.
- Zakaj 2: Zakaj zaposleni niso prepoznali lažnega sporočila?
    - Ker niso osveščeni o znakih lažnih sporočil.
- Zakaj 3: Zakaj kljub izobraževanju zaposleni niso osveščeni o znakih lažnih sporočil?
    - Ker niso posvetili dovolj pozornosti izobraževanju ali je bilo izobraževanje izvedeno že predolgo nazaj in so zaposleni pozabili pridobljene informacije.

Zgornji primer je dokaj enostaven, bolj kompleksni lahko zahtevajo precej vloženega truda, da se najde res pravi temeljni vzrok. Vendar je pomembno, da se najde pravi vzrok in s tem lažje določi ustrezen ukrep za odpravo, saj se tako možnost ponovitve pomanjkljivosti bistveno zmanjša.

Z namenom odprave temeljnih vzrokov, popravka izjem ter naslavljanja ugotovitve na način, da obvladuje povezano tveganje, notranji revizor poda revizijsko priporočilo. Slednje je tudi izhodišče za

vodje odgovornih organizacijskih enot, da pripravijo akcijske načrte. Oblika ugotovitve, kot je predstavljena v revizijskem poročilu, sestoji iz treh glavnih delov:

- ugotovitev,
- vzrok in učinek (vpliv tveganja),
- priporočilo.

Vsi trije deli se morajo celoviti dopolnjevati, naslavljati morajo vse že omenjene atribute (sodilo, stanje, vzrok, učinek), raven obravnave vsakega od njih je tudi odvisna od resnosti ugotovitve. V primeru, da je nekaj izpuščeno iz predstavitve, se poveča možnost, da so tudi aktivnosti za odpravo pomanjkljivosti nepopolne oziroma, da vodstvo ne razume ustrezno tveganja in morebiti tudi oporeka ugotovitvi. Pomembno je tudi, še posebno za kritične pomanjkljivosti, da so čim prej komunicirane odgovornim in s tem omogoči njihovo zgodnjo odpravo, hkrati pa zviša transparentnost revizijskega dela ter tudi nivo sodelovanja z revidiranci.

V zvezi z ugotovitvijo in priporočilo je pomembno tudi razlikovanje med nosilcem tveganja ter odgovornim za izvedbo ukrepa. Nosilec tveganja je organizacijska enota odgovorna za obvladovanje tveganj, ki so bila izpostavljena s strani notranjih revizorjev. Običajno je to revidirana enota. Odgovorni za izvedbo mora izvesti akcijski načrt, ki vodi k odpravi ugotovljene pomanjkljivosti. Pri njihovem imenovanju ima pomembno vlogo tudi enota, ki je nosilec tveganja, in sicer tekom priprave akcijskega načrta. Pogosto sta nosilec tveganja in odgovorni za izvedbo ista organizacijska enota.

Ena od pomembnih informacij, ki se navezujejo na ugotovitve, je ocene njihove kritičnosti, ki določajo prioriteto izvedbe ukrepov za odpravo. S tem namenom se za vsako ugotovitev najprej izvede ocenjevanje preostalega tveganja, ki sestoji:

- iz ocene verjetnosti nastanka dogodka,
- ocena vpliva na poslovanje.

Posamezni komponenti sta ocenjeni na podlagi kriterijev iz metodologije dela notranja revizije, in sicer s tristopenjskima lestvicama, ocena preostalega tveganja je kombinacija verjetnostni nastanka dogodke ter vpliva na poslovanje in je predstavljena prav tako s tristopenjsko lestvico, od visokega do nizkega.

Tabela 6: Verjetnost nastanka dogodka

Ocena	Opis	Kriteriji	Pogostost pojava
Velika	Tovrstni dogodki so se zgodili v preteklem letu ali se pogosto dogajajo.	- Dogodek se je zgodil pred kratkim v revidiranem področju ali v podobnih sistemih, enotah ali bankah; - Dogodek ima velik potencial za nastanek;	Enkrat letno ali pogosteje
Srednja	Tak dogodek se je že zgodil v banki ali podobni instituciji v branži oziroma se dogajajo občasno.	- Dogodek se pred kratkim ni zgodil, vendar se je že pojavil v preteklosti, na primer v podobnih institucijah; - Upravičeno lahko domnevamo, da se bo dogodek zgodil v prihodnjh treh letih;	Enkrat na tri leta
Majhna	Takšni dogodki se občasno zgodijo; verjetnost, da bo dogodek nastal vsako leto ali pogosteje je majhna	- Dogodek še ni nastal, - Obstaja velika verjetnost, da dogodek ne bo nastal v prihodnjih petih letih; - Verjetnost, da se bo dogodek pojavil kadarkoli v prihodnost je majhna	Enkrat na deset let

Tabela 7: Vpliv dogodka na poslovanje

Vrsta škode / stopnja	Nizek	Srednji	Visok
Vpliv na storitve za stranke	Ni učinka na kakovost storitev za komitente oziroma je padec kakovosti majhen, predvsem zaradi manjših nevšečnosti. Posledice večinoma niso vidne komitentom.	Kakovost storitev se močno zmanjša zaradi potrebe po drugačnem načinu dela (na primer prehod na ročni način dela). Padec kakovosti ni zanemarljiv, vendar lahko banka na kratki rok še vedno posluje v sprejemljivih okvirih.	Pride do prekinitve storitev v tolikšnem obsegu, da je banka v tem pogledu nezmožna normalno poslovati.
Izguba ugleda	Dogodek ne povzroči neposredne izgube ugleda. Medijske izpostavljenosti ni oziroma gre le za posamične omembe. Ni potreben dodaten napor pri stikih z javnostmi.	Izguba ugleda je možna, vendar naj ne bi imela velikega vpliva na delovanje. Opazna, a kratkotrajna medijska izpostavljenost,na primer omemba incidenta v medijih. Škodo je potrebno z ustreznimi stiki z javnostmi aktivno zmanjševati.	Izguba ugleda je lahko ogromna in resno lahko ogrozi delovanje banke. Pride do dalj časa trajajoče negativne medijske izpostavljenosti. Potrebna je obširnejša akcija stikov z javnostmi, ugled banke je močno načet.
Tveganje finančnih izgub (merila so v pravilniku za obravnavo dogodkov operativnega tveganja)	Izguba je majhna.	Vpliv na operativno delovanje banke ni zanemarljiv, pride do opazne izgube dohodka.	Pride do znatne, nepričakovane izgube.
Nespoštovanje zakonskih in pogodbenih obveznosti	Manjše nepravilnosti pri izpolnjevanju zakonskih in pogodbenih obveznosti. Majha verjetnost kazni in odškodninskih tožb.	Obstaja jasna kršitev zakonskih obveznosti. Srednja verjetnost kazni in odškodninskih tožb.	Hujša kršitev obveznosti, kjer obstaja visoka verjetnost sankcij in odškodninskih tožb z znatnimi finančnimi posledicami.
Izguba ključnih informacij	Ne pride do izgube informacij oziroma v tako majhnem obsegu, da je izgubo informacij mogoče brez večjega napora odpraviti.	Izguba informacij je opazna in ima neposreden vpliv na poslovanje banke. Kljub temu je mogoče z dodatnim delom stanje normalizirati v kratkem času.	Izguba informacij je za banko katastrofalna in ji onemogoča normalno poslovanje. Posledično visoki stroški. Hude kršitve zaupnosti, uničenje ali korupcija pri kritičnih informacijah, notranje ali zunanje razkritje oziroma

Vrsta škode / stopnja	Nizek	Srednji	Visok
			uporaba nezanesljivih, pristranskih ali nepravilnih informacij, ki imajo posledično velik vpliv na banko, stranke ali javno mnenje.
Drugo	Druga poslovna škoda, ki nima večjega vpliva na poslovanje banke.	Poslovna škoda, ki sicer vpliva na poslovanje banke, vendar je finančni učinek še sprejemljiv in kratkotrajen.	Vpliv na poslovanje in s tem povezanimi stroški je znaten, posledice so lahko dolgotrajne.

Tabela 8: Določitev stopnje preostalega tveganja

		Možen vpliv na doseganje ciljev		
		Velik	**Srednji**	**Majhen**
Verjetnost uresničitve tveganja	**Velika**	Visoko	Srednje ali visoko	Srednje
	Srednja	Srednje ali visoko	Srednje	Srednje ali nizko
	Majhna	Srednje	Srednje nizko	Nizko

V odvisnosti od posamezne situacije v banki ter glede na strokovno presojo revizorja, je končna raven tveganja, še posebej v primerih mejnih ocen preostalega tveganja (visoko ali srednje oziroma nizko ali srednje tveganje), lahko določena ali preverjena s pomočjo dopolnilnih pojasnjevalnih smernic, ki so predstavljene v spodnji tabeli.

Tabela 9: pojasnjevalne smernice za določanje končne ravni preostalega tveganja

RAVEN TVEGANJA	SPLOŠNE DEFINICIJE
VISOKO	- Skupna ocena upravljanja organizacije, upravljanja s tveganji in notranjih kontrol je nezadovoljiva ali pomanjkljiva: - velike pomanjkljivosti pri ustreznosti in/ali učinkovitosti upravljanja s tveganji in/ali notranjih kontrol, ki lahko resno ogrozijo bistvene interese banke; - visoka stopnja hudih pomanjkljivosti (neusklajenost s predpisi, popolno pomanjkanje kontrol), ki zahtevajo celovito reorganizacijo poslovnega področja/procesa/produkta/organizacijske enote. Vodstvo ne smatra, da je potrebno vpeljati kakršnekoli formalne zapisane politike in postopke za izvajanje nadzora. Nadzor nad postopki ni vzpostavljen in se ne izvaja; - velike pomanjkljivosti v varnostnem sistemu (v primeru zaupnosti, integritete, dosegljivosti in/ali logičnem in fizičnem dostopu); - pomanjkljivosti, ki so bile prvotno opredeljene kot "srednje tveganje", vendar so bile nadgrajene v "visoko tveganje" zaradi ponovnega nastopa in/ali nezadovoljivega ukrepanja glede na potrjen načrt; - zahtevano je takojšnje ukrepanje za zmanjšanje tveganja.

SREDNJE	- Ocena upravljanja organizacije, upravljanja s tveganji in notranjih kontrol je pomanjkljiva ali primerna: - pomanjkljivosti pri ustreznosti in/ali učinkovitosti upravljanja s tveganji in/ali notranjih kontrol, ki lahko ogrozijo bistvene interese banke. Nadzor se ne izvaja skladno z formalno dokumentiranimi internimi pravili in je prepuščen posameznikom; - politike/pravilniki niso podrobneje opredeljeni, postopki se izvajajo skladno s splošnimi pravili, velikokrat po ustnih navodilih; - pomanjkljivosti, ki so bile prvotno opredeljene kot "nizko tveganje", vendar so bile nadgrajene v "srednje tveganje" zaradi ponovnega nastopa in/ali nezadovoljivega ukrepanja glede na potrjen načrt; - ukrepanje mora biti brez zamud z namenom zmanjšanja tveganja.
NIZKO	- Ocena upravljanja organizacije, upravljanja s tveganji in notranjih kontrol je primerna, dobra ali zelo dobra: - posamezne pomanjkljivosti pri primernosti in/ali učinkovitosti upravljanja s tveganji in/ali notranjih kontrolah, ki lahko ogrozijo splošne interese banke; - kombinacija nekaterih pomanjkljivosti v kontrolnem sistemu, ki zahtevajo čimprejšnje korekcije s strani vodstva poslovnega področja/organizacijske enote. Vodstvo se zaveda potrebnosti spremljave in nadzora, vendar se le-ta izvaja neredno skladno s formalno zapisanimi postopki; - postopki, politike in razmejitev odgovornosti so okvirno opredeljene; - predlogi za izboljšave; - zahteva ukrepanje v razumnem roku z namenom zmanjšanja tveganja.

Z odvisnostjo od preostalega tveganje ugotovitve se določi prioriteta priporočila na lestvici od 1 do 3, pri čemer je 1 najbolj kritična. Od prioritete priporočila je odvisna tudi izhodiščna dolžina obdobja, v katerem je pričakovana izpeljava popravljalnih ukrepov, vendar se dolžina obdobja lahko ob ustrezni argumentaciji prilagodi okoliščinam. Povezanost ocenjenega preostalega tveganja, prioritete priporočila ter izhodiščna dolžina obdobja za izvedbo popravljalnih ukrepov je prikazana v spodnji tabeli.

Tabela 10: Povezava ocenjenega preostalega tveganja, prioritete priporočila ter izhodiščna dolžina obdobja za izvedbo popravljalnih ukrepov

Ocenjeno preostalo tveganje	Prioriteta priporočila	Izhodiščna dolžina obdobja
Visoko	1	1 mesec
Srednje	2	4 meseci
Nizko	3	9 mesecev

Revizijska ekipa mora stalno vzdrževati komunikacijo z revidiranci, saj imajo od tega korist oboji. Revizorji so tako bolje obveščeni o dogajanju na revidiranem področju, revidiranci pa lahko hitreje in učinkoviteje odpravljajo ugotovljene pomanjkljivosti. V primeru ugotovljenih kritičnih oziroma kompleksnih ugotovitev je potrebno organizirati usklajevalni sestanek, kjer so podrobneje predstavljene in potrjene ugotovitve, preverjeni izsledki glede vzrokov ter tudi dogovorjeni ukrepi za odpravo pomanjkljivosti.

Tekom pregleda so bile ugotovljene štiri pomanjkljivosti, ki so povzete spodaj. Podrobnosti so razvidne iz revizijskega poročila, ki je v prilogi 8.

- Komunikacija med aplikacijo za vodenjem osnovnih sredstev in povezanim sistemom za upravljanje zbirk podatkov na osnovi ranljivega protokola, prioritete 3.
- Interno razvita aplikacija za vodenje šifrantov (za interno uporabo) razkriva podatke o zaledni infrastrukturi, prioritete 3.
- Interno razvita aplikacija za vodenje šifrantov uporablja splošni neustrezen certifikat, prioritete 3.
- Uspešna simulacija napada ribarjenja (phising napada) zaradi prenizke osveščenosti zaposlenih, prioritete 2.

3.3 Poročanje o ugotovitvah notranje revizijskega posla

3.3.1 Osnutek poročila

Po zaključku dela na t.i. terenu začnejo revizorji s pripravo osnutka poročila. Slednji je v osnovi po obliki dokaj podoben končnemu poročilu, vendar mora biti jasno označen, da gre za osnutek, in sicer tako v imenu kot z vodnim žigom na vsaki strani. Praviloma se osnutek poročila, ki ga potrdi vodja notranje revizije, pošlje revidirancem vsaj pet delovnih dni pred zaključnim sestankom ter se zaprosi za povratno informacijo glede strinjanja z zapisanim, ki naj bi se tudi prejela pred omenjenim sestankom. Načeloma, če je komunikacija potekala tekom revizijskih postopkov, kot je predvideno, se običajno ne pričakuje novih bistvenih pripomb. Revidirance se zaprosi tudi za pripravo akcijskega načrta v zvezi z odpravo ugotovljenih pomanjkljivosti, ki bo vključen v končno poročilo.

3.3.2 Zaključni sestanek

Zaključni sestanek je sklican z vodji revidiranih enot ter predstavniki ostalih organizacijskih enot, ki bi jih revizijske ugotovitve morebiti zadevale. Na sestanku je predstavljen potek notranjerevizijskega pregleda, končne ugotovitve, ki pa se lahko ob tehtni argumentaciji še spremenijo, saj mogoče v določenih primerih vodstvo ni bilo v zadostni meri vključeno v aktivnosti tekom izvedbe revizije, običajno zaradi njihove zasedenosti, in se lahko šele sedaj podajo nekatera pojasnila, čeprav naj to ne bi bilo praksa. Potencialne spremembe so sicer običajno že nakazane v komentarjih v osnutku poročila.
V konkretnem primeru pregleda so bili na zaključni sestanek vabljeni vodja informacijske varnosti, vodja informatike ter vodja splošnih služb. Na vodje informatike je bil prisoten tudi vodja sistemskih administratorjev. Bistven del sestanka se je nanašal na dogovor glede podrobnosti v zvezi z izvedbo akcijskega načrta za odpravo ugotovljenih pomanjkljivosti.
Za izvedeni zaključni sestanek je bil pripravljen tudi zapisnik, ki je bil poslan v usklajevanje vsem prisotnim. Končni dokument je bil shranjen kot del revizijske dokumentacije v mapo C.02.

3.3.3 Končno poročilo in predstavitev upravi

Ker v konkretnem primeru pregleda tako niti tekom usklajevanja osnutka revizijskega poročila niti na zaključnem sestanku niso bili prejeti komentarji revidirancev, ki bi zahtevali pomembno spremembo revizijskega poročila, je odgovorni notranji revizor takoj po potrjenem zapisniku zaključnega sestanka pričel s pripravo končnega poročila, ki sestoji iz:

- glavnih podatkov na prvi strani v zvezi z vrsto pregleda (redni ali izredni), skupno oceno notranjerevizijskega pregleda ter povzetkom glavnih ugotovitev, ki podpirajo skupno oceno, datumom poročila, prejemniki poročila;
- navedbe, da je bil pregled je izveden skladno z Mednarodnimi standardi strokovnega ravnanja pri notranjem revidiranju ter da zasnova revizijskega pregleda temelji na COSO okviru notranjih kontrol;
- povzetka za vodstvo, ki obsega predstavitev cilja in obsega posla, kratke predstavitve področja in ocene podpodročij z utemeljitvami ocen;

- ugotovitev in priporočil, ki so podrobneje opisana na predlogah, iz katerih so jasno razvidne ugotovitve, vzroki in vplivi, priporočilo ter akcijski načrt za odpravo pomanjkljivosti;
- drugih informacij, ki se navezujejo na pojasnila glede postopkov usklajevanj ter splošni sklic na delovne papirje, iz katerih so razvidne podrobnosti opravljenih revizijskih postopkov, ter porabljeni čas za pregled.

V konkretnem primeru je bilo področje pregleda ocenjeno kot primerno, saj so rezultati pregleda pokazali manjše število pomanjkljivosti na področju (da komunikacija med aplikacijo za vodenjem osnovnih sredstev in povezanim sistemom za upravljanje zbirk podatkov na osnovi ranljivega protokola; da interno razvita aplikacija za vodenje šifrantov razkriva podatke o zaledni infrastrukturi; da interno razvita aplikacija za vodenje šifrantov uporablja neustrezen; da je bil test napada z ribarjenjem (phising napad) uspešen zaradi prenizke osveščenosti zaposlenih). Pri tem je potrebno pojasniti, da se aplikacije iz prvih treh točk uporabljalo le v notranjem omrežju, ki je dobro zaščiteno. Iz tega izhaja, da je tveganja za banko manjše. Pri četrti ugotovitvi, ki se nanaša na napad z ribarjenjem, je bilo potrebno izključiti avtomatske kontrole varnostnega sistema banke, ki preprečujejo dostavo elektronske pošte s sumljivo vsebino zaposlenim, saj se je e-pošta sicer najprej preusmerila v t.i. karanteno, iz katere jo je potrebno ročno sprostiti. Zaradi četrte pomanjkljivosti je bila dodeljena ocena lahko primerno in ne boljša, saj je človeški faktor po zadnjih podatkih eden glavnih faktorjev pri uspešnih kibernetskih napadih, zato je potrebna izvedba učinkovitih popravnih ukrepov. Kljub temu obstajajo, kot je opisano zgoraj, tudi nadomestne kontrole, ki preprečujejo, da bi bila banka izpostavljena prekomernemu tveganju.

Štiristopenjska lestvica ocen pregledov, ki je tudi del notranjerevizijskega poročila, je sicer sledeča:
- Dobro: Skupna ocena sistema notranjih kontrol za revidiran proces/področje/enoto je na splošno dobra. Ugotovitve kažejo samo na majhne pomanjkljivosti ali jih sploh ni. Priporočil ni oziroma jih je malo in so nizke prioritete.
- Primerno: Skupna ocena sistema notranjih kontrol za revidiran proces/področje/enoto kaže zadostno mitigiranje tveganj. Ugotovitve kažejo manjše pomanjkljivosti, ki se jih lahko odpravi tekom običajnih poslovnih aktivnosti. Dana so priporočila nižje prioritete.
- Pomanjkljivo: Skupna ocena sistema notranjih kontrol za revidiran proces/področje/enoto kaže nezadostno mitigiranje tveganj. Ugotovitve kažejo pomanjkljivosti, ki jih je potrebno odpraviti tekom implementacije priporočil, ki zahtevo stalno spremljavo.
- Nezadovoljivo: Skupna ocena sistema notranjih kontrol za revidiran proces/področje/enoto kaže nezadostno mitigiranje tveganj. Ugotovitve kažejo pomembne pomanjkljivosti, ki jih je potrebno nemudoma odpraviti, da se tveganje zmanjša na sprejemljivo stopnjo.

Zunanji izvajalec je sicer pripravil svoje poročilo, ki je bilo zelo tehnične narave. Zato so bile vse njegove ugotovitve povzete v poročilu, ki ga je pripravila služba notranje revizije in ki temelji na predlogi, katere uporabe je predpisana z internim aktom.

Končna verzija poročila je predstavljena na seji uprave. Pri tem bi uprava lahko tudi sprejela tveganje, ki bi izhajalo iz določene pomanjkljivosti, in hkrati sklenila, da se določeno priporočilo ne izvede. Po omenjeni predstavitvi se poročilo prek dokumentnega sistema pošlje upravi in revidirancem, v tem primeru:
- vodji informacijske varnosti,
- vodji informatike ter
- vodji splošnih služb.

Končno poročilo mora biti predhodno potrjeno s strani vodje notranje revizije in je bilo odloženo v mapo C.04. Povzetki poročil ter pomembne ugotovitve se poročajo tudi v kvartalnih oziroma letnih poročilih revizijski komisiji ter nadzornemu svetu.
Primer notranjerevizijskega poročila je v prilogi 8.

3.4 Razvidovanje in arhiviranje

Kot določa Mednarodni standard strokovnega ravnanja pri notranjem revidiranju številka 2330 morajo notranji revizorji dokumentirati zadostne, zanesljive, ustrezne in koristne informacije, ki podpirajo izide posla in ugotovitve. Pravilnik notranje revizije v banki sledi temu in zahteva pripravo in hrambo revizijske dokumentacije, ki dokazuje ustrezno izvedbo revizijskih aktivnosti in še zlasti dokumentacijo v zvezi z ugotovljenimi pomanjkljivostmi in podlage za oblikovanje zaključkov ter ocene. Hramba dokumentacije je določena z drugim pravilnikom, ki ureja to področje celoviti za celo banko, in sicer tako glede načina kot obdobij hrambe, pri čemer se:

- revizijski načrt in revizijsko poročilo hranijo stalno,
- ostala dokumentacija se hrani za obdobje 10 let v dokumentnem sistemu.

Elektronska dokumentacija, ki obsega veliko večino vseh dokumentov, je sicer zaradi načina arhiviranja, trenutno hranjena za stalno. Pomembna je tudi klasifikacija, torej razvrščanje dokumentov v skupine oziroma mape, zato je temu potrebno posvetiti ustrezno pozornost.

Služba notranje revizije pri svojem delu uporablja elektronski dokumentni sistem banke, ki omogoča vodenje dokumentacije v skladu s pravili za arhivsko gradivo v banki, arhiviranje ter vodenje revizijskih sledi glede manipulacije z dokumenti ter zelo natančno opredeljene dostope do njih. V primeru, da je revizijska dokumentacija v papirni obliki ter je ni mogoče digitalizirati, se odloži v posebne mape, v elektronski evidenci pa se kreira sklic nanjo.
Revizijska mapa je v grobem sestavljane iz petih delov, in sicer:

- načrtovanje,
- izvedba,
- poročanje
- nadziranje posla in kvaliteta ter
- spremljava priporočil.

Zadnji, peti del vsebuje samo povezavo na drugo aplikacijo, ki je namenjena spremljavi priporočil in je predstavljena v poglavju 3.6. Konkretni primer strukture revizijske mape za obravnavani revizijski pregled je predstavljena v spodnji tabeli.

Tabela 11: Struktura revizijske mape

Oznaka	Opis
A NAČRTOVANJE	
A.01	Potrditev začetka revizije z opredelitvijo ciljev in obsega
A.02	Najava
A.03	Uvodni sestanek
A.04	Memorandum o načrtovanju
A.05	Podlage (predpisi, dobre prakse, organigrami, predhodni revizijski pregledi, poročila…)
A.06	Začetna ocena tveganj in kontrol
A.07	Revizijski načrt in matrika
B IZVEDBA	
B.xx	Zapisniki sestankov Strategija, upravljanje, organiziranost Upravljanje tveganj Zunanje varnostno preverjanje storitev Varnostni pregled požarne pregrade Pregled sistemov za informacijsko zaščito Notranji varnostni pregled kritičnih aplikacij in sistemov Socialni inženiring Poročanje Nadzor

C POROČANJE	
C.01	Osnutek poročila
C.02	Zaključni sestanek
C.03	Predstavitev upravi
C.04	Končno poročilo
D NADZIRANJE POSLA IN KVALITETA	
D.01	Nadziranje posla
D.02	Kvaliteta posla
E SPREMLJAVA PRIPOROČIL	
E.01	Spremljava priporočil
F ZUNANJI IZVAJALEC	
F.01	Povpraševanje, ponudba, dogovor
F.02	Komunikacija
F.03	Poročilo
F.04	Spremljava

Elektronski dokumenti sistem olajša delo, saj z vgrajenimi kontrolami zagotavlja sledeče:

- status posla se ne more spremeniti v zaključen, če niso odloženi dokumenti, ki so vnaprej označeni kot nujni;
- status posla se ne more spremeniti v zaključen, če vsi relevantni dokumenti (glavni dokument v vsaki mapi) niso podpisan s strani pripravljalca ter nadzornika;
- dokumenti se lahko kreirajo iz predloge;
- oznake dokumentov so določene že vnaprej.

Kot že izhaja iz zgoraj omenjene kontrole v zvezi s podpisi, morajo biti vsi dokumenti tudi potrjeni tako s strani pripravljalca kot nadzornega, ki je vodja službe notranje revizije ali z njegove strani imenovan drugi zaposleni. Obvezni elementi posameznih dokumentov so tudi ustrezne oznake in opisi ter datumi izvedbe.

3.5 Nadzor nad izvedbo notranje revizijskega posla in kvaliteta izvedbe

V skladu z Mednarodnim standardom strokovnega ravnanja pri notranjem revidiranju številka 2340 je revizijski posel stalno nadziran z namenom zagotovitve, da so cilji doseženi, da je zagotovljena kakovost ter da se zaposleni strokovno izpopolnjujejo. Nadzor vrši vodja notranje revizije oziroma tudi druga neodvisna, posebej imenovana oseba zaposlena v službi notranje revizije. Glede na to, da je število zaposlenih v službi majhno, je del nadzora tudi v neformalni obliki, poleg tega je vodja po možnosti prisoten na pomembnejših sestankih. Vodja mora tudi potrditi (digitalno podpisati) relevantne (krovne) dokumente odložene v dokumentnem sistemu. Pomembno je tudi sprotno izpolnjevanje oziroma dopolnjevanje dokumentov z ustreznimi informacijami, saj vodja tako sledi napredku revizijskega posla.

Ob zaključku posla se kvaliteta posla ocenjuje tudi prek:

- ankete, ki jo izpolnijo revidiranci;
- kontrolnega lista za zagotavljanja kakovosti posameznih revizijskih pregledov.

Anketa se pošlje hkrati s končnim revizijskim poročilom in sloni na petstopenjski lestvici ocenjevanja posameznih delov izvedbe, med katerimi so:

- komunikacija,
- revizorjevo poznavanje področja,
- obremenitev revidirancev s pregledom,
- ocena ustreznosti ciljev in obsega,
- ugotovitve in zaključki,

- poročanje,
- ocena neodvisnosti in nepristranskosti,
- dodana vrednost pregleda.

Kontrolni list pa je namenjen preveritvi:
- upoštevanja vseh pomembnih tveganj,
- doslednosti uporabe predlog,
- konsistentni izvedbi nadzora tekom pregleda,
- doslednosti pri izvedbi korakov, na primer glede izpolnjevanja revizijskega načrta ali ovrednotenja kontrol,
- celovitosti dokumentacije,
- pravočasnega in celovitega dokumentiranja in arhiviranja,
- obsega porabljenega časa.

3.6 Spremljava izvajanja priporočil

Takoj po zaključku revizijskega pregleda, torej po pošiljanju končnega poročila, se priporočila vnesejo v posebno aplikacijo za njihovo spremljavo, ki podpira zagotavljanje skladnosti z Mednarodnim standardom strokovnega ravnanja pri notranjem revidiranju številka 2500 glede spremljanja napredovanja ukrepov za odpravo pomanjkljivosti. V omenjeno aplikacijo se vnesejo ugotovitve, priporočila in akcijski načrt z osebami, zadolženimi za izvedbo, izvedbeni roki ter tudi prioritete priporočil. Vsa formalna komunikacija glede izpolnjevanja priporočil se vodi prek te aplikacije. Vanjo odgovorne osebe vpisujejo pojasnila, posredujejo dokaze ter predlagajo spremembe statusov, ki jih mora potrditi odgovorni notranji revizor, za priporočila najvišje prioritete pa tudi vodja notranje revizije. Roki za izvedbo priporočil se v izjemnih primerih lahko tudi podaljšajo, in sicer s predhodno pridobitvijo mnenja službe notranje revizije ter potrditvijo uprave. Obdobje in število podaljšav je omejeno, in sicer je pogojeno tudi s prioriteto priporočila.

Možni statusi priporočil so štirje;
- odprto: priporočilo še ni bilo izvedeno, vendar tudi še ni zapadlo;
- v delu: priporočilo še ni zapadlo, vseeno je vsaj v pomembnem delu že realizirano;
- zapadlo: priporočilo je že zapadlo in še ni realizirano oziroma je realizirani del zanemarljiv;
- zaprto: priporočilo je že realizirano.

Sicer je možen tudi status, da je tveganje sprejeto ter se priporočilo ne izvede, za kar je potrebna odločitev uprave, vendar se v tem primeru in tudi na splošno ta status skoraj ni uporabljen.

Priporočila se spremljajo najmanj kvartalno, ko se tudi pripravlja poročilo za upravo, revizijsko komisijo ter nadzorni svet. Odgovorni zaposleni so sicer vzpodbujeni, da sproti vnašajo informacije glede izvedbe priporočil. Vsak kvartal ter tudi štirinajst dni pred iztekom roka posameznega priporočila za izvedbo odgovorne osebe prejmejo avtomatsko obvestilo. Aplikacija prav tako pošlje obvestilo odgovornim osebam ter odgovornim notranjim revizorjem ob vsakem vnosu v aplikacijo ali spremembi statusa priporočil.

SKLEP

Z izvedenim pregledom je upoštevajo opise postopkov ter dokumentiranih in poročanih rezultatov služba notranje revizije uspešno dokončala posel, na podlagi katerega lahko poslovodstvu poda ustrezno zagotovilo glede skladnosti s predpisi ter dobrimi praksami na področju kibernetske varnosti. S tem je notranja revizija izpolnila pričakovanja vodstva ter prispevala svoj del k ustrezni ureditvi tega področja informacijske varnosti, ki postaja vedno bolj pomembno, njegovo preverjanje pa zaradi naraščajočega obsega spletnega poslovanja in razvoja orodij vedno bolj kompleksno. Čeprav ni bilo kritičnih ugotovitev in posledično priporočil visokih prioritet, je takšen revizijski pregled v trenutnih okoliščinah koristen in običajno pri poslovodstvu dobro sprejet, saj daje potrditev, da so vlaganja, ki predstavljajo znatne zneske, koristno uporabljena.

Glede na kompleksnost področja se je potrdilo predvidevanje, da služba notranje revizije, čeprav zaposluje kader s področja revidiranja informacijske tehnologije, težko sama izvaja preglede, ki vključuje zahtevne tehnične preveritve. V zvezi s tem se je izkazalo, da se obrestujejo podrobni postopki načrtovanja revizijskega pregleda, kar velja tudi glede izbora zunanjega izvajalca, torej veščaka, ki mora biti strokoven in izkušen, hkrati pa dovolj fleksibilen, da se dopolnjuje z zaposlenimi v službi notranje revizija in tako skupaj celovito pokrijeta vse vidike področja, tako od upravljanja kot do izpostavljenosti in uporabe naprednih orodij za informacijsko varnost, vsak s svojega zornega kota, za katerega posedujeta znanje in izkušnje. Glede dogovora z zunanjim izvajalcem je pomembno, da dogovori podrobno pokrivajo ne samo obseg preverjanj, ampak tudi način izvedbe posameznih postopkov in predstavitve rezultatov. Pri tem se je za zelo koristno izkazalo kombiniranje več dobrih praks, oziroma natančneje standardov in okvirov, saj je bilo tako lažje ustrezno zagotoviti celovito pokritost izvedbe postopkov, čeprav se na prvi pogled mogoče zdi, da se predpisi v določeni meri podvajajo in s tem tudi delo. Pri angažiranju zunanjega izvajalca se je potrebno zavedati, da poleg koristi prinese tudi dodatna tveganja, ki jih je potrebno z ustreznimi ukrepi, kot so dovolj podrobno dogovorjen nivo izvedenih storitev ter nadzor, obvladovati.

Pri revizijskem pregledu se je ponovno izkazalo, koliko doprinese k kontrolnemu okolju človeški faktor, ki v primeru, da ne izvaja postopkov z najvišjo strokovnostjo in skrbnostjo, lahko izniči visoka vlaganja v najbolj sofisticirano opremo. Ena od ostalih splošnih ugotovitev, ki ne izhaja neposredno iz ciljev pregleda, je doseganje ravnotežja med striktnostjo varnostnih kontrol ter neoviranostjo poslovanja, kar je lahko podlaga za posel svetovanja in s tem še višjo dodano vrednost notranje revizije za banko.

LITERATURA IN VIRI

1. Chambers, Andrew. 2005. *Tolley's International Auditor's Handbook*. London: LexixNexis Butterworths.
2. COSO: *COSO - Celovit okvir notranjega revidiranja, povzetek*. 2013. https://si-revizija.si/datoteke/notranji-revizorji/93/coso_1.pdf, 19.4.2021.
3. COSO: *Enterprise Risk Management, Integrating with Strategy and Performance, Executive Summary*. 2017. Committee of Sponsoring Organizations of the Treadway Commission.
4. COSO: *Internal Controls – Integrated Framework, Executive Summary*. 2013. America Institute of Certified Public Accountants. Durham, ZDA.
5. Delovna gradiva z letnih konferenc ISACA, 2015 - 2019.
6. Infoblox: *How to think like a hacker and stop attacks faster with the MITRE ATT&CK Framework*. 2020. ISACA.
7. Interna navodila in pravilniki, ki obravnavajo področje informacijske varnosti v banki.
8. Interna navodila in pravilniki, ki obravnavajo področje notranjega revidiranja v banki.
9. Internal Auditor. *Attacks Test Cyber Resilience*. https://iaonline.theiia.org/2018/Pages/Attacks-Test-Cyber-Resilience.aspx.
10. Internal Auditor. *Internal auditors need to provide assurance over eight categories of resiliency*. https://iaonline.theiia.org/2017/Pages/Auditing-Cyber-Resiliency.aspx.
11. Internal Auditor. *What's Your Cyber Risk Appetite?* https://iaonline.theiia.org/2016/Pages/Whats-Your-Cyber-Risk-Appetite.aspx.
12. The Institute of Internal Auditors: *Framework for Control - COSO's five components of internal control and questions too important to ignore. The Institute of Internal Auditors*. https://global.theiia.org/standards-guidance/Public%20Documents/COSO_Control_Framework_n.ppt, 19.4.2021.
13. The Institute of Internal Auditors: *Global Technology Audit Guides (GTAGs), Information Technology Risk and Controls, 2nd Edition (predhodno GTAG 1)* (https://global.theiia.org/standards-guidance/recommended-guidance/practice-guides/Pages/Practice-Guides.aspx), 19.4.2021.
14. The institute of Internal Auditors: *Kodeks poklicne etike notranjih revizorjev, ki jih sprejema Inštitut notranjih revizorjev.* The institute of Internal Auditors. https://si-revizija.si/datoteke/splosno/588/nr-Kodeks_etike-IIA.pdf.
15. The Institute of Internal Auditors: *Mednarodni standardi strokovnega ravnanja pri notranjem revidiranju.* 2016. The Institute of Internal Auditors.
16. ISACA: *Cobit 2019 Framework - Governance and Management Objectives*. 2019. ISACA.
17. ISACA: *IT Audit Framework (ITAF), 4th Edition*. 2020. ISACA. Schaumburg. Information Systems Audit and Control Association.
18. Ivan, dr. Turk. 2002. *Pojmovnik računovodstva, financ in revizije*. Ljubljana.
19. Koletnik, Franc. 2007. *Notranje revidiranje*. Ljubljana: Slovenski inštitut za revizijo.
20. Koletnik, Franc. 2018. *Metodika izdelovana zaključnih del na Slovenskem inštitutu za revizijo za pridobitev strokovnega naziva preizkušeni notranji revizor*. Ljubljana: Slovenski inštitut za revizijo.
21. MITRE: *Finding Cyber Threats with ATT&CK™-Based Analytics*. 2017. The MITRE Corporation.
22. Osterman, Milan. 2007. *Poslovni pomen notranjih kontrol z vidika informatike*. Ljubljana: Ekonomska fakulteta Univerze v Ljubljani.
23. NIO – Nacionalni Interoperabilnostni Okvir. *Zakon o informacijski varnosti*, https://nio.gov.si/nio/asset/zakon+o+informacijski+varnosti+zinfv, 15.3.2021.
24. NIST. *Cybersecurity Framework*, https://www.nist.gov/cyberframework,15.6.2020.
25. OWASP: *OWASP Top 10 – 2017, The Ten Most Critical Web Application Security Risks*. https://owasp.org/www-pdf-archive/OWASP_Top_10-2017_%28en%29.pdf.pdf, 19.4.2021.
26. Protiviti: *Top 10 Lessons Learned from Implementing COSO 2013*. 2021.

27. RSA Security, *Cyber Risk Appetite*, https://www.rsa.com/content/dam/en/white-paper/cyber-risk-appetite.pdf, 15.6.2020.
28. Sawyer, Lawrance, M.A. Dittnehofer and J. H. Scheiner. 2003. Sawyer's *Internal Auditing, 5th edition*. Altamonte Springs: The Institute of Internal auditors.
29. *Sklep o ureditvi notranjega upravljanja, upravljalnem organu in procesu ocenjevanja ustreznega notranjega kapitala za banke in hranilnice*, Uradni list RS, št. 73/15, 49/16, 68/17, 33/18, 81/18 in 45/19. http://www.pisrs.si/Pis.web/pregledPredpisa?id=SKLE10628.
30. Slovenski inštitut za revizijo: *Kodeks notranjerevizijskih načel Slovenskega inštituta za revizijo*. Ur. l. RS, št. 40/2011, 27. 5. 2011. https://si-revizija.si/datoteke/splosno/519/nr-Kodeks_nr_nacel-11.pdf.
31. Slovenski inštitut za revizijo: *Kodeks poklicne etike notranjih revizorjev Slovenskega inštituta za revizijo*. Uradni list RS, št. 63/2011, 8. 8. 2011. https://si-revizija.si/datoteke/splosno/443/nr-Kodeks_poklic_etike-nr.pdf.
32. Solm R. 2018. *Cybersecurity and information security – what goes where*?, Information and Computer Security, Vol. 26, št. 1, stran 2-9.
33. *Standard SIST ISO/IEC 27001:2013 (Informacijska tehnologija – Varnostne tehnike – Sistemi upravljanja informacijske varnosti)*. 2013. Mednarodna organizacija za standardizacijo in Mednarodna elektrotehniška komisija.
34. *Standard SIST ISO/IEC 27002:2013 (Informacijska tehnologija - Varnostne tehnike - Pravila obnašanja pri kontrolah informacijske varnosti)*. 2013. Mednarodna organizacija za standardizacijo in Mednarodna elektrotehniška komisija.
35. World Economic Forum's *Global Risks Report*, https://reports.weforum.org/global-risks-report-2020/executive-summary/, 15.6.2020.
36. *Zakon o bančništvu (Z-Ban2)*. Uradni list RS, št. 25/15, 44/16 – ZRPPB, 77/16 – ZCKR, 41/17, 77/18 – ZTFI-1, 22/19 – ZIUDSOL in 44/19 – odl. US. http://www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO6716
37. Zveza računovodij, finančnikov in revizorjev Slovenije: *Pojmovnik*, https://www.zvezarfr.si/pripomocki/slovar. 24.11.2020

PRILOGE

Priloga 1: Seznam pogosto uporabljenih kratic
Priloga 2: Memorandum o načrtovanju
Priloga 3: Obvestilo o izvajanju notranjerevizijskega posla - Najava
Priloga 4: Začetna ocena tveganj in kontrol
Priloga 5: Revizijski program in matrika
Priloga 6: NIST okvir
Priloga 7: Delovni papir
Priloga 8: Revizijsko poročilo

Priloga 1: Seznam Pogosto Uporabljenih Kratic

BS – Banka Slovenije
CDR IV - Direktivi o kapitalskih zahtevah (Capital Requirements Directives)
COBIT - Kontrolni cilji za informacijske in sorodne tehnologije (Control Objectives for Information and Related Technologies)
CRR – Uredba o kapitalskih zahtevah (Capital Requirements Regulation)
DNS – Sistem domenskih imen (Domain Name System)
EBA – Evropski bančni organ (The European Banking Authority)
EDR – Sistem za zaznavanje in odzivanje na končnih točkah/napravah (Endpoint Detection and Response)
GDPR - Splošna uredba EU o varstvu podatkov (General Data Protection Regulation)
ISACA - Združenje za revizijo in nadzor informacijskih sistemov (Information Systems Audit and Control Association)
ISO/IEC – Mednarodna organizacija za standardizacijo, Mednarodna komisija za elektrotehniko (International Organization for Standardization/International Electrotechnical Commission)
ITAF - Okvir za dajanja zagotovil na področju informacijske tehnologije (IT Assurance Framework)
NIST - Narodni urad za standarde in tehnologijo - Agencija Ministrstva za trgovino Združenih držav Amerike (National Institute of Standards and Technology)
OSSTMM – Priročnik za metodologijo glede varnostnega testiranja (Open Source Security Testing Methodology Manual)
OWASP - Projekt za zaščito odprtih spletnih aplikacij (The Open Web Application Security Project)
SIEM - Sistem za upravljanje varnostnih dogodkov in tveganj (Security Information and Event Management)
SMTP – Preprost protokol za prenos elektronske pošte (Simple mail transfer protocol)
SNR – Služba notranje revizije
VPN – Navidezno zasebno omrežje (Virtual Private Network)

Priloga 2: Memorandum o načrtovanju

Memorandum o načrtovanju revizijskih aktivnosti	Oznaka papirja: A.04.01 Pripravil: Milan Osterman Pregledal: Vodja SNR
Revizijski pregled: Kibernetska varnost (RP-2021-03)	

1. Opis področja

Za banko je kibernetska varnost pomembna, zato vlaga občutna sredstva v to področje. Pregled vlaganj ter seznam kadrov v obdobjih 2015 – 2020 je v delovnih papirjih. Vzpostavljen je napredni požarni zid ter sistem SIEM. Opis in shema sta v delovnih papirjih.

Varnostnih incidentov v zadnjem obdobju ni bilo zaznanih. Zadnji je bil v 2015 (napad DDOS), ki pa ni predstavljal pomembe škode za banko razen nedosegljive spletne strani za nekaj ur. Pregled zaznav varnostnih sistemov ter dogodkov operativnega tveganja je v delovnih papirjih.

Organizacijsko se odgovornosti delijo predvsem med vodjem informacijske varnosti (spremljava tveganj na področju informacijske varnosti, predlogi ukrepov, svetovanje, obveščanjem poročanje vodstvu) ter informatiko (skrb za ustrezno delovanje informacijskega sistem), delno tudi skupnim službam (vodenje nabav, evidence).

2. Vključeni oddelki

Informacijska varnost
Informatika
Skupne službe

3. Zunanji in notranji predpisi/akti

Zunanji predpisi:

- Zakon o bančništvu
- Sklep o ureditvi notranjega upravljanja, upravljalnem organu in procesu ocenjevanja ustreznega notranjega kapitala za banke in hranilnice
- Zakon o informacijski varnosti
- Sklep o uporabi Smernic o poročanju o večjih incidentih v skladu z Direktivo (EU) 2015/2366 (PSD2)
- Smernice EBA o upravljanju tveganj, povezanih z IKT in varnostjo
- Zakon o varstvu osebnih podatkov
- GDPR uredba

Notranji akti:

- Varnostna politika,
- IT strategija banke,
- Pravilnik o obravnavi in poročanju varnostnih dogodkov,
- Pravilnik o načrtu neprekinjenega poslovanja,
- Pravilnik o upravljanju pravic in dostopov do informacijskih sistemov banke,
- Pravilnik o upravljanju sistemov in omrežja banke,
- Pravilnik o razvoju aplikacij,
- Pravilnik o upravljanju revizijskih sledi,
- Pravilnik o uporabi IKT opreme in dostopih,
- Pravilnik o skrbništvu sistemov, poročil in podatkov,
- Navodilo za izdelavo varnostnih kopij in arhiviranje,

- Navodilo za upravljanje strežnikov.

4. Predhodni zunanji in notranji pregledi

Revizijski pregled **Načrt neprekinjenega poslovanja (RP-2019-09)**: ni bilo ugotovljenih pomembnih pomanjkljivosti; ažuriranje dokumenta Načrt neprekinjenega poslovanja zaradi sprememb procesov je bili izvedeno v roku.
Redni revizijski pregled **IT varnost – dostopne pravice (RP-2019-02)**: potrebno nadgraditi postopke upravljanja pravic za dokumentni sistem – bilo izvedeno v roku; ažuriranje internih aktov – bilo izvedeno v roku.
Redni revizijski pregled **Upravljanje dogodkov operativnega tveganja (RP-2019-14):** Potrebno nadgraditi postopke poročanje škodnih dogodkov, vendar ne za področje IT.
Redni revizijski pregled **Upravljanje sprememb na področju informacijske tehnologije (RP-2020-02):** Potrebno nadgraditi postopke upravljanja sprememb glede prioritizacije in ustrezno dopolniti notranje akte. Priporočila zaključena v roku.
Redni revizijski pregled **Informacijska varnost (RP-2020-06):** Potrebne manjše dopolnitve varnostne politike ter ureditev pravic v nekaterih aplikacijah zaradi specifik upravljanja. Priporočila zaključena v rokih.

Pri zunanjih pregledih ni bilo ugotovljenih pomanjkljivosti.

5. Sklepi organov in odborov

Pregledani zapisniki uprave in IT odbora za IT področje in povezana področja. Povzetki so v delovnem papirju.

6. Notranja in zunanja poročila

Pregledana redna poročila za IT odpor in sejo uprave, komisije NS ter IT vprašalnik BS v okviru ICAAP za leto 2020. Povzetki so v delovnem papirju.

7. Cilj revizijskega pregleda

Cilj naloge je predstaviti izvedbo notranjerevizijskih postopkov ugotavljanja skladnosti kontrolnega sistema z zakonodajo in dobrimi praksami za področje kibernetske varnosti. Prejemniki revizijskega poročila tako prejmejo zagotovilo, v kolikšni meri kontrolni sistem na pregledanem področju izpolnjuje zahteve zakonodaje ter vodilnih dobrih praks v zvezi s kibernetsko varnostjo.

8. Ključni dejavniki tveganja

Pomembno je operativno tveganj:
- Neustrezna konfiguracija varnostnih sistemov, ki posledično ne bi zaznali oziroma bi prepozno zaznalo incidente
- Neustrezna obravnava varnostnih dogodkov
- Premalo osveščeni zaposleni – človeški faktor (pomembno predvsem z vidika socialnega inženiringa)

9. Okvirni obseg pregleda in predvideni revizijski postopki

Obseg:
- pregled podlag in notranje ureditve področja kibernetske varnosti
- Zunanje varnostno preverjanje storitev (splošni pregled naprav in storitev opravljen z avtomatiziranimi orodji ter delno ročnimi postopki iz zunanjega omrežja,

osredotočenost tega dela pregleda je bila na pridobivanju podatkov o omrežju, strežnikih, tipologiji, storitvah ter na pregledu DNS storitev, poštnih storitev, VPN povezav in na ta način odkrivanje pomanjkljivosti);
- Varnostni pregled požarne pregrade (dostopi, sistemske nastavitve, varnostne politike in nadzorovan vdorni test z uporabo omejenega nabora informacije – t.i. grey-box pristop);
- Pregled sistemov za informacijsko zaščito (SIEM sistema ter povezanih orodij, na primer za zaščito končnih naprav);
- Notranji varnostni pregled kritičnih aplikacij in sistemov (varnostni pregled strežnikov in omrežnih naprav, sistemske programske opreme, izbranih štirih kritičnih aplikacij (kritične na podlagi načrta neprekinjenega poslovanja) z vidika nepooblaščenega dostopa ter nepooblaščenega izvajanja operacij) ter povezanih internih aplikacij;
- Socialni inženiring (dva scenarija ribarjenja (phising-a), eden s priponko in eden s povezavo, fizični obisk pod pretvezo, socialni inženiring prek telefona).

Postopki:
- metode analiziranja/ proučevanja osnovne oz. temeljne dokumentacije (zakonodaja, dobre prakse, interni akti)
- identifikacija in analiza možnih tveganj
- intervjuji oseb pristojnih za izvajanje postopkov
- pregled in analiza dokumentacije o vpeljavi in upravljanju sistema
- preverjanje kontrol testiranje kontrol v omejenem obsegu (izbran vzorec zaznanih varnostnih dogodkov ter ukrepi)

10. Obdobje zajeto v pregled

Datum določen na podlagi zadnjega celovitejšega pregleda s področja informacijske varnosti – zato obdobje od 1.1.2020 – 31.12.2020.
Preveritev skladnosti kontrol z dobrimi praksami v dogovorjenem obdobju (februar 2021)

11. Vodja revizijskega pregleda in člani

Milan Osterman
Zunanji izvajalec za tehnični del pregleda

Priloga 3: Obvestilo o izvajanju notranjerevizijskega posla – Najava (A.02.01)

Prejemniki:
- Vodja informacijske varnosti - Uprava
- Vodja oddelka za informatiko
- Vodja splošnih služb

Pozdravljeni,

v skladu z letnim planom Službe za notranjo revizijo za leto 2021 vas obveščamo, da pričenjamo z redno revizijo " Kibernetska varnost (RP-2021-03)". Vključenost pregleda v letni načrt je bil potrjen s strani uprave in nadzornega sveta.

Cilj notranje revizijskega posla je preveriti skladnost upravljanja področja kibernetske varnosti z zakonodajo in dobrimi praksami.

Služba notranje revizije bo predvidoma začela z revizijskimi postopki 25.1.2021 in se ocenjuje, da bo zaključen v drugi polovici meseca marca 2021. Pregled bo izvedel Milan Osterman v sodelovanju z zunanjimi izvajalci za tehnični del pregleda.

Okvirni obseg pregleda bo predstavljal:
- Zunanje varnostno preverjanje storitev,
- Varnostni pregled požarne pregrade,
- Pregled sistemov za informacijsko zaščito (SIEM sistema ter povezanih orodij),
- Notranji varnostni pregled kritičnih aplikacij in ,
- Socialni inženiring.

Podrobnosti bodo predstavljene na uvodnem sestanku, za katerega bo vabilo poslano ločeno.

V zvezi s pregledom bi vas prosili, da bi nam vnaprej, in sicer najpozneje do 25.1.2021, poslali:
- Informacije glede sprememb v teku za obravnavano področje (spremembe internih aktov, sistemov – nove aplikacije in strojna oprema),
- Morebitne interna akte, ki niso objavljeni v zbirki internih aktov (na primer operativna delovna navodila).

Dodatna dokumentacija bo naročena tekom pregleda, prav tako bodo naknadno dogovorjeni vsi sestanki.

Za dodatne informacije smo na voljo

Lep pozdrav,
Služba notranje revizije
Milan Osterman

Priloga 4: Začetna ocena tveganj in kontrol

Zap. Št.	COSO	Kontrolni cilj	Tveganje	Vpliv	Verjetnost	Ocena tveganja	Kontrole	Začetna ocena kontrol
1	KONTROLNO OKOLJE	IT strategija s strategijo informacijske varnosti ter postavljeni cilji so ustrezni	Nevzpostavljena oziroma neustrezna IT strategija	Srednji	Majhna	Srednje	Dokument strategija, določene odgovornosti, redna preverjanja strategije in ocenjevanja	Ustrezna
2	KONTROLNO OKOLJE	IT strategija s strategijo informacijske varnosti ter postavljeni cilji so ustrezni	Strategija se ne spremlja in dopolnjuje	Srednji	Majhna	Nizko	Redne obravnave in dopolnitve strategije	Ustrezna
3	KONTROLNO OKOLJE	IT strategija s strategijo informacijske varnosti ter postavljeni cilji so ustrezni	Cilji glede kibernetske varnosti niso določeni oziroma ne podpirajo doseganje vizije banke (niso ustrezni)	Srednji	Srednja	Srednje	Operativni načrt banke, postavljena merila za spremljanje	Ustrezna
4	KONTROLNO OKOLJE	Kontrolno okolje podpira upravljanje kibernetske varnosti z zakonodajo in dobrimi praksami	Področje kibernetske varnosti ne dobi dovolj pozornosti / virov sredstev	Srednji	Majhna	Srednje	Finančni načrt, načrt kadrov	Ustrezna
5	KONTROLNO OKOLJE	Organizacijska kultura je ustrezna	Banka nima vzpostavljenega etičnega kodeksa oziroma ga zaposleni ne poznajo	Srednji	Majhna	Nizko	Etični kodeks, komunikacija, izobraževanja	Ustrezna
6	KONTROLNO OKOLJE	Kontrolno okolje podpira upravljanje kibernetske varnosti z zakonodajo in dobrimi praksami	Varnostna politika in spremljajoči dokumenti niso vzpostavljeni in ažurirani	Srednji	Srednja	Srednje	Dokument Varnostna politika, redne dopolnitve	Ustrezna
7	KONTROLNO OKOLJE	Organiziranost je ustrezna	Pristojnosti in odgovornosti niso opredeljene ali so opredeljene neustrezno, razmejitve niso ustrezne,	Srednji	Srednja	Srednje	Interni akti - politike, pravilniki, delovna navodila, opisi procesov	Ustrezna

Zap. Št.	COSO	Kontrolni cilj	Tveganje	Vpliv	Verjetnost	Ocena tveganja	Kontrole	Začetna ocena kontrol
			poročevalski in odločevalski tokovi niso ustrezni.					
8	KONTROLNO OKOLJE	Dokumentiranost pravil je ustrezna	Postopki niso v celoti in natančno popisani (podlage niso ustrezne)	Srednji	Srednja	Srednje	Pravilniki, delovna navodila, popisi procesov, ažurnost dokumentov	Neustrezna
9	KONTROLNO OKOLJE	Skladnost z zakonodajo ter predpisi	Zakonodajne zahteve in predpisi niso prepoznane oziroma ustrezno upravljane	Srednji	Srednja	Srednje	Opredeljen proces spremljanja in implementacije zakonodaje, določena odgovornost za področje informacijske tehnologije/varnosti	Ustrezna
10	KONTROLNO OKOLJE	Kadrovska organiziranost je ustrezna	Področje kibernetske varnosti je kadrovsko podhranjeno	Srednji	Majhna	Nizko	Kadrovski načrt, popolnjenost delovnih mest	Ustrezna
11	KONTROLNO OKOLJE	Kadrovska organiziranost je ustrezna	Neizkušeni zaposleni / brez ustreznih znanja (izobraževanj)	Srednji	Srednja	Srednje	Razvojni načrti kadrov, načrt izobraževanj in njegova izpolnitev, kriteriji za zasedbo delovnih mest	Ustrezna
12	KONTROLNO OKOLJE	Vodstvo je kompetentno, odločevalske linije so jasne	Zaposleni niso ustrezno vodeni	Srednji	Majhna	Nizko	Kriteriji za zasedbo vodilnih delovnih mest, kompetence vodilnih zaposlenih, letno ocenjevanje vodij	Ustrezna
13	OCENJEVANJE TVEGANJ	Tveganja se pravočasno zaznavajo in obravnavajo	Proces identifikacije, ocenjevanja in obvladovanja tveganja ni vzpostavljen in se ne izvaja	Srednji	Majhna	Nizko	Opredeljen proces, dovolj natančno opredeljeni postopki, dodeljene odgovornosti, poročila o upravljanju tveganj, katalog tveganj	Ustrezna
14	OCENJEVANJE TVEGANJ	Prekomerna tveganja se ne prevzemajo	Raven prevzemanja tveganj za kibernetsko varnost ni določena ali ni ustrezna	Srednji	Majhna	Nizko	Opredeljen postopek določanja sprejetega tveganja, določene	Ustrezna

Zap. Št.	COSO	Kontrolni cilj	Tveganje	Vpliv	Verjetnost	Ocena tveganja	Kontrole	Začetna ocena kontrol
							odgovornosti, potrjevanje sprejetega tveganja na nadzornem svetu, zapisniki obravnav	
15	OCENJEVANJE TVEGANJ	Tveganja se pravočasno zaznavajo in obravnavajo	Tveganja na področju kibernetske varnosti se ne identificirajo in redno ocenjujejo	Srednji	Srednja	Srednje	Opredeljeni postopki, dodeljene odgovornosti, poročila o aktivnostih, katalog tveganj	Ustrezna
16	OCENJEVANJE TVEGANJ	Tveganja so ustrezno upravljana	Postopki obvladovanja in odzivi na tveganja, vključno z analizo vzrokov, ter postopki spremljave niso opredeljeni oziroma so opredeljeni neustrezno	Srednji	Srednja	Srednje	Opredelitve postopkov, dodelitve odgovornosti, dokumentacija glede ukrepov, poročila	Ustrezna
17	OCENJEVANJE TVEGANJ	Tveganja so ustrezno upravljana	Tveganja niso pravočasno in ustrezno poročana	Srednji	Majhna	Nizko	Poročila o upravljanju s tveganji	Ustrezna
18	OCENJEVANJE TVEGANJ	Tveganja se pravočasno zaznavajo in obravnavajo	Možnost tveganja prevar niso obravnavane	Srednji	Majhna	Nizko	Opredelitev postopkov, dodelitev odgovornosti, katalog tveganj	Ustrezna
19	KONTROLNE AKTIVNOSTI	Kontrole dostopa podpirajo upravljanje kibernetske varnosti	Fizične kontrole dostopa niso vzpostavljene oziroma se ne izvajajo	Srednji	Majhna	Srednje	Pristopne kontrole, varnostna služba, video nadzorni sistemi	Ustrezna
20	KONTROLNE AKTIVNOSTI	Kontrole dostopa podpirajo upravljanje kibernetske varnosti	Logične kontrole dostopa niso vzpostavljene oziroma se ne izvajajo ustrezno vključno z administratorski dostopi	Velik	Srednja	Visoko	Večstopenjski, podrobno opredeljen sistem dodeljevanja in odvzemanja pravic, ažuren aktivni imenik, omejitev dodeljenih pravic na osnovi samo potrebnih, redna preverjanja	Ustrezna

Zap. Št.	COSO	Kontrolni cilj	Tveganje	Vpliv	Verjetnost	Ocena tveganja	Kontrole	Začetna ocena kontrol
21	KONTROLNE AKTIVNOSTI	Kontrole dostopa podpirajo upravljanje kibernetske varnosti	Kontrole oddaljenega dostopa niso vzpostavljene in se ne izvajajo	Velik	Majhna	Srednje	Opredeljen sistem dodeljevanja in odvzemanja pravic, spremljanje aktivnosti	Ustrezna
22	KONTROLNE AKTIVNOSTI	Kontrole upravljanja sprememb podpirajo upravljanje kibernetske varnosti	Proces upravljanja sprememb ni vzpostavljen oziroma se ne izvaja redno	Srednji	Srednja	Srednje	Podrobno opredeljen proces, orodja za upravljanje sprememb	Ustrezna
23	KONTROLNE AKTIVNOSTI	Dokumentiranost sistemov podpira vzpostavitev kontrol	Sheme (omrežje, toki podatkov) niso ustrezno dokumentirani	Majhen	Srednja	Nizko	Dokumenti glede shem, redna ažuriranja	Ustrezna
24	KONTROLNE AKTIVNOSTI	Ločenost posameznih delov omrežja podpira kontrole informacijske varnosti	Ločenost omrežij oziroma segmentov ni ustrezna	Srednji	Srednja	Srednje	Dokumentirani postopki, vpogled v sistem	Ustrezna
25	KONTROLNE AKTIVNOSTI	Kontrole nad komunikacijskimi tokovi omogočajo doseganje ustreznega nivoja informacijske varnosti	Mrežni tokovi niso opredeljeni in se ne nadzirajo	Srednji	Srednja	Srednje	Opredelitve mrežnih tokov po posameznih napravah, poročila o spremljanju	Ustrezna
26	KONTROLNE AKTIVNOSTI	Dostop do omrežja banke je varovan	Požarni zid ni ustrezno konfiguriran in upravljan	Velik	Srednja	Visoko	Poročila zunanjih izvajalcev, opredeljeni postopki, dodeljene odgovornosti	Ustrezna
27	KONTROLNE AKTIVNOSTI	Dostop do omrežja banke je varovan	Informacijski sistemi niso pravilno vzpostavljeni z vidika varnosti (neustrezne nastavitve), varnostni popravki niso nameščeni	Srednji	Srednja	Srednje	Ustrezne konfiguracije sistemov, izpis zadnjih namestitev popravkov	Ustrezna
28	KONTROLNE AKTIVNOSTI	Sistemi zaznavajo varnostne dogodke in	Sistem za upravljanje varnostnih dogodkov (SIEM)	Srednji	Majhna	Srednje	Ustrezna konfiguracija sistema, tehnična dokumentacija, poročila	Ustrezna

Zap. Št.	COSO	Kontrolni cilj	Tveganje	Vpliv	Verjetnost	Ocena tveganja	Kontrole	Začetna ocena kontrol
		omogočajo ustrezno ukrepanje	ni ustrezno konfiguriran/upravljan				zunanjega izvajalca, dodelitev odgovornosti, poročila sistema	
29	KONTROLNE AKTIVNOSTI	Odgovornosti in naloge zunanjega izvajalca je točno opredeljena, kvaliteta dela je nadzorovana	Sodelovanje z zunanjimi izvajalci ni dovolj podrobno opredeljeno, dela zunanjih izvajalcev niso nadzorovana	Srednji	Srednja	Srednje	Pogodba, sporazum o ravni storitve, poročila o spremljanju zunanjih izvajalcev	Ustrezna
30	KONTROLNE AKTIVNOSTI	Sistemi zaznavajo varnostne dogodke in omogočajo ustrezno ukrepanje	Ostali varnostni sistemi (protivirusni, EDR, na poštnem strežniku, DNS strežnik) niso vzpostavljeni in ne delujejo	Srednji	Majhna	Srednje	Izpis iz nadzornega sistema	Ustrezna
31	KONTROLNE AKTIVNOSTI	Sistemi zaznavajo varnostne dogodke, omogočajo ustrezno ukrepanje ter obravnavo	Varnostni dogodki niso ustrezno klasificirani, obravnavani oziroma dokumentirani	Srednji	Srednja	Srednje	Poročila o obravnavanih varnostnih dogodkih, zapisniki IT odbora	Ustrezna
32	KONTROLNE AKTIVNOSTI	Kritične aplikacije so varne z vidika poskusov nepooblaščenih dostopov ali izvajanja	Kritične aplikacije in sistemi niso ustrezno konfigurirani/upravljani	Srednji	Srednja	Srednje	Tehnična dokumentacija, nastavitve sistema, opredeljeni postopki in odgovornosti, seznam dogodkov operativnega tveganja, poročila	Ustrezna
33	KONTROLNE AKTIVNOSTI	Aktivnosti v sistemih se evidentirajo	Revizijske sledi niso opredeljene, se ne beležijo in pregledujejo	Srednji	Majhna	Nizko	Tehnična dokumentacija, interni akti glede revizijskih sledi, poročila o spremljanju revizijskih sledi	Ustrezna
34	KONTROLNE AKTIVNOSTI	Mogoče se alternativne izvedbe postopkov za	Nadomestni sistemi niso predvideni oziroma niso preverjeni, načrt obnove ni	Srednji	Majhna	Nizko	Vključenost v Načrt neprekinjenega poslovanja,	Ustrezna

Zap. Št.	COSO	Kontrolni cilj	Tveganje	Vpliv	Verjetnost	Ocena tveganja	Kontrole	Začetna ocena kontrol
		kritične procese v izrednih razmerah	ustrezen oziroma se ne posodablja				poročila o testiranjih Načrta neprekinjenega poslovanja	
35	KONTROLNE AKTIVNOSTI	Varnost komunikacij in podatkov je zagotovljena	Podatki in komunikacija (hranjeni in prenosi) niso ustrezno varovani (brez šifriranja ali šibko šifriranje)	Velik	Srednja	Visoko	Tehnična dokumentacija, opredelitev postopkov, pravilniki glede zaupnih podatkov	Ustrezna
36	KONTROLNE AKTIVNOSTI	Informacijski sistem banke omogoča tekoče izvajanje aktivnosti	Zmogljivosti opreme niso ustrezne (lahko tudi samo v izrednih razmerah)	Srednji	Srednja	Srednje	Poročila o spremljanju delovanja, poročila o testiranjih, načrt nabave IT sredstev	Ustrezna
37	KONTROLNE AKTIVNOSTI	Odtekanje podatkov bi bilo pravočasno zaznano in ukrepi izvedeni	Kontrole glede odtekanja podatkov niso vzpostavljene in se ne izvajajo	Srednji	Srednja	Srednje	Pravilniki, tehnična dokumentacija, nastavitve sistema, kontrole v sistemih glede zaznave nepooblaščenega dostopanja in neobičajnega prenosa podatkov	Ustrezna
38	KONTROLNE AKTIVNOSTI	Oprema izločena iz uporabe je ustrezno zavarovana	Naprave in programska oprema niso evidentirani, naprave niso zaščitene, odstranitev je izpeljana neustrezno oziroma ni dokumentirana	Srednji	Majhna	Nizko	Opredelitev postopkov, evidence, poročila o odstranitvah	Ustrezna
39	KONTROLNE AKTIVNOSTI	Ravnanja zaposlenih ustrezajo visokim varnostnim standardom	Zaposleni se ne zavedajo kibernetskih groženj in ne ravnajo preventivno	Srednji	Srednja	Srednje	Pravilniki, delovna navodila, komunikacija - vključno s opozorili, izobraževanja	Ustrezna
40	INFORMIRANJE IN KOMUNICIRANJE	Vodstvo se odloča na podlagi ustreznih informacij	Upravljalni organi/vodstvo nimajo dovolj in ustrezne informacije za odločanje	Srednji	Majhna	Srednje	Gradiva za vodstvo, redna poročila, zapisniki obravnav in sklepi	Ustrezna

Zap. Št.	COSO	Kontrolni cilj	Tveganje	Vpliv	Verjetnost	Ocena tveganja	Kontrole	Začetna ocena kontrol
41	INFORMIRANJE IN KOMUNICIRANJE	Komunikacija omogoča pravočasno in celovito obveščanje vseh relevantnih zaposlenih	Vse ustrezne organizacijske enote niso pravočasno in celovite obveščene o varnostnih dogodkih	Srednji	Srednja	Srednje	Poročila, ki jih prejemajo organizacijske enote	Ustrezna
42	INFORMIRANJE IN KOMUNICIRANJE	Dogodki s področja informacijske varnosti so ustrezno obravnavani	Kibernetska varnost ni ustrezno obravnavana s strani vodstva	Srednji	Srednja	Srednje	Zapisniki sej in sklepi	Ustrezna
43	INFORMIRANJE IN KOMUNICIRANJE	Zunanje institucije prejemajo zahtevane informacije pravočasno in v ustreznem obsegu te obliki	Poročevalske aktivnosti v zvezi z zunanjimi deležniki niso vzpostavljene oziroma se ne izvajajo ustrezno	Srednji	Majhna	Nizko	Poročila zunanjim institucijam, prejeta dokumentacija zunanjih institucij	Ustrezna
44	AKTIVNOSTI SPREMLJANJA	Opredelitve dolžnosti in nalog omogoča hitro in kvalitetno izvedbo brez nepotrebnih zamud ter zapletov	Koordinacija izvajanja aktivnosti ni opredeljena oziroma se ne izvaja	Srednji	Majhna	Nizko	Opredelitev postopkov v internih aktih, določitev odgovornosti	Ustrezna
45	AKTIVNOSTI SPREMLJANJA	Nadzor je vzpostavljen in poteka ustrezno	Vodstveni nadzor nad pregledom delovanja notranjih kontrol	Srednji	Srednja	Srednje	Opredelitev postopkov v internih aktih, določitev odgovornosti, poročila vodstvenega nadzora, poročila IT odbora	Ustrezna
46	AKTIVNOSTI SPREMLJANJA	Področje kibernetske varnosti je predmet rednih in celovitih pregledov	Preverjanja s strani neodvisnih funkcij se ne izvajajo redno	Srednji	Majhna	Srednje	Opredelitev postopkov v internih aktih, določitev odgovornosti, poročila neodvisnih pregledov	Ustrezna

OZNAKA IN VRSTA PREGLEDA

RP-2021-03 Redni pregled

NAZIV PREGLEDA

Kibernetska varnost

PODLAGA ZA IZVEDBO

Letni načrt službe notranje revizije za leto 2021

NAMEN, CILJI, SODILA IN OBSEG PREGLEDA

Namen:

- Podati zagotovilo o skladnosti področja kibernetske varnosti z dobrimi praksami

Cilj:

- Cilj notranje revizijskega posla je preveriti skladnost upravljanja področja kibernetske varnosti z dobrimi praksami.

Sodila:

- Zakonodaja, dobre prakse

Obseg posla:

- pregled podlag in notranje ureditve področja kibernetske varnosti;
- Zunanje varnostno preverjanje storitev (splošni pregled naprav in storitev opravljen z avtomatiziranimi orodji ter delno ročnimi postopki iz zunanjega omrežja, osredotočenost tega dela pregleda je bila na pridobivanju podatkov o omrežju, strežnikih, tipologiji, storitvah ter na pregledu DNS storitev, poštnih storitev, VPN povezav in na ta način odkrivanje pomanjkljivosti);
- varnostni pregled požarne pregrade (dostopi, sistemske nastavitve, varnostne politike in nadzorovan vdorni test z uporabo omejenega nabora informacije – t.i. grey-box pristop);
- pregled sistemov za informacijsko zaščito (SIEM sistema ter povezanih orodij, na primer za zaščito končnih naprav);
- notranji varnostni pregled kritičnih aplikacij in sistemov (varnostni pregled strežnikov in omrežnih naprav, sistemske programske opreme, izbranih štirih kritičnih aplikacij (kritične na podlagi načrta neprekinjenega poslovanja) z vidika nepooblaščenega dostopa ter nepooblaščenega izvajanja operacij) ter povezanih internih aplikacij;
- socialni inženiring (dva scenarija ribarjenja (phising-a), eden s priponko in eden s povezavo, fizični obisk pod pretvezo, socialni inženiring prek telefona).

4. OE IZVAJALKE PREDMETA POSLA

Informacijska varnost
Informatika
Splošne službe

5. OMEJITEV

Za izvedbo tehničnega dela pregleda je bil uporabljen zunanji izvajalec. Sistemi so preverjeni glede znanih ranljivosti v času izvedbe pregleda.

6. ČASOVNI OKVIR IZVEDBE POSLA

Revizijska skupina	**Načrtovani dnevi**	**Realizirani dnevi**
Milan Osterman	20	21

NAČRT PRIPRAVIL: Milan Osterman	**NAČRT POTRDIL: Vodja SNR**

MATRIKA

Povezava na matriko (Zap. Št.)	Revizijskih postopek	Zunanji izvajalec	Povezava na NIST	Delovni papir	Ugotovitev	Verjetnost	Vpliv	Preostalo tveganje	Priporočilo
1	Proučiti IT strategijo, preveriti odgovornosti, oceniti skladnost s poslovno strategijo in stopnjo podpiranja doseganja poslovnih ciljev	Ne	ID.BE-1, ID.BE-2, ID.BE-3, ID.BE-4	B.01	Področje informacijske varnosti je ustrezno vključeno v IT strategijo banke, ki je redno osveževana.	Majhna	Nizek	Nizko	/
3	Proučiti operativni načrt banke, preveriti odgovornosti, oceniti smiselnost uporabljenih kazalnikov, proučiti poročila glede doseganja kazalnikov	Ne	ID.BE-1, ID.BE-2, ID.BE-3	B.02	Vzpostavljeni so podrobni cilji ter kazalniki, ki se redno ocenjujejo in pregledujejo za ocenjevanje uspešnosti in obsega izvrševanja.	Majhna	Nizek	Nizko	/
4	Proučiti finančni načrt in načrt kadrov ter razliko med predlaganim in potrjenim načrtom, razgovor z odgovornimi za področje kibernetske varnosti, preveriti dejansko porabo sredstev	Ne	ID.AM-5, ID.BE-2, ID.BE-3, ID.BE-4	B.03	Področje prejema dovolj pozornosti vodstva ,vzpostavljen je IT odbor, kot svetovalni odbor upravi, ki redno obravnava tudi zadeve s področja kibernetske varnosti. Pomembne stvari se poročajo nadzornemu svetu v okviru upravljanja tveganj. Vse bistvene predlagane investicije so bile potrjene.	Majhna	Nizek	Nizko	/
6	Proučitev Varnostne politike in prilog, preveritev celovitosti glede na primere dobrih praks ter	Ne	ID.GV-1, ID.GV-2, ID.GV-3, ID.GV-4	B.04	Varnostna politika s prilogami je vzpostavljena in redno ažurirana (ob pomembnih spremembah	Majhna	Nizek	Nizko	/

MATRIKA

Povezava na matriko (Zap. Št.)	Revizijskih postopek	Zunanji izvajalec	Povezava na NIST	Delovni papir	Ugotovitev	Verjetnost	Vpliv	Preostalo tveganje	Priporočilo
	okvirov, preveriti odgovornosti, preveriti ažurnost dokumentov				oziroma pregledana najmanj letno).				
7	Preveriti obstoj in celovitost internih aktov glede organiziranosti banke (predvsem Pravilnik o organiziranost, Pravilnik o odborih, pravilnike in delovna navodila organizacijskih enot); preveritev popisa procesa Tehnološke-informacijske podpore s poudarkom na kibernetski varnosti glede delitev odgovornosti in organiziranosti, razgovor z odgovornimi za področje kibernetske varnosti glede organiziranosti dela/poročanj, odgovornosti; preveriti ažuriranje internih aktov	Ne	ID.GV-1, ID.GV-2, ID.AM-6, DE.DP-1, RS.CO-1	B.05	Pristojnosti in odgovornosti so splošno opredeljene v Aktu o organiziranosti, podrobne opredelitve so v posameznih pravilnikih, navodil ter v popisu procesa. Razmejitve so ustrezne.	Majhna	Nizek	Nizko	/
8	Proučitev pravilnikov in delovnih navodil, popisa procesa, preveritev podrobnosti opisanih zadolžitev in odgovornosti, preveritev ažuriranja internih aktov	Ne	ID.GV-2, ID.GV-3, ID.GV-4	B.06	Postopki so opredeljeni v internih aktih, ki se prav tako redno pregledujejo in osvežujejo. V času revizijskega pregleda je bilo v prenovi delovno navodilo za upravljanje sistema elektronske pošte zaradi menjave poštnega strežnika, ki je bilo zaključeno pred	Majhna	Nizek	Nizko	/

MATRIKA

Povezava na matriko (Zap. Št.)	Revizijskih postopek	Zunanji izvajalec	Povezava na NIST	Delovni papir	Ugotovitev	Verjetnost	Vpliv	Preostalo tveganje	Priporočilo
					koncem revizijskega pregleda. V fazi načrtovanja je bilo ugotovljeno, da Navodilo za upravljanje varnostnih sistemov ni ažurirano s spremembami zaradi nove opreme, vendar je dopolnjeno tekom pregleda.				
9	Proučiti proces spremljanja zakonodaje in predpisov za področje kibernetske varnosti, preveritev odgovornosti, preveritev implementacije za zadnje spremembe zakonodaje	Ne	ID.GV-3	B.07	Formalni postopki spremljanja in implementacije regulative so vzpostavljeni, odgovornosti so določene za vsa področja. Pregled zadnjih sprememb je pokazal, da so zakonodaja in predpisi ustrezno vključeni v dokumente banke.	Majhna	Nizek	Nizko	/
11	Proučiti razvojne načrte kadrov, preveritev izpolnitev načrta izobraževanja, primerjava kompetenc zaposlenih z opisi delovnih mest, razgovori z odgovornimi za področje kibernetske varnosti	Ne	PR.AT-1, PR.AT-2, PR.AT-5	B.08	Zaposleni so ustrezno izobraženi, saj se redno udeležujejo načrtovanih izobraževanj, ki so smiselna in potrebna glede na dodeljene naloge. Zaposleni so ustrezno izobraženi, saj se redno udeležujejo načrtovanih izobraževanj, ki so smiselna in potrebna	Majhna	Nizek	Nizko	/

MATRIKA

Povezava na matriko (Zap. Št.)	Revizijskih postopek	Zunanji izvajalec	Povezava na NIST	Delovni papir	Ugotovitev	Verjetnost	Vpliv	Preostalo tveganje	Priporočilo
					glede na dodeljene naloge. Njihovo število je zadostno, da omogoča ustrezno razmejitev dolžnosti ter nadomeščanje. Varnostni inženir ima nadomeščanje v okviru banke, poleg tega je pogodbeno urejeno sodelovanje z zunanjim izvajalcem, ki delno izvaja storitve SOC centra/Varnostno operativnega centra.				
15	Proučiti proces identifikacije in ocenjevanja tveganj, preveriti odgovornosti za izvedbo procesa, preveriti zadnje poročilo, oceniti smiselnost ocen, preveriti katalog tveganj in oceniti ustreznost glede na primere dobrih praks	Ne	ID.SC-2, ID.GV-4	B.09	Področje kibernetske varnosti je vključeno v redno ocenjevanje tveganj. Tveganja se identificirajo najmanj enkrat letno ter ob vsaki pomembni spremembi.	Majhna	Nizek	Nizko	/
16	Proučiti proces obvladovanja tveganj, proučiti poročilo glede obvladovanja tveganj, preveriti dodelitve odgovornosti, preveritev zapisnikov upravljalnih organov, oceniti smiselnost predlaganih ukrepov na podlagi dobrih praks	Ne	ID.SC-2, ID.SC-3, ID.SC-5, ID.RA-6, ID.RM-1	B.10	Nagnjenost k prevzemanju tveganj je za revidirano področje določena in potrjena. Zadnja identifikacija in ocena tveganja sta bili izvedeni v septembru 2020 zaradi prilagoditev aplikacij novim	Majhna	Nizek	Nizko	/

MATRIKA

Povezava na matriko (Zap. Št.)	Revizijskih postopek	Zunanji izvajalec	Povezava na NIST	Delovni papir	Ugotovitev	Verjetnost	Vpliv	Preostalo tveganje	Priporočilo
					produktom. V okviru revizijskega pregleda so bili pregledani postopki identifikacije ter ocenjevanja inherentnih tveganj, predpostavke in parametri, ustreznost ocene kontrolnega okolja ter preostalega tveganja. Indikatorji nagnjenosti k prevzemanju tveganj niso bili preseženi v nobenem primeru, prav tako niso bile odkrite pomanjkljivosti pri pregledu postopkov identifikacije ter ocenjevanja tveganj.				
19	Preveriti obstoj pristopnih kontrol in njihove delovanje (test kontrol, pregled log datotek), izvedba fizičnega obiska pod pretvezo s strani zunanjega izvajalca, pregled poročil o pregledih video nadzornih sistemov	Ne	PR.AC-2, PR.IP-5, DE.CM-2	B.11	Kontrole pristopa so vzpostavljene na vseh točkah in delujejo, kar potrjujejo tudi logi. Poročila potrjujejo delovanje video nadzornega sistema. Fizični obisk pod pretvezo je bil neuspešen, saj je receptor vse poskuse vstopa zaustavil, tudi poskusi	Majhna	Nizek	Nizko	/

MATRIKA

Povezava na matriko (Zap. Št.)	Revizijskih postopek	Zunanji izvajalec	Povezava na NIST	Delovni papir	Ugotovitev	Verjetnost	Vpliv	Preostalo tveganje	Priporočilo
					pridobivanja podatkov prek telefona so bili neuspešni.				
20	Preveritev opredelitev postopkov, preveritev tehnične dokumentacije, preveritev skladnosti podatkov v aplikaciji za upravljanje pravic ter dejanskega stanja za aktivni direktorij, preveritev administratorskih pravic za izbran sisteme, preveritev ustreznosti dodeljenih pravic za izbrane sistema na podlagi vzorca	Da	PR.AC-1, PR.AC-4, PR.AC-6, PR.AC-7	B.12	Postopki v zvezi z logičnimi kontrolami dostopov so vzpostavljeni, odgovornosti so prav tako opredeljene. Zahtevki in delovni tok je podprt s posebno aplikacijo. Ni bilo ugotovljenih pomanjkljivosti glede dodeljenih dostopov tako z vidika skladnosti zahtevkov in dejanskega stanja ter omejitve na minimalni potrebni obseg pravic. Pregled na vzorcu ni pokazal pomanjkljivosti (10% naključno izbranih aktivnih uporabnikov AD s preveritvijo za vse sisteme, zaposleni s spremembami delovnih mest v zadnjih dveh letih). Prav tako ni bilo ugotovljenih pomanjkljivostih pri uporabnikih s privilegiranimi pravicami (dodeljevanje, odvzemanje	Majhna	Nizek	Nizko	/

MATRIKA

Povezava na matriko (Zap. Št.)	Revizijskih postopek	Zunanji izvajalec	Povezava na NIST	Delovni papir	Ugotovitev	Verjetnost	Vpliv	Preostalo tveganje	Priporočilo
					gesel, upravičenost dodelitve, uporaba ROOT gesel).				
21	Preveritev postopkov, preveritev odgovornosti, preveritev poročil o nadzoru, preveritev skladnosti poročil ter revizijskih sledi	Da	PR.AC-3	B.13	Vsi oddaljeni dostopi se spremljajo glede časovnih oken, uporablja se dvofaktorska avtentikacija. Redno se preverja upravičenost dodelitve, za vse dodelitve je potrebno izvesti poseben postopek (izveden za vse primere).	Majhna	Nizek	Nizko	/
22	Preveritev postopkov, preveritev odgovornosti, pregled obstoja orodij za upravljanje sprememb s poudarkom na delitvah odgovornosti ter vodenju revizijskih sledi, izvedba pregleda sprememb na osnovi vzorca glede izvedbe, potrditve, dokumentiranosti in sledi	Ne	PR.DS-6, PR.DS-7, PR.IP-3, PR.MA-1, PR.MA-2	B.14	Proces upravljanja sprememb je opredeljen, postopki, odgovornosti in orodja so določeni. Revizijska sled se vodi, poročila se redno pripravljajo in posredujejo.	Majhna	Nizek	Nizko	/
24	Preveritev dokumentiranosti pravil glede upravljanja segmentov ter razdelitve omrežja na segmente, vpogled v sistem glede ločenosti segmentov, test nepooblaščenega prehajanja med segmenti (izvede zunanji izvajalec)	Da	PR.AC-5	B.15	Segmenti so ustrezno vzpostavljeni, prehodi so omejeni glede na popise tokov, z izjemo enega strežnika. Pri slednjem je bilo ugotovljeno, da je bil postavljen tik pred	Majhna	Nizek	Nizko	/

MATRIKA

Povezava na matriko (Zap. Št.)	Revizijskih postopek	Zunanji izvajalec	Povezava na NIST	Delovni papir	Ugotovitev	Verjetnost	Vpliv	Preostalo tveganje	Priporočilo
					pregledom in zato nastavitve še niso bile v celoti zaključene. Ker je preveritev pokazala, da postopki potekajo v skladu z načrti, priporočilo ni podano. Administracija je ustrezno urejena, tako z vidika dostopov kot beleženja in upravljanja sledi. DMZ prostor je restriktivno ločen od ostalega omrežja				
25	Proučitev popisa mrežnih tokov, pregled vzpostavitve omejitev glede mrežnih tokov v sistemu in nadzora (izvede zunanji izvajalec)	Da	DE.AE-1	B.16	Vse naprave imajo popisane dovoljene tokove ("karton"), poskusi nedovoljenih se spremljajo in obravnavajo.	Majhna	Nizek	Nizko	/
26	Proučitev tehnične dokumentacije, poročila zunanjih izvajalcev glede opravljenih nalog, preveritev odgovornosti (izvede zunanji izvajalec)	Da	DE.CM-1	B.17	Pri pregledu zunanjih storitev banke (javni segment informacijskega sistema) vključno s storitvami DNS in SMPT ni bilo ugotovljeno, da bi bilo dostopnih preveč informacij, ki bi pomagale napadalcem. Na nivoju omrežja pregled ni pokazal varnostnih pomanjkljivosti v konfiguraciji VPN sistema.	Majhna	Nizek	Nizko	/

MATRIKA

Povezava na matriko (Zap. Št.)	Revizijskih postopek	Zunanji izvajalec	Povezava na NIST	Delovni papir	Ugotovitev	Verjetnost	Vpliv	Preostalo tveganje	Priporočilo
					Požarna pregrada je ustrezno vzpostavljena – programska oprema je ažurirana, fizična postavitev ter segmenti so ustrezno vzpostavljeni. Varnostne politike so vzpostavljene in se upoštevajo. IPS/IDS zaščita je vključena, uporabljeni protokoli se avtomatično pregledujejo. Vsi poskusi vdorov so bili neuspešni. Varnostni popravki so ažurno nameščeni, uporabljajo se močni algoritmi in protokoli.				
27	Varnostni pregled s strani zunanjega izvajalca z avtomatiziranimi orodji ter ročnimi postopki z upoštevanjem OWASP top10 ter Mitre Att&ck	Da	DE.CM-3, DE.CM-4, DE.CM-5, DE.DP-1, DE.DP-2, DE.DP-3, DE.DP-4, DE.DP-5	B.18	Pregled s strani zunanjega izvajalca ni pokazal pomanjkljivosti glede varnostnih nastavitev, varnostni popravki so ažurno nameščeni.	Majhna	Nizek	Nizko	/
28	Izvedba pregleda s strani zunanjega izvajalca: proučitev dokumentacije, preveritev odgovornosti, izvedba simulacij	Da	DE.CM-3, DE.CM-4, DE.CM-5, DE.CM-8	B.19	Vsi simulirani varnostni dogodki so bili pravočasno zaznani s strani varnostnih centralnih sistemov oziroma	Majhna	Nizek	Nizko	/

MATRIKA

Povezava na matriko (Zap. Št.)	Revizijskih postopek	Zunanji izvajalec	Povezava na NIST	Delovni papir	Ugotovitev	Verjetnost	Vpliv	Preostalo tveganje	Priporočilo
	napadov, zbiranja informacij iz zunanjega omrežja, poskusov nepooblaščenih dostopov iz zunanjega omrežja ter notranjega omrežja, uporabe nepooblaščenih naprav v notranjem omrežju, poskusov nepooblaščenih dostopov iz notranjega omrežja, prikritega (lateral movement) med segmenti, izvedba neavtoriziranih ter neobičajnih aktivnosti (v skladu z Mitre Att&ck) ter spremljanje zaznavanja dogodkov, obveščanja ter izvedba ukrepov, preveritev nastavitev sistema glede na dobre prakse				na končnih napravah, uspešno sporočeni v sistem SIEM, sproženi so bili ustrezni ukrepi. Ni bilo zaznanih pomanjkljivosti, da določeni viri (naprave) ne bi bili vključeni.				
29	Preveritev določil pogodbe ter sporazume o ravni storitve (SLA), proučitev poročil o spremljanju aktivnosti zunanjih izvajalcev, preveritev odgovornosti	Ne	DE.CM-6, ID.SC-4, PR.AT-3	B.20	Pogodbena razmerja so ustrezno urejena vključno z dogovorom o nivoju storitev, delovanje se stalno spremlja, za kar je vzpostavljen proces (vključno s poročanje), ki ga spremlja služba za upravljanje tveganj.	Majhna	Nizek	Nizko	/
30	Izvedba pregleda s strani zunanjega izvajalca: proučitev dokumentacije, preveritev	Da	DE.CM-7, DE.AE-2, DE.AE-3,	B.21	Pri pregledu ostalih sistemov za informacijsko zaščito je bilo ugotovljeno, da so ti	Majhna	Nizek	Nizko	/

MATRIKA

Povezava na matriko (Zap. Št.)	Revizijskih postopek	Zunanji izvajalec	Povezava na NIST	Delovni papir	Ugotovitev	Verjetnost	Vpliv	Preostalo tveganje	Priporočilo
	odgovornosti, izvedba simulacij napadov (v skladu z Mitre Att&ck) ter spremljanje zaznavanja dogodkov in sporočanja v centralni sistem		DE.AE-4, DE.AE-5		sistemi (EDR zaščita končnih naprav, protivirusni programi) ustrezno vzpostavljeni s performančnega ter varnostnega vidika, da so sposobni pravočasno zaznati varnostne dogodke, prav tako so ustrezni postopki obravnave ter sporočanja. Varnostni popravki so ažurno nameščeni, uporabljajo se močni algoritmi in protokoli. Redundanca DNS strežnikov je vzpostavljena, prav tako so ustrezno onemogočene storitve nepooblaščenim osebam. Ranljivosti SMTP strežnikov elektronske pošte niso bile zaznane, zaščita proti pošiljanju nezaželene pošte je vzpostavljena, aktivirani so mehanizmi za preprečevanje ponarejenih sporočil.				
31	Preučitev dokumentacije (pravilnikov ter navodil),	Da	DE.AE-2, DE.AE-3,	B.22	Vsak dogodek je vpisan v poseben sistem za vodenje	Majhna	Nizek	Nizko	/

MATRIKA

Povezava na matriko (Zap. Št.)	Revizijskih postopek	Zunanji izvajalec	Povezava na NIST	Delovni papir	Ugotovitev	Verjetnost	Vpliv	Preostalo tveganje	Priporočilo
	preveritev odgovornosti, pregled zahtevkov glede na opredelitve v internih aktih, pregled zapisnikov IT odbora, pregled rednih poročil in izrednih poročanj		DE.AE-4, DE.AE-5, RS.RP-1, RS.AN-1, RS.AN-2, RS.AN-3, RS.AN-4, RS.AN-5, RS.MI-1, RS.MI-2, RS.MI-3, RS.IM-1, RS.IM-2		zahtevkov, bistveni podatki so obvezna polja za vnos. Poročilo o zamudah pri ukrepih se redno generira ter posreduje.				
32	Varnostni pregled izbranih aplikacij s strani zunanjega izvajalca z avtomatiziranimi orodji ter ročnimi postopki z upoštevanjem OWASP top10 ter Mitre Att&ck	Da	PR.IP-1, PR.IP-2, PR.PT-3, PR.DS-8	B.23	Pri notranjem varnostnem pregledu kritičnih aplikacij in sistemov je bili za aplikacijo za upravljanje z osnovnimi sredstvi ugotovljeno, da komunikacija s sistemom za upravljanje zbirk podatkov poteka z uporabo ranljivega protokola, kar bi v primeru prestrezanja napadalcu olajšalo možnost dešifriranja poslanih podatkov, ter za interno razvito aplikacija za vodenje šifrantov, da	Srednja	Nizek	Srednje	RP-2021-03-01, RP-2021-03-02, RP-2021-03-03

MATRIKA

Povezava na matriko (Zap. Št.)	Revizijskih postopek	Zunanji izvajalec	Povezava na NIST	Delovni papir	Ugotovitev	Verjetnost	Vpliv	Preostalo tveganje	Priporočilo
					razkriva podatke o zaledni infrastrukturi ter da uporablja neustrezni certifikat. V drugih primerih se uporabljajo močni šifrirni algoritmi, močni protokoli ter ustrezni certifikati.				
33	Pregled vodenja revizijskih sledi v posameznih sistemih; preveritev glede celovitosti podatkov za celotno obdobje zadnjih dveh let; preveritev beleženja podatkov v relevantnih sistemih v zvezi z vdornim testom; pregled dokazil glede periodične kontrole spremljanja s strani skrbnikov aplikacije in poročanja; pregled vključitve virov v SIEM za kritične sisteme in njihove spremljava v sistemu SIEM.	Da	PR.PT-1	B.24	Kljub temu, da je bila začetna ocena tveganja nizka, je to tveganje vključeno v pregled zaradi zakonskih zahtev. Pregled je pokazal, da se v vseh sistem vodijo revizijske sledi. Iz kritičnih sistemov po opredelitvi banke v določenem delu posredujejo v nadzorni sistem SIEM. Iz vseh sistemov se najmanj enkrat letno pregledujejo in ugotovitve poročajo službi za informacijsko varnost.	Majhna	Nizek	Nizko	/
35	Varnostni pregled hranjenja podatkov ter komunikacijskih poti s strani zunanjega izvajalca z avtomatiziranimi orodji ter ročnimi postopki z upoštevanjem OWASP top10 ter Mitre Att&ck	Da	PR.DS-1, PR.DS-2, PR.IP-4, PR.PT-4	B.25	Pregled je pokazal, da se uporabljajo močni šifrirni algoritmi, razen v primeru aplikacije za vodenjem osnovnih sredstev (povezava	Majhna	Nizek	Nizko	/

MATRIKA

Povezava na matriko (Zap. Št.)	Revizijskih postopek	Zunanji izvajalec	Povezava na NIST	Delovni papir	Ugotovitev	Verjetnost	Vpliv	Preostalo tveganje	Priporočilo
					na priporočilo RP-2021-03-01).				
36	Razgovor z odgovornimi za informacijske sisteme, pregled načrtov nabav, pregled poročil o delovanju, pregled poročil o testiranjih	Da	PR.DS-4	B.26	Poročila o delovanju ter poročila o testiranjih so pokazala, da so zmogljivosti ustrezne. Vzpostavljen je postopek spremljanja limitov ter eskalacij ski mehanizmi, prav tako odgovornosti.	Majhna	Nizek	Nizko	/
37	Varnostni pregled s strani zunanjega izvajalca z avtomatiziranimi orodji ter ročnimi postopki z upoštevanjem OWASP top10 ter Mitre Att&ck glede ustreznosti kontrol v zvezi z odtekanjem podatkov, proučitev pravilnikov in tehnične dokumentacije	Da	PR.DS-5	B.27	Kontrole so vzpostavljene - teko preprečevalne (omejitve na portih in uporabi oblačnih in sorodnih rešitvah) kot zaznavalne (nenavadni prenosi).	Majhna	Nizek	Nizko	/
39	Proučitev pravilnikov in navodil, pregled preteklih dogodkov in ukrepov, pregled izobraževanj in komunikacij na to temo, izvedba simulacije socialnega inženiringa na podlagi dveh scenarijev (lažno sporočil s priponko, lažno sporočilo s povezavo) s strani zunanjega izvajalca	Da	PR.AT-1, PR.IP-11	B.28	V okviru izvajanja postopkov socialnega inženiringa sta bila izvedena dva scenarija ribarjenja (phisinga) – najprej je bilo poslano lažno sporočilo kadrovske službe s podatki o finančni nagradi v pripeti zlonamerni datoteki, nato pa	Srednji	Srednji	Srednje	RP-2021-03-04

MATRIKA

Povezava na matriko (Zap. Št.)	Revizijskih postopek	Zunanji izvajalec	Povezava na NIST	Delovni papir	Ugotovitev	Verjetnost	Vpliv	Preostalo tveganje	Priporočilo
					še vabilo k prijavi v nov lažni spletni portal banke prek povezave v sporočilu. Datoteko je kljub znakom, da je sporočilo lažno, odprlo osem ljudi, na spletno povezavo v drugem lažnem sporočilu pa je kliknilo enajst zaposlenih, nobeden ni vnesel prijavni podatkov.				
40	Proučitev gradiv, poročil, zapisnikov obravnav in sklepov, razgovor z odgovornimi	Ne	RS.CO-2, RS.CO-3, RS.CO-4	B.29	Pri poročanju pomanjkljivosti niso bile ugotovljene. Najmanj mesečno oziroma pogosteje po potrebi vodja informacijske varnosti v sodelovanju z oddelkom za informatiko ter po potrebi tudi drugimi odgovornimi enotami pripravi redno poročilo, ki ga obravnava IT odbor, z njim je seznanjena tudi uprava. Nadzorni svet se seznani s pomembnimi zadevami v okviru upravljanja tveganj.	Majhna	Nizek	Nizko	/

MATRIKA

Povezava na matriko (Zap. Št.)	Revizijskih postopek	Zunanji izvajalec	Povezava na NIST	Delovni papir	Ugotovitev	Verjetnost	Vpliv	Preostalo tveganje	Priporočilo
41	Proučitev poročil, razgovor z odgovornimi iz posameznih organizacijskih enot	Ne	RS.CO-2, RS.CO-3, RS.CO-4	B.30	Služba za upravljanje tveganj ter Oddelek za informatiko redno prejemata poročila s področja kibernetske varnosti ter sta vključena v relevantno komunikacijo.	Majhna	Nizek	Nizko	/
42	Proučitev zapisnikov obravnav in sklepov, razgovor z odgovornimi	Ne	ID.BE-3	B.31	IT odbor mesečno obravnava poročila, sprejeti so ustrezni sklepi. Uprava je redno seznanjena o aktivnostih pred obravnave redne periodične točke. Obravnave so ustrezno dokumentirane, ukrepi se spremljajo. Uprava potrjuje pomembne zadeve, kjer je zahtevano, oziroma je seznanjena. Tudi obravnave nadzornega sveta so ustrezno dokumentirani, realizacija sklepov se spremlja.	Majhna	Nizek	Nizko	/
45	Pregled pravilnikov, pregled poročil o izvedenih nadzorih, razgovor z odgovornimi vodji	Ne	RS.CO-2, RC.CO-3	B.32	Vodstveni nadzor se izvaja in se dokumentira, kar potrjujejo poročila o delu/aktivnostih posameznih oddelkov za upravo.	Majhna	Nizek	Nizko	/

MATRIKA

Povezava na matriko (Zap. Št.)	Revizijskih postopek	Zunanji izvajalec	Povezava na NIST	Delovni papir	Ugotovitev	Verjetnost	Vpliv	Preostalo tveganje	Priporočilo
46	Pregled poročil o izvedenih pregledih, pregled načrtov dela odgovornega za informacijsko varnost, razgovor z odgovornim za informacijsko varnost	Ne	DE.DP-4, RS.CO-3, RC.CO-3	B.33	Poročila organizacijske enote Informacijska varnost potrjujejo izvedbo vsaj enega obsežnejšega pregleda s področja informacijske varnosti letno, ukrepi se spremljajo in poročajo.	Majhna	Nizek	Nizko	/

Priloga 6: NIST okvir

Funkcija	Kategorija	Oznaka	Podkategorija	Povezava na Cobit, ISO 27001
Identificiranje (ID)	Upravljanje sredstev (ID.AM): Podatki, osebje, naprave, sistemi in naprave, ki organizaciji omogočajo doseganje poslovnih ciljev, se identificirajo in upravljajo v skladu z njihovim sorazmernim pomenom za organizacijske cilje in strategijo tveganja organizacije.	ID.AM-1	ID.AM-1: Popisane so fizične naprave in sistemi v organizaciji	COBIT 5 BAI09.01, BAI09.02; ISO/IEC 27001:2013 A.8.1.1, A.8.1.2
		ID.AM-2	ID.AM-2: Programske platforme in aplikacije znotraj organizacije so popisane	COBIT 5 BAI09.01, BAI09.02, BAI09.05; ISO/IEC 27001:2013 A.8.1.1, A.8.1.2, A.12.5.1
		ID.AM-3	ID.AM-3: Popisani so organizacijski komunikacijski in podatkovni tokovi	COBIT 5 DSS05.02; ISO/IEC 27001:2013 A.13.2.1, A.13.2.2
		ID.AM-4	ID.AM-4: Zunanji informacijski sistemi so evidentirani	COBIT 5 APO02.02, APO10.04, DSS01.02; ISO/IEC 27001:2013 A.11.2.6
		ID.AM-5	ID.AM-5: Viri (npr. strojna oprema, naprave, podatki, čas, osebje in programska oprema) so razvrščeni glede na njihovo klasifikacijo, kritičnost in poslovno vrednost	COBIT 5 APO03.03, APO03.04, APO12.01, BAI04.02, BAI09.02; ISO/IEC 27001:2013 A.8.2.1
		ID.AM-6	ID.AM-6: Vloge in odgovornosti kibernetske varnosti za vse zaposlene in zunanje deležnike (npr. dobavitelji, kupci, partnerji) so določene	COBIT 5 APO01.02, APO07.06, APO13.01, DSS06.03; ISO/IEC 27001:2013 A.6.1.1
	Poslovno okolje (ID.BE): poslanstvo, cilji, zainteresirane strani in dejavnosti organizacije so razumljeni in prednostni; te informacije se uporabljajo za obveščanje o vlogah, odgovornostih in odločitvah na področju kibernetske varnosti.	ID.BE-1	ID.BE-1: Vloga organizacije je opredeljena in komunicirana	COBIT 5 APO08.01, APO08.04, APO08.05, APO10.03, APO10.04, APO10.05; ISO/IEC 27001:2013 A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2
		ID.BE-2	ID.BE-2: Prepozna se in sporoči se mesto organizacije v kritični infrastrukturi in njenem industrijskem sektorju	COBIT 5 APO02.06, APO03.01; ISO/IEC 27001:2013 Določilo 4.1
		ID.BE-3	ID.BE-3: Vzpostavljene in komunicirane so prednostne naloge organizacijskega poslanstva, cilji in dejavnosti	COBIT 5 APO02.01, APO02.06, APO03.01

Funkcija	Kategorija	Oznaka	Podkategorija	Povezava na Cobit, ISO 27001
		ID.BE-4	ID.BE-4: Vzpostavljene so odvisnosti in kritične funkcije za zagotavljanje kritičnih storitev	COBIT 5 APO10.01, BAI04.02, BAI09.02; ISO/IEC 27001:2013 A.11.2.2, A.11.2.3, A.12.1.3
		ID.BE-5	ID.BE-5: Zahteve za odpornost, ki podpirajo zagotavljanje kritičnih storitev, so določene za vsa stanja delovanja	COBIT 5 BAI03.02, DSS04.02; ISO/IEC 27001:2013 A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1
	Upravljanje (ID.GV): Politike, postopki in procesi za upravljanje in spremljanje regulativnih, pravnih, tveganih, okoljskih in operativnih zahtev organizacije so razumljivi in obveščajo o obvladovanju tveganj kibernetske varnosti.	ID.GV-1	ID.GV-1: Organizacijska politika kibernetske varnosti je vzpostavljena in sporočena	COBIT 5 APO01.03, APO13.01, EDM01.01, EDM01.02; ISO/IEC 27001:2013 A.5.1.1
		ID.GV-2	ID.GV-2: Vloge in odgovornosti kibernetske varnosti so usklajene in usklajene z notranjimi vlogami in zunanjimi partnerji	COBIT 5 APO01.02, APO10.03, APO13.02, DSS05.04; ISO/IEC 27001:2013 A.6.1.1, A.7.2.1, A.15.1.1
		ID.GV-3	ID.GV-3: Zakonske in regulativne zahteve glede kibernetske varnosti, vključno glede zasebnosti, so razumljene in upravljane	COBIT 5 BAI02.01, MEA03.01, MEA03.04; ISO/IEC 27001:2013 A.18.1.1, A.18.1.2, A.18.1.3, A.18.1.4, A.18.1.5
		ID.GV-4	ID.GV-4: Procesi upravljanja in obvladovanja tveganj obravnavajo tveganja kibernetske varnosti	COBIT 5 EDM03.02, APO12.02, APO12.05, DSS04.02; ISO/IEC 27001:2013 Določilo 6
	Ocena tveganja (ID.RA): Organizacija razume tveganje kibernetske varnosti za organizacijske operacije (vključno s poslanstvom, funkcijami, podobo ali ugledom), organizacijskimi sredstvi in posamezniki.	ID.RA-1	ID.RA-1: Ranljivosti sredstev so prepoznane in dokumentirane	COBIT 5 APO12.01, APO12.02, APO12.03, APO12.04, DSS05.01, DSS05.02; ISO/IEC 27001:2013 A.12.6.1, A.18.2.3
		ID.RA-2	ID.RA-2: Obveščanje o kibernetskih grožnjah prek kanalov za izmenjavo informacij	COBIT 5 BAI08.01; ISO/IEC 27001:2013 A.6.1.4
		ID.RA-3	ID.RA-3: Ugotovljene in dokumentirane so tveganja, tako notranja kot zunanja	COBIT 5 APO12.01, APO12.02, APO12.03, APO12.04; ISO/IEC 27001:2013 določilo 6.1.2
		ID.RA-4	ID.RA-4: Ugotovljeni so potencialni poslovni vplivi in verjetnosti	COBIT 5 DSS04.02; ISO/IEC 27001:2013 A.16.1.6, Določilo 6.1.2

Funkcija	Kategorija	Oznaka	Podkategorija	Povezava na Cobit, ISO 27001
		ID.RA-5	ID.RA-5: Ocenjevanje tveganj se izvaja	COBIT 5 APO12.02; ISO/IEC 27001:2013 A.12.6.1
		ID.RA-6	ID.RA-6: Odzivi na tveganja so opredeljeni in prednostni	COBIT 5 APO12.05, APO13.02; ISO/IEC 27001:2013 Določilo 6.1.3
	Strategija upravljanja s tveganji (ID.RM): Prednostne naloge, omejitve, tolerance in predpostavke organizacije so določene in uporabljene v podporo odločitvam o operativnem tveganju.	ID.RM-1	ID.RM-1: Organizacijske zainteresirane strani vzpostavijo, upravljajo in se dogovorijo o procesih upravljanja tveganj	COBIT 5 APO12.04, APO12.05, APO13.02, BAI02.03, BAI04.02 ; ISO/IEC 27001:2013 Določilo 6.1.3, Določilo 8.3, Določilo 9.3
		ID.RM-2	ID.RM-2: Raven sprejemanja tveganj je določena in jasno izraženo	COBIT 5 APO12.06; ISO/IEC 27001:2013 Določilo 6.1.3, Določilo 8.3
		ID.RM-3	ID.RM-3: Organizacija o določitvi tolerance za tveganje temelji na njeni vlogi v kritični infrastrukturi in analizi tveganj za posamezne sektorje	COBIT 5 APO12.02; ISO/IEC 27001:2013 Določilo 6.1.3, Določilo 8.3
	Obvladovanje tveganja dobavne verige (ID.SC): Prednostne naloge, omejitve, tolerance in predpostavke organizacije so določene in se uporabljajo za podporo odločitvam o tveganjih, povezanih z obvladovanjem tveganja v dobavni verigi. Organizacija je vzpostavila in izvaja postopke za ugotavljanje, ocenjevanje in upravljanje tveganj v dobavni verigi.	ID.SC-1	ID.SC-1: Proces upravljanja kibernetskih tveganj je vzpostavljen	COBIT 5 APO10.01, APO10.04, APO12.04, APO12.05, APO13.02, BAI01.03, BAI02.03, BAI04.02; ISO/IEC 27001:2013 A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2
		ID.SC-2	ID.SC-2: Dobavitelji in zunanji partnerji informacijskih sistemov, komponent in storitev se identificirajo, razvrstijo in ocenijo s pomočjo postopka ocene tveganja	COBIT 5 APO10.01, APO10.02, APO10.04, APO10.05, APO12.01, APO12.02, APO12.03, APO12.04, APO12.05, APO12.06, APO13.02, BAI02.03; ISO/IEC 27001:2013 A.15.2.1, A.15.2.2
		ID.SC-3	ID.SC-3: Pogodbe z dobavitelji in neodvisnimi partnerji se uporabljajo za izvajanje ustreznih ukrepov, namenjenih izpolnjevanju ciljev programa kibernetske varnosti organizacije in načrta za obvladovanje tveganj v kibernetski dobavni verigi.	COBIT 5 APO10.01, APO10.02, APO10.03, APO10.04, APO10.05; ISO/IEC 27001:2013 A.15.1.1, A.15.1.2, A.15.1.3

Funkcija	Kategorija	Oznaka	Podkategorija	Povezava na Cobit, ISO 27001
		ID.SC-4	ID.SC-4: Dobavitelji in neodvisni partnerji se redno ocenjujejo z uporabo revizij, rezultatov preskusov ali drugih oblik ocenjevanja, da se potrdi, da izpolnjujejo svoje pogodbene obveznosti.	COBIT 5 APO10.01, APO10.03, APO10.04, APO10.05, MEA01.01, MEA01.02, MEA01.03, MEA01.04, MEA01.05 ; ISO/IEC 27001:2013 A.15.2.1, A.15.2.2
		ID.SC-5	ID.SC-5: Načrtovanje in preskušanje odzivov in izterjave se izvaja z dobavitelji in neodvisnimi ponudniki	COBIT 5 DSS04.04; ISO/IEC 27001:2013 A.17.1.3
Ščitenje (PR)	Upravljanje identitete, preverjanje pristnosti in nadzor dostopa (PR.AC): Dostop do fizičnih in logičnih sredstev in pripadajočih naprav je omejen na pooblaščene uporabnike, procese in naprave ter se upravlja skladno z ocenjeno nevarnostjo nepooblaščenega dostopa do pooblaščenih dejavnosti in transakcij.	PR.AC-1	PR.AC-1: Identitete in poverilnice so izdane, upravljane, preverjene, preklicane in revidirane za pooblaščene naprave, uporabnike in procese	COBIT 5 DSS05.04, DSS06.03; ISO/IEC 27001:2013 A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.4, A.9.2.6, A.9.3.1, A.9.4.2, A.9.4.3
		PR.AC-2	PR.AC-2: Fizični dostop do sredstev se upravlja in varuje	COBIT 5 DSS01.04, DSS05.05; ISO/IEC 27001:2013 A.11.1.1, A.11.1.2, A.11.1.3, A.11.1.4, A.11.1.5, A.11.1.6, A.11.2.1, A.11.2.3, A.11.2.5, A.11.2.6, A.11.2.7, A.11.2.8
		PR.AC-3	PR.AC-3: Upravljan je oddaljeni dostop	COBIT 5 APO13.01, DSS01.04, DSS05.03; ISO/IEC 27001:2013 A.6.2.1, A.6.2.2, A.11.2.6, A.13.1.1, A.13.2.1
		PR.AC-4	PR.AC-4: Upravljanje dovoljenj in dovoljenj za dostop vključuje načela najmanjših privilegijev in ločitve nalog	COBIT 5 DSS05.04; ISO/IEC 27001:2013 A.6.1.2, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5
		PR.AC-5	PR.AC-5: Celovitost omrežja je zaščitena (npr. segmentacija omrežja)	COBIT 5 DSS01.05, DSS05.02; ISO/IEC 27001:2013 A.13.1.1, A.13.1.3, A.13.2.1, A.14.1.2, A.14.1.3
		PR.AC-6	PR.AC-6: Identitete so preverjene in vezane na poverilnice ter uveljavljene v interakcijah	COBIT 5 DSS05.04, DSS05.05, DSS05.07, DSS06.03 ; ISO/IEC 27001:2013, A.7.1.1, A.9.2.1

Funkcija	Kategorija	Oznaka	Podkategorija	Povezava na Cobit, ISO 27001
		PR.AC-7	PR.AC-7: preverjanje pristnosti uporabnikov, naprav in drugih sredstev (npr. Enofaktorski, večfaktorski) je sorazmeren s tveganjem transakcije (npr. Varnostna in zasebna tveganja posameznikov ter druga organizacijska tveganja)	COBIT 5 DSS05.04, DSS05.10, DSS06.10; ISO/IEC 27001:2013 A.9.2.1, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3, A.18.1.4
	Ozaveščanje in usposabljanje (PR.AT): Osebje in partnerji organizacije dobijo izobraževanje o ozaveščanju o kibernetski varnosti in so usposobljeni za izvajanje nalog in odgovornosti, povezanih s kibernetsko varnostjo, v skladu s povezanimi politikami, postopki in dogovori.	PR.AT-1	PR.AT-1: Vsi uporabniki so obveščeni in usposobljeni	COBIT 5 APO07.03, BAI05.07; ISO/IEC 27001:2013 A.7.2.2, A.12.2.1
		PR.AT-2	PR.AT-2: privilegirani uporabniki razumejo svoje vloge in odgovornosti	COBIT 5 APO07.02, DSS05.04, DSS06.03; ISO/IEC 27001:2013 A.6.1.1, A.7.2.2
		PR.AT-3	PR.AT-3: Tretje zainteresirane strani (npr. Dobavitelji, kupci, partnerji) razumejo svoje vloge in odgovornosti	COBIT 5 APO07.03, APO07.06, APO10.04, APO10.05; ISO/IEC 27001:2013 A.6.1.1, A.7.2.1, A.7.2.2
		PR.AT-4	PR.AT-4: Vodstveni delavci razumejo svoje vloge in odgovornosti	COBIT 5 EDM01.01, APO01.02, APO07.03; ISO/IEC 27001:2013 A.6.1.1, A.7.2.2
		PR.AT-5	PR.AT-5: Osebje za fizično in kibernetsko varnost razume svoje vloge in odgovornosti	COBIT 5 APO07.03; ISO/IEC 27001:2013 A.6.1.1, A.7.2.2
	Varnost podatkov (PR.DS): Informacije in zapisi (podatki) se upravljajo skladno s strategijo tveganja organizacije za zaščito zaupnosti, celovitosti in razpoložljivosti informacij.	PR.DS-1	PR.DS-1: Podatki hrambi (arhivi) so zaščiteni	COBIT 5 APO01.06, BAI02.01, BAI06.01, DSS04.07, DSS05.03, DSS06.06; ISO/IEC 27001:2013 A.8.2.3
		PR.DS-2	PR.DS-2: Podatki med prenosom so zaščiteni	COBIT 5 APO01.06, DSS05.02, DSS06.06; ISO/IEC 27001:2013 A.8.2.3, A.13.1.1, A.13.2.1, A.13.2.3, A.14.1.2, A.14.1.3
		PR.DS-3	PR.DS-3: Sredstva se formalno upravljajo med odstranjevanjem, prenosom in odlaganjem	COBIT 5 BAI09.03; ISO/IEC 27001:2013 A.8.2.3, A.8.3.1, A.8.3.2, A.8.3.3, A.11.2.5, A.11.2.7

Funkcija	Kategorija	Oznaka	Podkategorija	Povezava na Cobit, ISO 27001
		PR.DS-4	PR.DS-4: Vzdrževanje ustrezne zmogljivosti za zagotovitev razpoložljivosti	COBIT 5 APO13.01, BAI04.04; ISO/IEC 27001:2013 A.12.1.3, A.17.2.1
		PR.DS-5	PR.DS-5: Izvedena je zaščita pred uhajanjem podatkov	COBIT 5 APO01.06, DSS05.04, DSS05.07, DSS06.02; ISO/IEC 27001:2013 A.6.1.2, A.7.1.1, A.7.1.2, A.7.3.1, A.8.2.2, A.8.2.3, A.9.1.1, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5, A.10.1.1, A.11.1.4, A.11.1.5, A.11.2.1, A.13.1.1, A.13.1.3, A.13.2.1, A.13.2.3, A.13.2.4, A.14.1.2, A.14.1.3
		PR.DS-6	PR.DS-6: Mehanizmi preverjanja integritete se uporabljajo za preverjanje programske opreme, vdelane programske opreme in celovitosti informacij	COBIT 5 APO01.06, BAI06.01, DSS06.02; ISO/IEC 27001:2013 A.12.2.1, A.12.5.1, A.14.1.2, A.14.1.3, A.14.2.4
		PR.DS-7	PR.DS-7: Razvojno (-a) okolje (-a) za preskušanje je ločeno od proizvodnega okolja	COBIT 5 BAI03.08, BAI07.04; ISO/IEC 27001:2013 A.12.1.4
		PR.DS-8	PR.DS-8: Za preverjanje celovitosti strojne opreme se uporabljajo mehanizmi za preverjanje integritete	COBIT 5 BAI03.05; ISO/IEC 27001:2013 A.11.2.4
	Procesi in postopki za zaščito informacij (PR.IP): Varnostne politike (ki obravnavajo namen, obseg, vloge, odgovornosti, zavezanost k upravljanju in usklajevanje med organizacijskimi enotami), procesi in postopki se vzdržujejo in uporabljajo za upravljanje zaščite informacijskih sistemov in sredstev .	PR.IP-1	PR.IP-1: Ustvari se in vzdržuje osnovna konfiguracija informacijske tehnologije / industrijskih nadzornih sistemov, ki vključuje varnostna načela (npr. Koncept najmanjše funkcionalnosti)	COBIT 5 BAI10.01, BAI10.02, BAI10.03, BAI10.05; ISO/IEC 27001:2013 A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4
		PR.IP-2	PR.IP-2: Izveden je življenjski cikel razvoja sistema za upravljanje sistemov	COBIT 5 APO13.01, BAI03.01, BAI03.02, BAI03.03; ISO/IEC 27001:2013 A.6.1.5, A.14.1.1, A.14.2.1, A.14.2.5
		PR.IP-3	PR.IP-3: Vzpostavljeni so postopki za nadzor sprememb konfiguracije	COBIT 5 BAI01.06, BAI06.01; ISO/IEC 27001:2013 A.12.1.2,

Funkcija	Kategorija	Oznaka	Podkategorija	Povezava na Cobit, ISO 27001
				A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4
		PR.IP-4	PR.IP-4: Varnostne kopije informacij se izvajajo, vzdržujejo in preizkušajo	COBIT 5 APO13.01, DSS01.01, DSS04.07 ; ISO/IEC 27001:2013 A.12.3.1, A.17.1.2, A.17.1.3, A.18.1.3
		PR.IP-5	PR.IP-5: Izpolnjeni so pravilniki in predpisi glede fizičnega okolja za organizacijska sredstva	COBIT 5 DSS01.04, DSS05.05; ISO/IEC 27001:2013 A.11.1.4, A.11.2.1, A.11.2.2, A.11.2.3
		PR.IP-6	PR.IP-6: Podatki se uničijo v skladu s politiko	COBIT 5 BAI09.03, DSS05.06; ISO/IEC 27001:2013 A.8.2.3, A.8.3.1, A.8.3.2, A.11.2.7
		PR.IP-7	PR.IP-7: Dopolnjevanje zaščitnih procesov	COBIT 5 APO11.06, APO12.06, DSS04.05; ISO/IEC 27001:2013 A.16.1.6, Določilo 9, Določilo 10
		PR.IP-8	PR.IP-8: Učinkovitost zaščitnih tehnologij	COBIT 5 BAI08.04, DSS03.04; ISO/IEC 27001:2013 A.16.1.6
		PR.IP-9	PR.IP-9: Načrti odzivanja (odziv na nezgode in neprekinjeno poslovanje) in načrti obnove (obnova incidentov in nesreče) so vzpostavljeni in se upravljajo	COBIT 5 APO12.06, DSS04.03; ISO/IEC 27001:2013 A.16.1.1, A.17.1.1, A.17.1.2, A.17.1.3
		PR.IP-10	PR.IP-10: Preizkušeni so načrti odziva in obnovitve	COBIT 5 DSS04.04; ISO/IEC 27001:2013 A.17.1.3
		PR.IP-11	PR.IP-11: Kibernetska varnost je vključena v prakse v zvezi s človeškimi viri (npr. odstranjevanje pravic, pregled osebja)	COBIT 5 APO07.01, APO07.02, APO07.03, APO07.04, APO07.05; ISO/IEC 27001:2013 A.7.1.1, A.7.1.2, A.7.2.1, A.7.2.2, A.7.2.3, A.7.3.1, A.8.1.4
		PR.IP-12	PR.IP-12: Načrt za obvladovanje ranljivosti je razvit in izveden	COBIT 5 BAI03.10, DSS05.01, DSS05.02; ISO/IEC 27001:2013 A.12.6.1, A.14.2.3, A.16.1.3, A.18.2.2, A.18.2.3

Funkcija	Kategorija	Oznaka	Podkategorija	Povezava na Cobit, ISO 27001
	Vzdrževanje (PR.MA): Vzdrževanje in popravila komponent industrijskega nadzornega in informacijskega sistema se izvajajo v skladu s politikami in postopki.	PR.MA-1	PR.MA-1: Vzdrževanje in popravila organizacijskih sredstev se izvajajo in beležijo z odobrenimi in nadzorovanimi orodji	COBIT 5 BAI03.10, BAI09.02, BAI09.03, DSS01.05; ISO/IEC 27001:2013 A.11.1.2, A.11.2.4, A.11.2.5, A.11.2.6
		PR.MA-2	PR.MA-2: Oddaljeno vzdrževanje organizacijskih sredstev je odobreno, zapisano in izvedeno na način, ki preprečuje nepooblaščen dostop	COBIT 5 DSS05.04; ISO/IEC 27001:2013 A.11.2.4, A.15.1.1, A.15.2.1
	Zaščitna tehnologija (PR.PT): Tehnične varnostne rešitve se upravljajo, da se zagotovi varnost in odpornost sistemov in sredstev v skladu s povezanimi politikami, postopki in dogovori.	PR.PT-1	PR.PT-1: Revizijski sledi (logi) so vzpostavljeni, se dokumentirajo, izvajajo in pregledujejo v skladu s politiko	COBIT 5 APO11.04, BAI03.05, DSS05.04, DSS05.07, MEA02.01; ISO/IEC 27001:2013 A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.12.7.1
		PR.PT-2	PR.PT-2: Odstranljivi mediji so zaščiteni in njegova uporaba omejena v skladu s politiko	COBIT 5 APO13.01, DSS05.02, DSS05.06 ; ISO/IEC 27001:2013 A.8.2.1, A.8.2.2, A.8.2.3, A.8.3.1, A.8.3.3, A.11.2.9
		PR.PT-3	PR.PT-3: Načelo najmanjše funkcionalnosti je vključeno s konfiguriranjem sistemov, ki zagotavljajo samo bistvene zmogljivosti	COBIT 5 DSS05.02, DSS05.05, DSS06.06; ISO/IEC 27001:2013 A.9.1.2
		PR.PT-4	PR.PT-4: Komunikacijska in nadzorna omrežja so zaščitena	COBIT 5 DSS05.02, APO13.01; ISO/IEC 27001:2013 A.13.1.1, A.13.2.1, A.14.1.3
		PR.PT-5	PR.PT-5: Za doseganje zahtev glede odpornosti v običajnih in neugodnih razmerah se uporabljajo mehanizmi (npr. Varni pred napakami, uravnoteženje bremena, vroča zamenjava).	COBIT 5 BAI04.01, BAI04.02, BAI04.03, BAI04.04, BAI04.05, DSS01.05; ISO/IEC 27001:2013 A.17.1.2, A.17.2.1
Zaznava (DE)	Anomalije in dogodki (DE.AE): zaznajo se nepravilne aktivnosti in razume potencialni vpliv dogodkov.	DE.AE-1	DE.AE-1: Vzpostavljena in upravljana je osnova omrežnih operacij in pričakovanih podatkovnih tokov za uporabnike in sisteme	COBIT 5 DSS03.01; ISO/IEC 27001:2013 A.12.1.1, A.12.1.2, A.13.1.1, A.13.1.2
		DE.AE-2	DE.AE-2: Zaznani dogodki se analizirajo, da bi razumeli cilje in metode napada	COBIT 5 DSS05.07; ISO/IEC 27001:2013 A.12.4.1, A.16.1.1, A.16.1.4

Funkcija	Kategorija	Oznaka	Podkategorija	Povezava na Cobit, ISO 27001
		DE.AE-3	DE.AE-3: Podatki o dogodkih se zbirajo in povezujejo iz več virov in senzorjev	COBIT 5 BAI08.02; ISO/IEC 27001:2013 A.12.4.1, A.16.1.7
		DE.AE-4	DE.AE-4: Učinek dogodkov je določen	COBIT 5 APO12.06, DSS03.01; ISO/IEC 27001:2013 A.16.1.4
		DE.AE-5	DE.AE-5: Določeni so pragovi za opozarjanje na nesreče	COBIT 5 APO12.06, DSS03.01; ISO/IEC 27001:2013 A.16.1.4
	Varnostno stalno spremljanje (DE.CM): Nadzirajo se informacijski sistem in sredstva, da se ugotovijo kibernetski dogodki in preveri učinkovitost zaščitnih ukrepov.	DE.CM-1	DE.CM-1: Omrežje se spremlja, da zazna morebitne dogodke kibernetske varnosti	COBIT 5 DSS01.03, DSS03.05, DSS05.07
		DE.CM-2	DE.CM-2: Nadzira se fizično okolje, da se zaznajo morebitni dogodki kibernetske varnosti	COBIT 5 DSS01.04, DSS01.05; ISO/IEC 27001:2013 A.11.1.1, A.11.1.2
		DE.CM-3	DE.CM-3: Nadzira se dejavnost osebja, da se odkrijejo morebitni dogodki kibernetske varnosti	COBIT 5 DSS05.07; ISO/IEC 27001:2013 A.12.4.1, A.12.4.3
		DE.CM-4	DE.CM-4: Zaznana je zlonamerna koda	COBIT 5 DSS05.01; ISO/IEC 27001:2013 A.12.2.1
		DE.CM-5	DE.CM-5: Zaznana je nepooblaščena mobilna koda	COBIT 5 DSS05.01; ISO/IEC 27001:2013 A.12.5.1, A.12.6.2
		DE.CM-6	DE.CM-6: Nadzira se dejavnost zunanjih ponudnikov storitev, da se odkrijejo morebitni dogodki kibernetske varnosti	COBIT 5 APO07.06, APO10.05; ISO/IEC 27001:2013 A.14.2.7, A.15.2.1
		DE.CM-7	DE.CM-7: Izvaja se nadzor nepooblaščenega osebja, povezav, naprav in programske opreme	COBIT 5 DSS05.02, DSS05.05; ISO/IEC 27001:2013 A.12.4.1, A.14.2.7, A.15.2.1
		DE.CM-8	DE.CM-8: Izvedejo se skeniranja ranljivosti	COBIT 5 BAI03.10, DSS05.01; ISO/IEC 27001:2013 A.12.6.1
	Procesi zaznavanja (DE.DP): postopki in postopki zaznavanja se vzdržujejo in preizkušajo, da se zagotovi zavedanje o nepravilnih dogodkih.	DE.DP-1	DE.DP-1: Vloge in odgovornosti za odkrivanje so natančno opredeljene, da se zagotovi odgovornost	COBIT 5 APO01.02, DSS05.01, DSS06.03; ISO/IEC 27001:2013 A.6.1.1, A.7.2.2
		DE.DP-2	DE.DP-2: Dejavnosti odkrivanja izpolnjujejo vse veljavne zahteve	COBIT 5 DSS06.01, MEA03.03, MEA03.04; ISO/IEC 27001:2013 A.18.1.4, A.18.2.2, A.18.2.3

Funkcija	Kategorija	Oznaka	Podkategorija	Povezava na Cobit, ISO 27001
		DE.DP-3	DE.DP-3: testirani so postopki zaznavanja	COBIT 5 APO13.02, DSS05.02; ISO/IEC 27001:2013 A.14.2.8
		DE.DP-4	DE.DP-4: sporočajo se informacije o zaznavanju dogodkov	COBIT 5 APO08.04, APO12.06, DSS02.05; ISO/IEC 27001:2013 A.16.1.2, A.16.1.3
		DE.DP-5	DE.DP-5: Postopki zaznavanja se nenehno izboljšujejo	COBIT 5 APO11.06, APO12.06, DSS04.05; ISO/IEC 27001:2013 A.16.1.6
Odziv (RS)	Načrtovanje odzivov (RS.RP): Odzivni procesi in postopki se izvajajo in vzdržujejo, da se zagotovi odziv na zaznane incidente kibernetske varnosti.	RS.RP-1	RS.RP-1: Načrt odziva se izvede med incidentom ali po njem	COBIT 5 APO12.06, BAI01.10; ISO/IEC 27001:2013 A.16.1.5
	Komunikacije (RS.CO): odzivne dejavnosti se usklajujejo z notranjimi in zunanjimi zainteresiranimi stranmi (npr. Zunanja podpora organov pregona).	RS.CO-1	RS.CO-1: Osebje pozna svoje vloge in vrstni red operacij, kadar je potreben odziv	COBIT 5 EDM03.02, APO01.02, APO12.03; ISO/IEC 27001:2013 A.6.1.1, A.7.2.2, A.16.1.1
		RS.CO-2	RS.CO-2: Poročajo o incidentih v skladu z uveljavljenimi merili	COBIT 5 DSS01.03; ISO/IEC 27001:2013 A.6.1.3, A.16.1.2
		RS.CO-3	RS.CO-3: izmenjava informacij poteka v skladu z načrti odzivanja	COBIT 5 DSS03.04; ISO/IEC 27001:2013 A.16.1.2, Določilo 7.4, Določilo 16.1.2
		RS.CO-4	RS.CO-4: Usklajevanje z zainteresiranimi stranmi poteka skladno z načrti odzivanja	COBIT 5 DSS03.04; ISO/IEC 27001:2013 Določilo 7.4
		RS.CO-5	RS.CO-5: Prostovoljna izmenjava informacij poteka z zunanjimi zainteresiranimi stranmi, da se doseže širše ozaveščanje o kibernetski varnosti	COBIT 5 BAI08.04; ISO/IEC 27001:2013 A.6.1.4
	Analiza (RS.AN): Analiza se izvaja za zagotovitev učinkovitega odzivanja in podporo okrevanju.	RS.AN-1	RS.AN-1: Preučujejo se obvestila sistemov za odkrivanje	COBIT 5 DSS02.04, DSS02.07; ISO/IEC 27001:2013 A.12.4.1, A.12.4.3, A.16.1.5
		RS.AN-2	RS.AN-2: Vpliv incidenta je razumljen	COBIT 5 DSS02.02; ISO/IEC 27001:2013 A.16.1.4, A.16.1.6

Funkcija	Kategorija	Oznaka	Podkategorija	Povezava na Cobit, ISO 27001
		RS.AN-3	RS.AN-3: Izvajajo se forenzični pregledi	COBIT 5 APO12.06, DSS03.02, DSS05.07; ISO/IEC 27001:2013 A.16.1.7
		RS.AN-4	RS.AN-4: Incidenti so razvrščeni v skladu z načrti odzivanja	COBIT 5 DSS02.02; ISO/IEC 27001:2013 A.16.1.4
		RS.AN-5	RS.AN-5: Vzpostavljeni so procesi za sprejemanje, analizo in odzivanje na ranljivosti, ki jih organizacija razkrije iz notranjih in zunanjih virov (npr. Notranje preskušanje, varnostni bilteni ali raziskovalci varnosti).	COBIT 5 EDM03.02, DSS05.07
	Blažitev (RS.MI): Izvajajo se dejavnosti za preprečevanje razširitve dogodka, ublažitev njegovih učinkov in reševanje incidenta.	RS.MI-1	RS.MI-1: Incidenti so obvladovani	COBIT 5 APO12.06; ISO/IEC 27001:2013 A.12.2.1, A.16.1.5
		RS.MI-2	RS.MI-2: Incidenti so ublaženi	COBIT 5 APO12.06; ISO/IEC 27001:2013 A.12.2.1, A.16.1.5
		RS.MI-3	RS.MI-3: Novo odkrite ranljivosti se ublažijo ali dokumentirajo kot sprejeta tveganja	COBIT 5 APO12.06; ISO/IEC 27001:2013 A.12.6.1
	Izboljšave (RS.IM): Aktivnosti organizacijskega odzivanja se izboljšajo z vključevanjem izkušenj iz sedanjih in prejšnjih dejavnosti odkrivanja / odzivanja.	RS.IM-1	RS.IM-1: Načrti odzivov vključujejo pridobljene izkušnje	COBIT 5 BAI01.13; ISO/IEC 27001:2013 A.16.1.6, Določilo 10
		RS.IM-2	RS.IM-2: Posodobljene strategije odzivanja	COBIT 5 BAI01.13, DSS04.08; ISO/IEC 27001:2013 A.16.1.6, Določilo 10
Okrevanje (RC)	Načrtovanje izterjave (RC.RP): Izvajajo se in vzdržujejo postopki in postopki izterjave, ki zagotavljajo obnovo sistemov ali sredstev, ki jih prizadenejo kibernetske varnosti.	RC.RP-1	RC.RP-1: Načrt obnovitve se izvede med incidentom kibernetske varnosti ali po njem	COBIT 5 APO12.06, DSS02.05, DSS03.04; ISO/IEC 27001:2013 A.16.1.5
	Izboljšave (RC.IM): Načrtovanje in procesi okrevanja se izboljšajo z vključitvijo pridobljenih spoznanj v prihodnje dejavnosti.	RC.IM-1	RC.IM-1: Načrti za obnovo vključujejo pridobljene izkušnje	COBIT 5 APO12.06, BAI05.07, DSS04.08; ISO/IEC 27001:2013 A.16.1.6, Določilo 10
		RC.IM-2	RC.IM-2: Strategije obnovitve so posodobljene	COBIT 5 APO12.06, BAI07.08; ISO/IEC 27001:2013 A.16.1.6, Določilo 10

Funkcija	Kategorija	Oznaka	Podkategorija	Povezava na Cobit, ISO 27001
	Komunikacije (RC.CO): Obnovitvene dejavnosti se usklajujejo z notranjimi in zunanjimi stranmi (npr. Centri za usklajevanje, ponudniki internetnih storitev, lastniki napadalnih sistemov, žrtve, drugi CSIRT-ji in prodajalci).	RC.CO-1	RC.CO-1: Upravljajo se odnosi z javnostmi	COBIT 5 EDM03.02; ISO/IEC 27001:2013 A.6.1.4, Določilo 7.4
		RC.CO-2	RC.CO-2: Izvedba ukrepov za izboljšanje uglede	COBIT 5 MEA03.02; ISO/IEC 27001:2013 Določilo 7.4
		RC.CO-3	RC.CO-3: Dejavnosti okrevanja se komunicirajo notranjim in zunanjim zainteresiranim stranem ter izvršnim in vodstvenim skupinam	COBIT 5 APO12.06; ISO/IEC 27001:2013 Določilo 7.4

Priloga 7: Delovni papir

Zaupno
DELOVNI PAPIR

BANKA D.D.

Revizija: Kibernetska varnost (RP-2021-03)	**Oznaka D.p.:** B.07.01
Pripravil: Milan Osterman, 9.2.2021	
Pregledal: Vodja službe notranje revizije	
Revizijski cilj: Skladnost z zakonodajo ter predpisi Zakonodajne zahteve in predpisi so prepoznane in ustrezno upravljane.	
Sodila: Upoštevana metodologija: - NIST v. 1.1 - Cobit 2019, Cobit 5 - ISO/IEC 27001:2013 Zakonodaja, podzakonski akti in predpisi Banke Slovenije: - Zakon o bančništvu (ZBan-2; (Uradni list RS, št. 25/15, 44/16 – ZRPPB, 77/16 – ZCKR, 41/17, 77/18 – ZTFI-1, 22/19 – ZIUDSOL in 44/19 – odl. US); 13.5.2015 - Sklep o ureditvi notranjega upravljanja, upravljalnem organu in procesu ocenjevanja ustreznega notranjega kapitala za banke in hranilnice (Uradni list RS, št. 73/15, 49/16, 68/17, 33/18, 81/18 in 45/19); veljavnost od 30.11.2015 - Zakon o informacijski varnosti (Uradni list RS, št. 30/18); veljavnost od 11.5.2018 - Sklep o uporabi Smernic o poročanju o večjih incidentih v skladu z Direktivo (EU) 2015/2366 (PSD2) (Uradni list RS, št. 11/18); veljavnost od 2.3.2018 - Smernice EBA o upravljanju tveganj, povezanih z IKT in varnostjo (EBA/GL/2019/04), Sklep o uporabi Smernic o upravljanju tveganj, povezanih z IKT in varnostjo (Uradni list RS, št. 52/20); veljavnost od 30.6.2020 - Zakon o varstvu osebnih podatkov (ZVOP-1), veljavnost od 1.1.2005 - GDPR, UREDBA (EU) 2016/679 EVROPSKEGA PARLAMENTA IN SVETA z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES (Splošna uredba o varstvu podatkov) Interni akti: - Varnostna politika, - Pravilnikom o obravnavi in poročanju varnostnih dogodkov, - Pravilnikom o načrtu neprekinjenega poslovanja, - Pravilnikom o upravljanju pravic in dostopov do informacijskih sistemov banke, - Pravilnikom o upravljanju sistemov in omrežja banke, - Pravilnikom o upravljanju revizijskih sledi, - Pravilnikom o uporabi IKT opreme in dostopih, - Pravilnikom o skrbništvu sistemov, poročil in podatkov, - Navodilom za izdelavo varnostnih kopij in arhiviranje.	

Izvedeni revizijski postopki:
Revizijski postopki se nanašajo na preveritve, da so zakonodajne zahteve spremljajo, prepoznajo in ustrezno implementirajo (NIST kategorija ID.GV-3: Zakonske in regulativne zahteve glede kibernetske varnosti, vključno glede zasebnosti, so razumljene in upravljane).

Pri tem so bile smiselno upoštevane naslednje zahteve:
- Cobit 5, BAI02.01 (Cobit 2019: BAI02.01)
- Cobit 5, MEA03.01 (Cobit 2019: MEA03.01)
- Cobit 5, MEA03.04 (Cobit 2019: MEA03.04)
- ISO/IEC 27001:2013, A.18.1.1
- ISO/IEC 27001:2013, A.18.1.2
- ISO/IEC 27001:2013, A.18.1.3
- ISO/IEC 27001:2013, A.18.1.4
- ISO/IEC 27001:2013, A.18.1.5

Izvedeni so bili sledeči revizijski postopki:
- Ali so postopki za spremljanje in implementacijo zakonodaje vezani na kibernetsko varnost ustrezno vzpostavljeni in izvajani ter odgovornosti določene
    - Preveri, ali je področje kibernetske varnosti vključeno v proces spremljave in implementacijo zakonodaje v banki
    - Preveri odgovornosti za spremljanje in implementacijo zakonodaje
    - Iz orodja R1 za spremljanje skladnosti z zakonodajo izpiši zakonodajo za področje informacijsko varnosti (najmanj Zakon o bančništvu (ZBan-2), Sklep o ureditvi notranjega upravljanja, upravljalnem organu in procesu ocenjevanja ustreznega notranjega kapitala za banke in hranilnice, Zakon o informacijski varnosti, Sklep o uporabi Smernic o poročanju o večjih incidentih v skladu z Direktivo (EU) 2015/2366 (PSD2), Smernice EBA o upravljanju tveganj, povezanih z IKT in varnostjo (EBA/GL/2019/04), Sklep o uporabi Smernic o upravljanju tveganj, povezanih z IKT in varnostjo, Zakon o varstvu osebnih podatkov (ZVOP-1), UREDBA (EU) 2016/679 EVROPSKEGA PARLAMENTA IN SVETA z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES (Splošna uredba o varstvu podatkov)) ter preveri implementacijo v banki ter oceni stopnjo skladnosti. Preveri sledenje spremembam, regulatornim in pravnim, ali so postopki ustrezno vzpostavljeni in izvajani, ali so spremembe pravočasno identificirane, vpeljane in potrjene
    - Opravi razgovor z odgovornimi za kibernetsko varnost (vodja informacijske varnosti v banki, vodja oddelka za informatiko) in oceni postopke zagotavljanja skladnosti z zakonodajo
    - Opravi razgovor z vodjo oddelka za skladnost in oceni postopke zagotavljanja skladnosti z zakonodajo ter stopnjo skladnosti za področje kibernetske varnosti.
    - Pridobi in preuči poročila oddelka za skladnost glede doseganja skladnosti z zakonodajo za področje kibernetske varnosti
    - Preglej škodne dogodke za zadnji dve leti, če so bile identificirane neskladnosti ali dogodki operativnega tveganja s področja skladnosti v zvezi s kibernetsko varnostjo
    - Preveri zahteve glede doseganja skladnosti zunanjih izvajalcev z regulatornimi zahtevami (preglej pogodbe z zunanjimi izvajalci glede osnovnih zahtev iz Sklepa o ureditvi notranjega upravljanja, upravljalnem organu in procesu ocenjevanja ustreznega notranjega kapitala za banke in hranilnice ter glede zaupnosti podatkov ter varovanja osebnih podatkov)
    - Preveri poročila o spremljanju zunanjih izvajalcev za zadnji dve leti ter izvedbo morebitnih popravljalnih ukrepov

- Preveri poročila, zapisnike obravnav glede pravnih in zakonodajnih zadev v zvezi z informacijsko varnostjo (IT odbor) za zadnji dve leti.
- Ali so zakonske zahteve glede pravic intelektualne lastnine ustrezno upoštevane
- Ali so zapisi (podatki) zaščiteni pred izgubo, uničenjem, ponarejanjem, nepooblaščenim dostopom in nepooblaščeno objavo v skladu z zahtevami zakonodaje, predpisov in pogodb ter poslovnimi zahtevami (preveri skladnost s iz Sklepom o ureditvi notranjega upravljanja, upravljalnem organu in procesu ocenjevanja ustreznega notranjega kapitala za banke in hranilnice ter glede zaupnosti podatkov ter varovanja osebnih podatkov; v primeru ugotovljenih pomanjkljivosti pri izvedbi postopkov v skladu z MITRE ATT&CK preuči skladnost banke s to točko in vpliv)
- Ali so osebni podatki varovani v skladu z GDPR – pridobi poročilo DPO, opravi razgovor z DPO, preveri dogodke operativnega tveganja. Preveri ustreznost izvedbe morebitnih ukrepov.

Ugotovitve:
Banka ima vzpostavljen pravilnik o spremljanju in implementaciji zakonodaje, ki opredeljuje postopke glede spremljanja in implementacija zakonodaje za IT področje (odgovorni vodja informacijske varnosti ter Oddelek za informatiko). Akt je ustrezno posodobljen, potrjen in objavljen v zbirki internih aktov, da so z njimi seznanjene odgovorne osebe in vsi relevantni zaposleni.

Zakonske zahteve glede intelektualne lastnine ter varstva osebnih podatkov so implementirane. Razgovor z DPO (Odgovorna oseba za varstvo osebnih podatkov) ter njegova poročila niso nakazala pomanjkljivosti.

V času pregleda je bila vsa relevantna zakonodaja implementirana v banki – pregled usklajenosti med izpisom iz orodja za spremljavo ter bančnimi internimi akti ni pokazal napak, kar pomeni skladnost v celoti.

Zapisniki IT odbora vključujejo ustrezne sledi glede obravnave, akcijskih načrtov ter spremljave izvedbe. Preverjeno za EBA smernice ter Sklep Banke Slovenije v zvezi z njimi.

Razgovori z odgovornimi niso pokazali na pomanjkljivosti. Vodstvo se zaveda tveganj in posledic neskladnosti z zakonodajo, zato temu področju posvečajo veliko pozornost. Postopki so dokumentirani.

Razgovor z oddelkom za skladnost ter njihova poročila prav tako ne izpostavljajo kakšne pomanjkljivosti glede področja kibernetske varnosti. Implementacije zakonodaje so bile izveden v rokih.

Banka ima pogodbo z enim zunanjim izvajalcem za pregledano področje – dobava in vzdrževanje varnostne opreme za obdobje 1.5.2018 – 30.4.2022. Pogodbe vključujejo vse potrebne elemente (preverjeno s kontrolnikom za preverjanje zunanjih izvajalcev), nivo izvajanja se stalno spremlja (pridobljena kvartalna poročila), popravljalni ukrepi niso bili potrebni.

Za področje kibernetske varnosti ni bili evidentiranih dogodkov operativnega tveganja niti niso bili zaznani znaki glede spremljanja in implementacija zakonodaje, osebnih podatkov, intelektualne lastnine ali zunanjega izvajalca.

Podrobnosti so razvidne iz dokazil spodaj (povezave do e-hrambe).

Sklep (tveganje, vpliv, priporočila):
Pomanjkljivosti niso bile ugotovljene.

Povezave – dokazila:

- Pravilnik o spremljanju in implementaciji zakonodaje (povezava na e-hrambo)
- Varnostna politika (povezava na e-hrambo)
- Pogodba (vključno z SLA) z zunanjim izvajalcem za dobavo in vzdrževanje varnostnega sistema, izpolnjen kontrolnih za pregled (povezava na e-hrambo)
- Poročila oddelka za skladnost (povezava na e-hrambo)
- Poročila glede spremljanja zunanjega izvajalca (povezava na e-hrambo)
- Poročila in zapisniki obravnav IT odbora (povezava na e-hrambo)
- Zapisniki sestankov (povezava na e-hrambo)

Revizijsko poročilo

Pregled	Kibernetska varnost
Oznaka	RP-2021-03
Vrsta pregleda	Redni pregled
Datum poročila	9.4.2021
Skupna ocena	Primerno

Ocena:

Področje kibernetske varnosti v banki je v bistvenih elementih ocenjeno kot skladna z zakonodajo ter izbranimi dobrimi praksami. Glede strategije, upravljanja, organiziranosit, upravljanja tveganj, varnosti storitev navzven, vzpostavitve in upravljanja požarne pregrade, sistemov za informacijsko zaščito, poročanja in nadzora ni bilo ugotovljenih pomembnih pomanjkljivosti. Ugotovljene so bile pomanjlkjivosti v zvezi s socialnim inženiringom glede premajhnega zavedanja zaposlenih o informacijske varnosti in posledično neustreznega ravnanja ter v zvezi z interno razvitima aplikacijama pri notranjem varnostnem pregledu aplikacij glede pomanjkljivih varnostnih nastavitev. Zato so bila dana štiri priporočila – eno stopnje 2 glede dodatnih izobraževanj in dviga osveščenosti zaposlenih glede kibernetske varnosti ter tri stopnje 3 glede dopolnitev varnostnih nastavitev prej omenjene aplikacije. Slednje slabosti so sicer kompenzirane z drugimi kontrolami. Na podlagi tega je skupna ocena na podlagi pregleda Primerno.

Prejemniki:
Uprava

Vodja informatike
Vodja informacijske varnosti
Vodja splošnih služb
Direktor divizije Podpora

Pregled izvedel:

Milan Osterman

Potrdil:

Vodja notranje revizije

Notranje revizijski pregled je izveden skladno z Mednarodnimi standardi strokovnega ravnanja pri notranjem revidiranju. Zasnova revizijskega pregleda temelji na COSO okviru notranjih kontrol.

LEGENDA OCEN:

Dobro – Skupna ocena sistema notranjih kontrol za revidiran proces/področje/enoto je na splošno dobra. Ugotovitve kažajo samo na majhne pomanjkljivosti ali jih sploh ni. Priporočil ni oziroma jih je malo in so nizke prioritete.

Primerno – Skupna ocena sistema notranjih kontrol za revidiran proces/področje/enoto kaže zadostno mitigiranje tveganj. Ugotovitve kažajo manjše pomanjkljivosti, ki se jih lahko odpravi tekom običajnih poslovnih aktivnosti. Dana so priporočila nižje prioritete.

Pomanjkljivo – Skupna ocena sistema notranjih kontrol za revidiran proces/področje/enoto kaže nezadostno mitigiranje tveganj. Ugotovitve kažajo pomanjkljivosti, ki jih je potrebno odpraviti tekom implementacije priporočil, ki zahtevo stalno spremljavo.

Nezadovoljivo - Skupna ocena sistema notranjih kontrol za revidiran proces/področje/enoto kaže nezadostno mitigiranje tveganj. Ugotovitve kažajo pomembne pomanjkljivosti, ki jih je potrebno nemudoma odpraviti, da se tveganje zmanjša na sprejemljivo stopnjo.

VSEBINA

POVZETEK ZA VODSTVO

CILJ IN OBSEG

Cilj notranje revizijskega posla je preveriti skladnost upravljanja področja kibernetske varnosti z zakonodajo in dobrimi praksami. Dano zagotovilo se nanaša na stopnjo, v kolikšni meri kontrolni sistem na pregledanem področju izpolnjuje zahteve zakonodaje ter vodilnih dobrih praks v zvezi s kibernetsko varnostjo, kar bo dalo odgovor na vprašanje, ali je kibernetska varnost banke glede na splošno znane ranljivosti v času pregleda ustrezna in je omejeno na oceno uspešnosti delovanja kontrol z vidika skladnosti z zakonodajo in dobrimi praksami. Na sodila se nanašajo zakonodaja (Zakon o bančništvu, Sklep o ureditvi notranjega upravljanja, upravljalnem organu in procesu ocenjevanja ustreznega notranjega kapitala za banke in hranilnice, Zakon o informacijski varnosti, Zakon o varstvu osebnih podatkov, Splošna uredba o varstvu podatkov, Sklep o uporabi Smernic o poročanju o večjih incidentih v skladu z Direktivo (EU) 2015/2366 (PSD2), Smernice EBA o upravljanju tveganj, povezanih z IKT in varnostjo (EBA/GL/2019/04)), izbrane dobre prakse NIST ter glede na področja revidiranja Cobit, ISO 27001/27002, MITRE ATT&CK in interni akti.

Opravljen je bil pregled področja kibernetske varnosti, in sicer:

- Pregled strategije, podlag in notranje ureditve področja kibernetske varnosti;
- Zunanje varnostno preverjanje storitev (splošni pregled naprav in storitev opravljen z avtomatiziranimi orodji ter delno ročnimi postopki iz zunanjega omrežja, osredotočenost tega dela pregleda je bila na pridobivanju podatkov o omrežju, strežnikih, tipologiji, storitvah ter na pregledu DNS storitev, poštnih storitev, VPN povezav in na ta način odkrivanje pomanjkljivosti);
- Varnostni pregled požarne pregrade (dostopi, sistemske nastavitve, varnostne politike in nadzorovan vdorni test z uporabo omejenega nabora informacije – t.i. grey-box pristop);
- Pregled sistemov za informacijsko zaščito (SIEM sistema ter EDR orodij za zaščito končnih naprav);
- Notranji varnostni pregled kritičnih aplikacij in sistemov (varnostni pregled strežnikov in omrežnih naprav, sistemske programske opreme, izbranih štirih kritičnih aplikacij (kritične na podlagi načrta neprekinjenega poslovanja) z vidika nepooblaščenega dostopa ter nepooblaščenega izvajanja operacij), in sicer aplikacij za podporo procesu financiranja, za upravljanje portfeljev finančnih instrumentov, glavna knjiga in saldakonti, aplikacija za poročanje strank ter dveh povezanih interno razvitih aplikacij za vodenje šifrantov ter vodenje osnovnih sredstev;
- Socialni inženiring (dva scenarija ribarjenja (phising-a), eden s priponko in eden s povezavo, fizični obisk pod pretvezo, socialni inženiring prek telefona).

Tehnični del pregleda (pregled naprav in storitev opravljen z avtomatiziranimi orodji, nastavitve sistemov, priprava scenarijev ribarjenja in pošiljanje povezanih sporočil) je izvedel zunanji izvajalec pod nadzorom službe notranje revizije.

Pregledano obdobje za postopke v zvezi s pregledom evidence varnostnih dogodkov, poročil ter zapisnokov je bilo leto 2020.

Varnostni pregled sistemov s strani zunanjega izvajalca je potekal od 1.2.2021 – 10.2.2021.

OMEJITVE

Za izvedbo tehničenga dela pregleda je bil uporabljen zunanji izvajalec.

V okviru varnostnega pregleda sistemov so bile preverjene ranljivosti znane v času izvedbe aktivnosti.

KRATKA PREDSTAVITEV PODROČJA

Kibernetska varnost razume se na splošno razume kot sposobnost zaščititi, varovati in braniti kibernetski prostor pred kibernetskimi grožnjami, incidenti in kibernetskimi napadi.
V banki notranje omrežje in demilitarizirano omrežje (do slednjega se dostopa tudi od zunaj, na primer dostopi strank in e-pošta) od zunanjega omrežja (interneta) ločuje napredni požarni zid.
Odgovornost za kibernetsko varnost se deli predvsem med varnostnega inženirja (vsebinski vidik) ter oddelkom za informatiko (tehnični vidik), vendar morajo ustrezen nivo zavedanja imeti vsi zaposleni, saj se jih lahko izrabi v okviru socialnega inženiringa za kibernetski napad. Pomembni sta tudi ustrezna nastavitve (konfiguracije) ter ažurno osveževanje programske opreme z varnostnimi popravki.
Za zaznavo in upravljanje varnostnih dogodkov v informacijskem sistemu banke se uporablja tudi poseben sistem (SIEM), s katerim upravlja OE za informacijsko varnost s pomočjo zunanjega izvajalca.

Pogosteje uporabljene kratice:
DNS – Sistem domenskih imen (Domain Name System)
VPN – Navidezno zasebno omrežje (Virtual Private Network)
SIEM - Sistem za upravljanje varnostnih dogodkov in tveganj (Security Information and Event Management)

OCENE PODPODROČIJ Z UTEMELJITVAMI

Revidirano podpodročje	Dobro	Zadovoljivo	Nezadovoljivo	Slabo
Strategija, upravljanje, organiziranost				
Upravljanje tveganj				
Upravljanje pravic dostopov				
Upravljanje požarne pregrade in javnega segmenta informacijskega sistema banke				
Upravljanje sistemov za informacijsko zaščito				
Upravljanje kritičnih aplikacij in sistemov				
Socialni inženiring				
Poročanje				
Nadzor				
Skupna ocena				

Področje informacijske varnosti je ustrezno vključeno v IT strategijo banke, ki je redno osveževana. Vzpostavljeni so podrobni cilji ter kazalniki, ki se redno ocenjujejo in pregledujejo za ocenjevanje uspešnosti in obsega izvrševanja. Področje prejema dovolj pozornosti vodstva ter sredstev, vzpostavljen je IT odbor, kot

svetovalni odbor upravi, ki redno obravnava tudi zadeve s področja kibernetske varnosti. Pomembne stvari se poročajo nadzornemu svetu v okviru upravljanja tveganj.

Varnostna politika s prilogami je vzpostavljena in redno ažurirana, in sicer ob pomembnih spremembah oziroma pregledana najmanj letno. Postopki so opredeljeni v internih aktih, ki se prav tako redno pregledujejo in osvežujejo. V času revizijskega pregleda je bilo v prenovi delovno navodilo za upravljanje sistema elektronske pošte zaradi menjave poštnega strežnika. V fazi načrtovanja je bilo ugotovljeno, da Navodilo za upravljanje varnostnih sistemov ni ažurirano s spremembami zaradi nove opreme, vendar je bilo dopolnjeno tekom pregleda. Odgovornosti in naloge so podrobno opredeljene, zaposleni so ustrezno izobraženi, saj se redno udeležujejo načrtovanih izobraževanj, njihovo število je zadostno, da omogoča ustrezno razmejitev dolžnosti ter nadomeščanje. Varnostni inženir ima nadomeščanje v okviru banke, poleg tega je pogodbeno urejeno sodelovanje z zunanjim izvajalcem, ki delno izvaja storitve SOC centra/Varnostno operativnega centra. Pogodbena razmerja so ustrezno urejena vključno z dogovorom o nivoju storitev, delovanje se stalno spremlja.
Formalni postopki spremljanja in implementacije regulative so vzpostavljeni, odgovornosti so določene za vsa področja. Pregled zadnjih sprememb je pokazal, da so zakonodaja in predpisi ustrezno vključeni v dokumente banke. Področje kibernetske varnosti je vključeno v redno ocenjevanje tveganj. Tveganja se identificirajo najmanj enkrat letno ter ob vsaki pomembni spremembi. Nagnjenost k prevzemanju tveganj je za revidirano področje določena in potrjena. Zadnja identifikacija in ocena tveganja sta bili izvedeni v septembru 2020 zaradi prilagoditev aplikacij novim produktom. V okviru revizijskega pregleda so bili pregledani postopki identifikacije ter ocenjevanja inherentnih tveganj, predpostavke in parametri, ustreznost ocene kontrolnega okolja ter preostalega tveganja. Indikatorji nagnjenosti k prevzemanju tveganj niso bili preseženi v nobenem primeru, prav tako niso bile odkrite pomanjkljivosti pri pregledu postopkov identifikacije ter ocenjevanja tveganj.
Proces upravljanja sprememb je opredeljen, postopki, odgovornosti in orodja so določeni. Revizijska sled se vodi, poročila se redno pripravljajo in posredujejo.

Postopki v zvezi z logičnimi kontrolami dostopov so vzpostavljeni, odgovornosti so prav tako opredeljene. Zahtevki in delovni tok je podprt s posebno aplikacijo. Ni bilo ugotovljenih pomanjkljivosti glede dostopov tako z vidika skladnosti zahtevkov in dejanskega stanja ter omejitve na minimalni potrebni obseg pravic. Pregled na vzorcu ni pokazal pomanjkljivosti (10% naključno izbranih aktivnih uporabnikov AD s preveritvijo za vse sisteme, zaposleni s spremembami delovnih mest v zadnjih dveh letih). Prav tako ni bilo ugotovljenih pomanjkljivostih pri uporabnikih s privilegiranimi pravicami (dodeljevanje, odvzemanje gesel, upravičenost dodelitve, uporaba ROOT gesel). Vsi oddaljeni dostopi se spremljajo glede časovnih oken, uporablja se dvofaktorska avtentikacija. Redno se preverja upravičenost dodelitve, za vse dodelitve je potrebno izvesti poseben postopek (izveden za vse primere).

Požarna pregrada je ustrezno vzpostavljena – programska oprema je ažurirana, fizična postavitev ter segmenti so ustrezno vzpostavljeni. Varnostne politike so vzpostavljene in se upoštevajo. IPS/IDS zaščita je vključena, uporabljeni protokoli se avtomatično pregledujejo. Segmenti so ustrezno vzpostavljeni, prehodi so omejeni glede na popise tokov, z izjemo enega strežnika. Pri slednjem je bilo ugotovljeno, da je bil postavljen tik pred pregledom in zato dokumentiranje še ni bilo v celoti zaključene. Ker je preveritev pokazala, da postopki potekajo v skladu z načrti, priporočilo ni podano. Administracija je ustrezno urejena, tako z vidika dostopov kot beleženja in upravljanja sledi,. DMZ prostor je restriktivno ločen od ostalega omrežja. Vdorni test ni pokazal pomanjlkjivosti, Varnostni pregled požarne pregrade je bil tudi izveden s strani zunanjega izvajalca.

Pri pregledu zunanjih storitev banke, ki je bil izveden s strani zunanjega izvajalca, je bil predmet pregleda javni naslovni prostor banke (javni segment informacijskega sistema) vključno s storitvami DNS (sistem domenskih ime) in SMTP (protokol za prenos e-pošte). Pri tem ni bilo ugotovljeno, da bi bilo dostopnih preveč informacij, ki bi pomagale napadalcem. Skeniranje naprav je bilo izvedeno z namenskimi orodji (NMAP, Nessus, Metasploit Framework), čemur je sledil ročni pregled. Pomanjkljivosti pri tem niso bile ugotovljene. Varnostni popravki so ažurno nameščeni, uporabljajo se močni algoritmi in protokoli. Redunanca DNS strežnikov je vzpostavljena, prav tako so ustrezno onemogočene storitve nepooblaščenim osebam. Ranljivosti

SMTP strežnikov elektronske pošte niso bile zaznane, zaščita proti pošiljanju nezaželene pošte je vzpostavljena, aktivirani so mehanizmi za preprečevanje ponarejenih sporočil. Na nivoju omrežja pregled ni pokazal varnostnih pomanjkljivosti v konfiguraciji VPN sistema.

Pri pregledu sistemov za informacijsko zaščito je bilo ugotovljeno, da so ti sistemi (SIEM, EDR - zaščita končnih naprav) ustrezno vzpostavljeni z vidika zmogljivosti in varnosti, da so sposobni pravočasno zaznati varnostne dogodke, prav tako so ustrezni postopki obravnave ter sporočanja. Pregled je temeljil na simulaciji napadov v povezavi z vdornimi testi pri pregledu požarne pregrade in ga je izvedel zunanji izvajalec. Vsi simulirani varnostni dogodki so bili pravočasno zaznani s strani varnostnih centralnih sistemov oziroma na končnih napravah, uspešno sporočeni v sistem SIEM, sproženi so bili ustrezni ukrepi. Vsak varnostni dogodek je vpisan v poseben sistem za vodenje zahtevkov, bistveni podatki so obvezna polja za vnos. Poročilo o zamudah pri ukrepih se redno generira ter posreduje. Tekom pregleda ni bilo zaznanih pomanjkljivosti, da določeni viri (naprave) ne bi bili vključeni. Kontrole za preprečevanje odtekanja podatkov so vzpostavljene - tako preprečevalne (omejitve na portih in uporabi oblačnih in sorodnih rešitvah) kot zaznavalne (nenavadni prenosi). Vse naprave imajo popisane dovoljene tokove ("karton"), poskusi nedovoljenih se spremljajo in obravnavajo. Poročila o delovanju sistemov z vidika zmogljivosti ter poročila o testiranjih so pokazala, da so zmogljivosti ustrezne. Vzpostavljen je postopek spremljanja limitov ter eskalacijski mehanizmi, prav tako odgovornosti.

Notranji varnostni pregled kritičnih aplikacij (za podporo procesu financiranja, za upravljanje portfeljev finančnih instrumentov, glavna knjiga in saldakonti, aplikacija za poročanje strank ter dveh povezanih interno razvitih aplikacij za vodenje šifrantov ter vodenje osnovnih sredstev) in sistemov je bil izveden s strani zunanjega izvajalca z namenskim orodjem (Nessus) ter ročnimi postopki, in sicer sta bila preverjena vidika nepooblaščenega dostopa ter nepooblaščenega izvajanja operacij. Pri aplikacij za upravljanje z osnovnimi sredstvi je bilo ugotovljeno, da komunikacija s sistemom za upravljanje zbirk podatkov poteka z uporabo ranljivega protokola, kar bi v primeru prestrezanja napadalcu olajšalo možnost dešifriranja poslanih podatkov (priporočilo RP-2021-03-01). Za interno razvito aplikacija za vodenje šifrantov je bilo ugotovljeno, da razkriva podatke o zaledni infrastrukturi (priporočilo RP-2021-03-02) ter da uporablja neustrezen certifikat (priporočilo RP-2021-03-03). V vseh drugih primerih se uporabljajo močni šifrirni algoritmi, močni protokoli ter ustrezni certifikati.

V okviru izvajanja postopkov socialnega inženiringa sta bila izvedena dva scenarija ribarjenja (phisinga) – najprej je bilo poslano lažno sporočilo kadrovske službe s podatki o finančni nagradi v pripeti zlonamerni datoteki, nato pa še vabilo k prijavi v nov lažni spletni portal banke prek povezave v sporočilu. Datoteko so kljub znakom, da je sporočilo lažno, odprli trije zaposleni, na spletno povezavo v drugem lažnem sporočilu pa je kliknilo šest zaposlenih, nobeden ni vnesel prijavni podatkov (priporočilo RP-2021-03-04). Fizični obisk pod pretvezo je bil neuspešen, saj je receptor vse poskuse vstopa zaustavil, tudi poskusi pridobivanja podatkov prek telefona so bili neuspešni.

Pri poročanju pomanjkljivosti niso bile ugotovljene. Najmanj mesečno oziroma pogosteje po potrebi varnostni inženir v sodelovanju z oddelkom za informatiko ter po potrebi tudi drugimi odgovornimi enotami pripravi redno poročilo, ki ga obravnava IT odbor, z njim je seznanjena tudi uprava. Nadzorni svet se seznani s pomembnimi zadevami v okviru upravljanja tveganj.
Tudi glede nadzora ni bilo ugotovljenih pomanjkljivosti. Vodstveni nadzor se izvaja in se dokumentira, kar potrjujejo poročila o delu organizacijskih enot za upravo. IT odbor zaseda redno, vse pomembne zadeve so uvrščene na dnevni red, obravnave so ustrezno dokumentirane, ukrepi se spremljajo. Uprava potrjuje pomembne zadeve, kjer je zahtevano, oziroma je seznanjena. Tudi obravnave nadzornega sveta so ustrezno dokumentirani, realizacija sklepov se spremlja. Poročila organizacijske enote Informacijska varnost potrjujejo izvedbo vsaj enega obsežnejšega pregleda s področja informacijske varnosti letno, ukrepi se spremljajo in poročajo.

UGOTOVITVE IN PRIPOROČILA

Komunikacija med aplikacijo za vodenjem osnovnih sredstev in povezanim sistemom za upravljanje zbirk podatkov na osnovi ranljivega protokola	
Oznaka ugotovitve	RP-2021-03-01
Proces	Informacijsko-tehnološka podpora
Nosilec tveganja	Informatika
Skupina tveganj	Operativno
Prioriteta priporočila	3

Ugotovitev
Aplikacija za upravljanje z osnovnimi sredstvi zapisuje podatke v ločeno zbirko podatkov v okviru sistema Oracle. Komunikacija med samo aplikacijo ter sistemov za upravljanje zbirk podatkov Oracle poteka na osnovi protokola TLS 1.0. Ta verzija protokola je zastarela (najnovejši PCI DSS standard je niti ne dovoljuje več) in ranljiva (ranljivost CVE-2011-3389).

Vzrok in vpliv
Aplikacija za upravljanje z osnovnimi sredstvi je v uporabi že vrsto let. Ob njenih nadgradnjah se protokol komuniciranja s sistemom za zpravljanje zbirk podatkov ni spreminjal. Zunanji razvijalec aplikacije pojasnjuje, da se protokol ni spreminjal, ker je aplikacija v uporabi pri večih strankah in bi lahko pri kateri od njih prišlo do napak pri delovanju sistema. Razvijalec ocenjuje, da ker komunikacija poteka samo interno, znotraj notranjega omrežja ob pravilnih varnostnih mehanizmih tveganje zanemarljivo.
V primeru, da bi napadalec uspel vdreti v notranje omrežje banke bi zaradi uporabe zastarelega protokola lažje razvozlal poslane podatke med aplikacijo za upravljanje z osnovnimi sredstvi ter sistemov sistemov za upravljanje zbirk podatkov. Ker komunikacija poteka le v notranjem omrežju banke, ki je primerno varovano, ter se prenašajo manj kritični podatki z vidika zaupnosti preostalo tveganje res ni visoko.

Priporočilo
Priporoča se sprememba protokola s ciljem povišenja varnosti ter ocena varnosti, ki jo zasleduje zunanji izvajalec ter glede na ugotovitve izvedba ukrepov.

Akcijski načrt

Oznaka ukrepa	Ukrep	Odgovorni za izvedbo	Rok
RP-2021-03-01.01	Analiza vplivov spremembe protokola na delovanje sistema.	Oddelek za informatiko	15.4.2021
RP-2021-03-01.02	Nadgradnja protokola.	Oddelek za informatiko	30.4.2021
RP-2021-03-01.03	Preučitev pogodbenih razmerij z zunanjim razvijalcem glede pogodbenih določil za zagotavljanje ustreznega nivoja varnosti sistemov	Skupne službe	30.4.2021

Interno razvita aplikacija za vodenje šifrantov razkriva podatke o zaledni infrastrukturi	
Oznaka ugotovitve	RP-2021-03-02
Proces	Informacijsko-tehnološka podpora
Nosilec tveganja	Informatika
Skupina tveganj	Operativno
Prioriteta priporočila	3

Ugotovitev
Za interno razvito spletno aplikacijo za vodenje šifrantov je bilo ugotovljeno, da razkriva podatke o zaledni infrastrukturi, ki niso nujni za delovanje aplikacije.

Vzrok in vpliv
Aplikacija je bila razvita interno v banki kot preprosto orodje za pomoč pri vodenju šifrantov. Ker se uporablja le interno, ni bila varnostno pregledana, kot je to zahtevano za kritične aplikacije.
Podatki, ki jih aplikacija razkriva bi napadalcu olajšale delu pri pridobivanju nepooblaščenega dostopa in uporabe. Ker se aplikacija uporablja le v notranjem omrežju banke ter se v njej obdelujejo le podatki, ki so z vidika zaupnosti manj kritični, preostalo tveganje ni visoko.

Priporočilo
Priporoča se prikritje podatkov o zaledni infrastrukturi.

Akcijski načrt

Oznaka ukrepa	Ukrep	Odgovorni za izvedbo	Rok
RP-2021-03-02.01	Spremenijo se nastavitve, ki bodo preprečevale razkrivanje podatkov o o zaledni infrastrukturi.	Oddelek za informatiko	15.4.2021

Interno razvita aplikacija za vodenje šifrantov uporablja neustrezen certifikat	
Oznaka ugotovitve	RP-2021-03-03
Proces	Informacijsko-tehnološka podpora
Nosilec tveganja	Informatika
Skupina tveganj	Operativno
Prioriteta priporočila	3

Ugotovitev
Interno razvita aplikacija za vodenje šifrantov uporablja za avtentikacijo pri komunikaciji z drugimi sistemi neustrezen certifikat.

Vzrok in vpliv
Aplikacija uporablja neustrezen certifikat zaradi napačnih nastavitev pri njenem razvoju. V primeru, da napadalec pridobi dostop do certifikata, lahko prestreza komunikacijo pri sistemih, ki ga uporabljajo, torej v tem primeru pri interno razviti aplikaciji za vodenje šifrantov. Ker aplikacija deluje oziroma komunicira le v notranjem omrežju banke, ki je primerno varovano, ter ne obdeluje podatkov, ki so z kritični vidika zaupnosti, preostalo tveganje ni visoko.

Priporočilo
Priporoča se uporabo ustreznega certifikatov za specifično aplikacijo.

Akcijski načrt

Oznaka ukrepa	Ukrep	Odgovorni za izvedbo	Rok
RP-2021-03-03.01	Sprememba nastavitve aplikacije, da bo uporabljala ustrezen certifikat.	Oddelek za informatiko	

Uspešna simulacija napada ribarjenja (phising napada) zaradi prenizke osveščenosti zaposlenih	
Oznaka ugotovitve	RP-2021-03-04
Proces	Informacijsko-tehnološka podpora
Nosilec tveganja	Informacijska varnost
Skupina tveganj	Operativno
Prioriteta priporočila	2

Ugotovitev

V okviru izvajanja postopkov socialnega inženiringa sta bila izvedena dva scenarija ribarjenja (phisinga):

- najprej je bilo poslano lažno sporočilo kadrovske službe s podatki o finančni nagradi v pripeti zlonamerni datoteki,
- nato je bilo poslano še vabilo k prijavi v lažni spletni portal prek povezave v sporočilu.

Datoteko so kljub znakom, da je sporočilo lažno (napačni zapisi imen organizacijskih enot, tuja domena), odprli trije zaposleni, na spletno povezavo v drugem lažnem sporočilu (spletni portal povsem nepovezan z banko, tuja domena) pa je kliknilo šest zaposlenih, vendar nobeden ni vnesel prijavnih podatkov. Sicer je potrebno upoštevati, da je bilo po dogovoru med zunanjim izvajalcem in banko potrebno omiliti avtomatske kontrole sistema banke, ki preprečujejo prejem elektronske pošte s sumljivo vsebino, saj so se sporočila sicer najprej uvrstila v karanteno, iz katere jih je potrebno sprostiti ročno. Poleg tega sistem preprečuje zagon datotek iz zunanjih virov v primeru podatkov o finančni nagradi, medtem ko v primeru lažne povezave svojih podatkov ni vnesel nobeden od zaposlenih.

Vzrok in vpliv

Napadi so bili uspešni zaradi prenizke osveščenosti zaposlenih. Čeprav je vsak zaposleni deležen ustreznega izobraževanja ob nastopu dela, vsaj enkrat letno se izvedejo posebne izobraževalne aktivnosti s področja kibernetske varnosti, ki vključujejo socialni inženiring ter vsaj enkrat mesečno varnostni inženir obvešča o napadih, se zaposleni premalo zavedajo tveganj povezanih s tem. V primeru uspešne izvedbe socialnega inženiringa lahko napadalec pridobi možnost dostopa do IT sistemov banke, zaupnih podatkov ali povzroči škodo na virih banke, ki lahko predstavlja pomemben negativni finančni vpliv na banko ali izgubo ugleda.

Priporočilo

Priporoča se:

- izvedba dodatnih izobraževanj s podrobno predstavitvijo tveganj,
- preverjanje osveščenosti zaposlenih,
- preglede (testiranja) na tem področju (napadi ribarjenja - phising).

Akcijski načrt

Oznaka ukrepa	Ukrep	Odgovorni za izvedbo	Rok
RP-2021-03-04.01	Izvedba dodatnega izobraževanja za vse zaposlene s podrobno predstavitvijo tveganj in možnih vrst napadov v praksi. Izobraževanje bo vključevalo preverjanje znanja.	Varnostni inženir	31.5.2021
RP-2021-03-04.02	Redni letni varnostni pregledi s simulacijami napadov	Varnostni inženir	31.12.2021

	ribarjenj, izvedba prvega do konca leta 2021.		

OSTALO

USKLAJEVANJE
Osnutek poročila je bil revidirancem poslan 30.3.2021. Zaključni sestanek je bil izveden dne 5.4.2021. Pripombe so bile smiselno upoštevane po presoji službe notranje revizije. Pomembnih razlik v stališčih med revidiranci in službo notranje revizije ni bilo, vsa priporočila vključno z roki za izvedbo ukrepov so usklajena.

RAZNO
Podrobnosti pregleda so razvidne iz delovnih papirjev, ki jih hrani služba notranje revizije. Skupaj je bilo za pregled porabljeno 21 človek dni (brez upoštevanja časa zunanjega izvajalca, vključen čas za koordinacijo).